

## SAB 2016. GADA DARBĪBAS PĀRSKATS

Satversmes aizsardzības birojs (SAB) ir viena no trim Latvijas valsts drošības iestādēm. Likumā noteiktā kārtībā SAB veic izlūkošanu un pretizlūkošanu, klasificētās informācijas aizsardzību, kā arī veic un kontrolē informācijas apmaiņu ar starptautiskām organizācijām.

SAB 2016. gada darbības pārskatā svarīgākais:

- Būtiskākos drošības draudus reģionā rada Krievija – tās agresija Ukrainā, militārā spēka demonstrēšana un provokācijas NATO ārējo robežu tiešā tuvumā, pret kaimiņvalstīm vērstie informatīva kara un hibrīdkara elementi.
- Varas režīms Krievijā kontroli pār iekšpolitiskajiem procesiem nodrošina, arvien lielākā mērā ierobežojot demokrātiju, pilsonisko brīvību un mediju neatkarību. Uz Krievijas iedzīvotājiem vērstā propaganda uzsver Rietumvalstu atbildību par Krievijas sarežģīto ekonomisko situāciju un iedzīvotāju dzīves līmeņa pasliktināšanos.
- Krievijas izlūkošanas un drošības dienesti izvērš aktīvu darbu pret Latviju un sabiedroto interesēm. Izlūkošanas prioritāte ir NATO drošības politika un aktivitātes reģionā, kā arī Latvijas aizsardzības un militārās spējas. SAB konstatējis interesi par plaša spektra iekšpolitikas, ārpolitikas un ekonomikas jautājumiem.
- Krievijas ietekme Latvijas informatīvajā telpā joprojām veido vienu no būtiskākajiem Latvijas valsts drošības ilgtermiņa apdraudējumiem. Līdzīgi kā iepriekšējā periodā arī 2016. gadā Krievijas propaganda bija vērstā uz NATO un Latvijas drošības politikas diskreditāciju un centieniem mazināt sabiedrības atbalstu NATO spēku klātbūtnes palielināšanai reģionā.
- Pēdējos gados sabiedrība Baltijas jūras reģionā, kā arī Rietumvalstīs kopumā, ir kļuvusi kritiskāka pret Krievijas propagandu, apmelošanas un diskreditācijas kampaņām, Maskavas vadītu pseidoeskspertu un prokrievisku organizāciju centieniem imitēt pilsoniskas aktivitātes.
- Krievijas pieaugošās kiberspējas un gatavība tās pielietot rada vienu no visstraujāk augošajiem draudiem Rietumvalstu drošībai. 2016. gadā vairāki kiberuzbrukumi Latvijā tika vērsti pret valsts institūcijām, kā arī privātām kompānijām un medijiem. Kiberuzbrukumi Latvijā visbiežāk tiek veikti spiegošanas nolūkā, inficējot mērķa personas datoru, kad tas atver viltotu e-pasta vēstuli.

### Ievads

2016. gads Eiropas drošībai bija pilns izaicinājumu. Krievija turpināja agresiju Ukrainā, īstenoja militāras aktivitātes reģionā un izvērta nemilitāros līdzekļus situācijas ietekmēšanai citās valstīs. Lielu apdraudējumu radīja starptautiskais terorisms, ekstrēmisms un radikalizācija, joprojām aktuāls bija migrācijas jautājums un konflikta attīstība Tuvajos Austrumos un Ziemeļāfrikā.

Latvijā būtiskākos drošības apdraudējumus rada Krievijas agresīvā politika, tajā skaitā pret Latviju vērstās ietekmes aktivitātes un propaganda, Krievijas izlūkošanas un drošības dienestu darbība. Kā viens no straujāk augošajiem draudiem Rietumvalstu, tajā skaitā Latvijas, drošībai ir Krievijas radītais kiberapdraudējums.

Aizvadītais gads bija zīmīgs ar NATO lēmumu palielināt sabiedroto klātbūtni reģionā, sniedzot Baltijas valstīm un Polijai atbalstu NATO ārējo robežu drošības garantēšanā. NATO kolektīvās drošības stiprināšana ir SAB darbības pamatā, īstenojot izlūkošanas, pretizlūkošanas un klasificētās informācijas aizsardzības funkcijas.

## Krievija

Galvenie Krievijas ārpolitikas mērķi nav mainījušies un tie ir - atjaunot un nostiprināt Krievijas ietekmi it īpaši postpadomju valstīs un Eiropā, un tikt atzītai par pasaules lielvaru. Krievija koncentrējās uz savas ietekmes un lomas palielināšanu reģionālā un globālā līmenī, kā arī uz Rietumvalstu pozīciju un vienotības vājināšanu.

Krievija joprojām NATO vērtē kā oponentu. 2016. gada decembrī apstiprinātajā Krievijas Ārpolitikas koncepcijā NATO paplašināšanās un militārās klātbūtnes palielināšanās Krievijas pierobežā joprojām tika raksturota kā drauds Krievijas drošībai. Lai izdarītu spiedienu uz kaimiņvalstīm un NATO, Krievija izteikti demonstrēja savu militāro varenību arī Baltijas jūras reģionā. Krievijas lidaparāti vairākkārt pārkāpa kaimiņvalstu gaisa telpu vai arī veica bīstamus manevrus Latvijas sabiedroto militāro vienību tuvumā. Tāpat uz Krievijas pierobežas rajoniem un konflikta reģioniem tika nosūtīts papildu militārais aprīkojums. Militārā spēka demonstrācijas tika kombinētas ar attiecīgu politisko retoriku un propagandu. Krievija savas aktivitātes publiski attaisno kā atbildes reakciju uz palielinātu, un Krievijas medijos pārspīlētu, NATO dalībvalstu militāro klātbūtni tās robežu tuvumā, taču Krievija pastiprinātu militārā spēka izvēršanu uzsāka vēl ilgi pirms NATO lēmuma par klātbūtnes pastiprināšanu Baltijā.

Nozīmīgu lomu Krievijas stratēģiskajā komunikācijā ieņem militārās mācības, kuru apmērs un skaits pēdējo gadu laikā ir ievērojami pieaudzis. 2016. gadā lielākās Krievijas militārās mācības *Kavkaz-2016* notika Ukrainas tuvumā. To laikā Krievija uzskatāmi demonstrēja gatavību nepieciešamības gadījumā militāri aizsargāt savas tiesības uz Krimu. Īpaši vērienīgas Krievijas un Baltkrievijas militārās mācības *Zapad-2017* šoruden notiks pie NATO dalībvalstu robežām.

Krievija turpināja meklēt dažādus veidus, kā pārvarēt starptautisko izolāciju un panākt savu ārpolitisko interešu realizāciju dažādos jautājumos. Sīrijas konfliktā Krievija ir viena no galvenajām ieinteresētajām pusēm, kura nevēlas, lai tai tuvs sabiedrotais Sīrijas līderis Asads zaudētu varu. Asada atbalstīšanai un Eiropas Savienības demonstratīvai šķelšanai Krievija izmantoja arī Krievijas ārpolitikai simpatizējošu Eiropas Parlamenta deputātu no vairākām valstīm vizītes Sīrijā. Krievija izmantoja līdzīgas simboliskas vizītes, kurās bija iesaistīti dažāda līmeņa pārstāvji no ES valstīm, lai leģitimizētu Krimas aneksiju un demonstrētu vienotības trūkumu ES pieņemto sankciju turpināšanai.

2016. gadā Krievija turpināja izmantot dažādas informatīva kara un hibrīdkara metodes, lai vājinātu Rietumvalstu pozīcijas globālā līmenī, sašķeltu Rietumvalstu vienotību, īpaši ES un NATO ietvaros, un ietekmētu politiskos procesus šajās valstīs. Arvien aktīvāk tiek izmantotas kiberspējas. Publiskajā telpā plaši izskanējusi informācija par centieniem ietekmēt ASV prezidenta vēlēšanas, kad kiberuzbrukumu laikā iegūtā informācija tika izmantota, lai manipulētu ar sabiedrisko domu un ietekmētu vēlēšanu izvēli. Krievijas informatīvā kara metodes bija vairāk vērstas uz jau esošo Krievijas atbalstītāju mobilizāciju, nevis uz jaunu atbalstītāju piesaistīšanu. Kopumā Krievijas propaganda efektīvāk strādāja NVS valstīs, tomēr tā tika vēsta arī pret Eiropu. Krievija atvēl ievērojamus resursus telekanāla "RT" un multimediju platformas "Sputnik" darbībai Eiropā, tomēr iepretim ieguldītajam efekts ir niecīgs. Lai arī Krievija ir panākusi plašu "RT" televīzijas pieejamību, tās reitingi ir zemi. Saskaņā ar starptautisko kompāniju "Gallup" un "Pew Research" aptaujām pēdējos gados Krievijas un V. Putina personīgais tēls ir negatīvs un būtiski atpaliek no ASV, ES, Vācijas, Ķīnas. Tas ir spēkā arī starp to valstu iedzīvotājiem, kuri tradicionāli uzskatīti par Krievijai draudzīgiem, piemēram, Vācija, Francija, Itālija. Salīdzinot ar propagandu, Kremļa intereses Rietumvalstīs ievērojami efektīvāk nodrošina ekonomiskais lobījs.

Krievijas izlūkošanas un drošības dienesti nemainīgi ir viens no būtiskākajiem V. Putina režīma varas elementiem. Izlūkošanas un drošības dienesti realizē gan režīma iekšpolitiskās, gan arī ārpolitiskās intereses – Krievijā neitralizē režīma oponentus un režīmam nevēlamas parādības, savukārt ārpus tās iegūst izlūkošanas informāciju, realizē ietekmes pasākumus, tostarp arī

provokācijas un agresīvas operācijas, kā tas notiek Ukrainā. Krievijas izlūkošanas un drošības dienestu ietekme un pilnvaras turpina palielināties. Aizvadītā gada pavasarī tika uzsākta viena no nozīmīgākajām pēdējo gadu reformām, kuras rezultātā tiks izveidots jauns valsts iekšējās drošības stiprināšanai paredzēts drošības dienests – Nacionālā garde. Paredzams, ka uz iekšlietu karaspēka un dažādu speciālo vienību pamata veidotā dienesta formēšana noslēgsies 2018. gada sākumā, tajā ietverot vairākus simtus tūkstošus militārpersonu.

V. Putina režīma galvenais iekšpolitikas uzdevums nemainīgi ir valsts iekšējo procesu kontroles un stabilitātes nodrošināšana, kas tiek panākta, arvien lielākā mērā ierobežojot demokrātiju, pilsonisko brīvību un mediju neatkarību. Pēdējos gados Krievijā pieņemti vairāki likumi, kuru rezultātā būtiski paplašinājušās varas iespējas vērsties pret tai nevēlamām organizācijām, medijiem un personām. Kontroles palielināšana tiek pamatota gan ar cīņu pret terorismu, gan naidīgu ārvalstu ietekmi. Specdienesti un tiesībsargājošās iestādes arī pirms likumu pieņemšanas ir īstenojušas represijas pret nevēlamām aktivitātēm vai viedokļiem, patvaļīgi interpretējot tiesību normas un piedēvējot “ekstrēmismu” visdažādākajām iedzīvotāju vai pilsonisko organizāciju aktivitātēm.

Visi ietekmīgākie mediji Krievijā pieder valsts kompānijām vai režīmam pietuvinātiem īpašniekiem. 2016. gada janvārī spēkā stājās grozījumi likumā “Par masu medijiem”, kas noteica, ka ārvalstniekiem drīkstēs piederēt tikai 20% mediju kapitāldaļu, kā arī ir aizliegts Krievijā reģistrēt medijus. Šo likuma izmaiņu rezultātā lielākā daļa ārvalstu mediju Krievijā darbību ir pārtraukuši.

Vēl pirms medijiem ierobežojumi tika piemēroti nevalstiskām organizācijām (NVO), kas saņem ārvalstu finansējumu un iesaistās politiskās aktivitātēs, turklāt politisko aktivitāšu jēdziens tiek piemērots visai plaši. Šādām NVO jāreģistrējas kā “ārvalstu aģenti”, tās ir pakļautas stingrai uzraudzībai un virknei ierobežojumu. “Ārvalstu aģentu” sarakstā iekļautās NVO bieži saskaras ar naidīgu attieksmi, jo sabiedrībai ir ilgstoši skaidrots, ka Rietumvalstis vēlas panākt situācijas destabilizāciju Krievijā.

2016. gada jūlijā Krievijas prezidents apstiprināja vairāku desmitu likumu grozījumus jeb tā saukto “Jarovajas likumu paketi”. Oficiāli tie ir vērsti pret terorismu un ekstrēmismu, bet faktiski vienkāršo varas iestāžu iespējas vērsties pret režīmam nevēlamām organizācijām un personām, piemērojot tām administratīvus un kriminālus sodus. Pieņemtajos grozījumos iekļauta norma, kas nosaka, ka telekomunikāciju kompānijām un interneta operatoriem no 2018. gada 6 mēnešus jāglabā visi dati (informācija par telefonsarunām, epastiem, lejupielādētiem datiem utt.), kā arī jānodrošina specdienestiem pieeju šiem datiem pat bez īpašas tiesas atļaujas. Kompānijām ir jānodrošina specdienestiem arī šifrēto datu atšifrēšanas iespējas.

Uz Krievijas iedzīvotājiem vērstā propaganda uzsver Rietumvalstu atbildību par Krievijas sarežģīto ekonomisko situāciju un iedzīvotāju dzīves līmeņa pasliktināšanos - divu gadu laikā iedzīvotāju reālie ienākumi samazinājušies vidēji par 12,3 %. Vissliktākā ekonomiskā situācija bija novērojama Krievijas reģionos, kuros pieaugusi sociāli ekonomiskā spriedze un neapmierinātība. Pusē Krievijas reģionu gadā laikā pieauguši parādi. Savukārt eksperti secinājuši, ka astoņos Krievijas federālajos apgabalos novērojamas ekonomiskās depresijas pazīmes. “Pelēkās” ekonomikas īpatsvars ekonomiski aktīvo iedzīvotāju vidū sasniedzis aptuveni 40 %. Lai novērstu finansiālu sabrukumu pēc straujā naftas cenas un budžeta ieņēmumu krituma, Krievija 2016. gadā aktīvi izmantoja iepriekšējos periodos uzkrātās rezerves, mobilizēja ieņēmumus no valsts kompānijām, palielināja atsevišķus nodokļus. Krievija arī realizēja vairāku valsts aktīvu pārdošanu, taču tā nereti izvērtās par aktīvu pārdali starp elites pārstāvjiem aizdomīgu darījumu virknējumā.

2016. gada nogalē pēdējos divus gadus novērotā ekonomikas lejupslīde Krievijā faktiski beidzās un ir vērojamas stabilizācijas pazīmes, tomēr kopumā ekonomiskā situācija joprojām ir sarežģīta. Nepieciešamās reformas tiek novilcinātas, budžets joprojām atkarīgs no naftas cenām, savukārt finanšu rezerves, kuras līdz šim bija nozīmīgākais budžeta stabilitātes elements, saskaņā ar ekspertu aplēsēm tiks iztērētas tuvākā gada – pusotra laikā.

## **Ārvalstu izlūkošanas un drošības dienesti**

Ārpus NATO un ES valstu izlūkošanas un drošības dienestu (turpmāk – ārvalstu specdienestiem) darbs ir būtisks valsts drošības apdraudējums, kas vērsts gan pret Latvijas nacionālajām, gan sabiedroto interesēm un kolektīvo drošību. Ārvalstu specdienestu darbības mērķis ir iegūt publiski nepieejamu un apsteidzošu informāciju, kas dienesta pārstāvētajai valstij dotu priekšrocības politisku, ekonomisku un militāru lēmumu pieņemšanai. Bez informācijas vākšanas specdienesti īsteno aktīvos pasākumus, kuru mērķis ir ietekmēt Latvijas, ES un NATO lēmumu pieņemšanu, kā arī sabiedrības viedokli.

2016. gadā SAB īstenoja pretizlūkošanas darbu pret vairāku ārvalstu specdienestiem. Lielāko apdraudējumu Latvijas interesēm rada Krievijas izlūkošanas un drošības dienestu aktīvā darbība, savukārt citu valstu specdienestu aktivitātes vērtējamas kā mērenas un būtisku apdraudējumu Latvijas interesēm nerada.

Ārvalstu specdienesti aktivitātes pret Latviju izvērš, izmantojot diplomātisko pārstāvniecību piesegu un strādājot no savas valsts teritorijas. Darbs no teritorijas ietver aktivitātes uz valstu robežas, īslaicīgas izlūku vizītes Latvijā, kā arī darbu pret Latvijas valsts piederīgajiem, tiem atrodoties dienestu pārstāvētajās valstīs. Savukārt aktīvo pasākumu īstenošanai nereti tiek izmantoti mediji, virtuālā telpa un sociālie tīkli, kur specdienestu lomu un iesaisti noteikt ir sarežģīti. Specdienestu darba metodes ietver darbu ar informācijas avotiem un kontaktpersonām, informācijas iegūšanu no atklātajiem avotiem, bet arvien lielāka nozīme specdienestu darbā ir tehnisko spēju attīstībai, tajā skaitā darbībām kibertelpā un signālizlūkošanai.

Krievijas specdienestu izlūkošanas prioritāte ir NATO drošības politikas lēmumi un aktivitātes reģionā, Latvijas aizsardzības un militārās spējas, tajā skaitā Nacionālie bruņotie spēki un Valsts Robežsardze, situācija uz NATO ārējās robežas. Krievijas specdienestu intereses skar ne tikai Latvijas aktivitātes NATO ietvaros, bet arī Eiropas Savienībā un citās starptautiskās organizācijās. Arī 2016. gadā konstatēta specdienestu interese par iekšpolitiku, ekonomiku, enerģētikas politiku.

SAB novērojis pastiprinātu izlūkošanas un drošības dienestu interesi par jautājumiem, kas var uzrunāt pretēji noskaņotas sabiedrības grupas valsts iekšienē, vai kļūt par pamatu starpvalstu diskusijām. Piemēram, migrācijas politika, Latvijas nostāja attiecībā uz Lielbritānijas izstāšanos no ES, kā arī ASV prezidenta vēlēšanu iznākums ir bijuši Krievijas specdienestu redzeslokā. Interese par tēmām, kas potenciāli var radīt šķelšanos un konfliktu, sasaucas ar Krievijas īstenoto ārpolitiku, un specdienestu iegūtā informācija var tikt izmantota propagandas un ietekmes pasākumos.

## **Krievijas ietekmes pasākumi un propaganda**

Krievijas īstenoto ietekmes pasākumu mērķis ilgtermiņā ir maksimāli palielināt ģeopolitisko ietekmi reģionā, vienlaikus vājinot NATO un ES, kā arī Baltijas valstu pozīcijas šajās organizācijās. Attiecīgi Latvijā Krievija īsteno informatīvo politiku un propagandu, izmanto ietekmes aģentus un kontrolētas organizācijas, lai pēc iespējas vājinātu Latvijas valsti: veicinātu sabiedrības neuzticību valstij un valdībai, apšaubītu Latvijas ģeopolitisko kursu NATO un ES ietvaros, īstētu Latvijas starptautisko diskreditāciju, veicinātu konflikta potenciālu, uzsverot un saasinot etniskās, lingvistiskās, vēstures izpratnes atšķirības. Vienlaikus ietekmes pasākumu mērķis ir slavēt iespējamus ieguvumus, ja Latvija atbalstītu Kremļa intereses un redzējumu reģionā, un veicināt “krievu pasaules” nostiprināšanos sabiedrībā kopumā vai atsevišķās iedzīvotāju grupās.

Pēdējos gados sabiedrība Baltijas jūras reģionā, kā arī Rietumvalstīs kopumā, ir kļuvusi kritiskāka pret Krievijas propagandu, apmelošanas un diskreditācijas kampaņām, Maskavas vadītu pseidoeskpertu un prokrievisku organizāciju centieniem imitēt pilsoniskas aktivitātes. Virkne Eiropas

valstu un arī ES pēdējā gada laikā ir izveidojušas vai pastiprinājušas pretpasākumus Krievijas informatīvajai ietekmei. Līdz ar to Krievijas ietekmes pasākumi kļūst arvien specifiskāk izstrādāti un mērķēti, ietekmes operācijās arvien lielāka loma ir tieši kontrolētiem ietekmes aģentiem. Krievijas institūcijas turpina darbu arī ar lielākām sabiedrības grupām, piemēram, tautiešiem, tomēr plašu un izplūdušu ietekmes pasākumu efektivitāte nav augsta, un finansējums tam ticis samazināts.

Ņemot vērā informācijas izšķirošo nozīmi visu sociālpolitisko procesu virzībā, Krievijas ietekme Latvijas informatīvajā telpā joprojām veido vienu no būtiskākajiem Latvijas valsts drošības ilgtermiņa apdraudējumiem.

Latvijā retranslētie Kremļa kontrolētie televīzijas kanāli veido galveno pamatu Krievijas informatīvai ietekmei Latvijā. Tomēr, tā kā šo kanālu mērķauditorija ir Krievijas pašmāju sabiedrība, tajos nevar tikt efektīvi izvērstas specifiski Latvijas skatītājiem izstrādātas propagandas kampaņas. Vienlaikus šo mediju lietošana Latvijā veicina Kremlim labvēlīga pasaules redzējuma un vērtību izplatīšanos. Arī atsevišķu Latvijas krievvalodīgo mediju darbība sniedz atbalstu Krievijas propagandai, tajos tiek iekļauts Kremļa kontrolētu mediju veidots saturs un uzturēta agresīva retorika pret Latvijas valsti, kas sasaucas ar Maskavas mērķiem un propagandas vēstījumiem.

2016. gadā turpinājās Krievijas centieni veidot Baltijā papildus informatīvās ietekmes iespējas, kas ļautu Kremlim īstenot vietējai situācijai speciāli pieskaņotas propagandas kampaņas. 2016. gada sākumā darbu uzsāka Krievijas ziņu aģentūras "Rossija Segodņa" projekta "Sputņik" interneta vietnes Latvijas un Igaunijas versijas, 2016. gada nogalē - arī Lietuvas versija. Krievijas kuratoriem nepieciešamo viedokli šajās vietnēs izsaka atlasīti Krievijas, ārvalstu un vietējie eksperti. Dominē negatīva rakstura vai kritiska informācija par Latviju, Baltijas valstīm, ES un NATO un pozitīva – par Krieviju. Tomēr pašlaik "Sputņik" informatīvais produkts Baltijas valstīs nav konkurētspējīgs, tā efektivitāte ir niecīga un sabiedrība to atpazīst kā Krievijas propagandas projektu, tādējādi ierobežojot darbības iespējas.

Līdzīgi kā iepriekšējā gadā arī pērn Krievijas ietekmes aktivitātes informatīvajā telpā galvenokārt bija saistītas ar NATO klātbūtnes palielināšanu Baltijas jūras reģionā. Propagandas uzdevumi attiecībā uz Latvijas (un Baltijas) sabiedrību ir radīt iespaidu, ka nevis Krievijas, bet NATO politika palielina drošības riskus reģionā. Krievijas interesēs ir mazināt Latvijas sabiedrības atbalstu NATO klātbūtnes palielināšanai reģionā, tāpēc Kremļa kontrolētie mediji pēc iespējas negatīvākā gaismā cenšas atspoguļot sabiedroto spēkus, apšaubā Alianses vienotību un gatavību aizsargāt Baltijas valstis. Savukārt Latvijas aizsardzības sistēma un bruņotie spēki tiek rādīti kā neprofesionāli un vāji, cenšoties mazināt sabiedroto atbalstu Baltijai.

Tautiešu politika joprojām ir redzamākais Krievijas ietekmes instruments Latvijā, tomēr ar tā palīdzību Krievija var manipulēt tikai ar atsevišķām personām un organizācijām, nevis vadīt visus Latvijas krievvalodīgos iedzīvotājus. Cieša sadarbība Krievijas tautiešu politiku īstenojošām institūcijām izveidojusies ar nelielu Latvijas krievvalodīgo organizāciju aktīvistu skaitu. Šo personu darbības ietekme uz plašāku politisko procesu Latvijā ir salīdzinoši zema un to politiskā redzamība Latvijas masu medijos izriet galvenokārt no atsevišķām provokatīvām akcijām. Tautiešu organizāciju līderi kā noteiktu vēstījumu nesēji tiek izmantoti Latvijas starptautiskajā diskreditācijā un kā "rietumvalstu eksperti" tiek izmantoti uz Krievijas iekšējo auditoriju mērķētajā propagandā.

Kopumā Krievijas ietekmes iespējas Latvijā nav pietiekamas, lai veiktu masveidīgu, efektīvu un uz tūlītēju rezultātu vērstu kampaņu iekšpolitiskās situācijas destabilizēšanai vai sabiedrības ietekmēšanai.

## Kiberapdraudējums

Ārpus NATO un ES esošo valstu specdienestu, bruņoto spēku kibervienību, kā arī valstu vadītu haktīvistu darbība Rietumvalstīm rada vienu no visstraujāk augošajiem drošības apdraudējumiem. Arī vairāku teroristisku organizāciju darbības kibertelpā arvien biežāk tiek skatītas kā vērā ņemams drauds.

Kibertelpā ir izšķirami vairāki apdraudējumu veidi: spiegošana, informācijas operācijas sabiedrības viedokļa un politiķu ietekmēšanai, kā arī destruktīvas darbības pret informāciju tehnoloģiju (IT) sistēmām vai industriālo infrastruktūru, kuru darbība ir atkarīga no IT. Nereti uzbrukumam var būt vienlaicīgi vairāki mērķi. Piemēram, uzbrukuma mērķis var būt psiholoģiskā ietekmēšana un vienlaicīgi informācijas iegūšana.

Kiberapdraudējums var tikt vērsti gan pret valsts, gan privāto sektoru. Uzbrukumi var tikt veikti no privātiem datoriem un kontiem. Tie var būt vērsti pret interesējošo personu vai arī pret pastarpināti saistītām personām, piemēram, ģimenes locekļiem, ja vien tas ļauj sasniegt pretinieka mērķus.

Kiberspējas dažādu mērķu sasniegšanai attīsta un aktīvi izmanto liela daļa valstu izlūkošanas un drošības dienestu, bet lielāko kiberapdraudējumu Latvijai rada Krievijas kiberspēju pieaugums un gatavība tās pielietot pret Latviju un sabiedrotajiem.


Krievija kiberooperācijas izmanto gan kā atsevišķas aktivitātes, gan arī izvēršot kibernetiskus uzbrukumus kā atbalsta pasākumus cita veida operācijās. Kiberspējas kā nozīmīga hibrīdkara sastāvdaļa tiek izmantotas Krievijas operācijās Ukrainā un Sīrijas konflikta ietvaros.

Krievijas izlūkošanas un drošības dienestu īstenotajiem ietekmes pasākumiem kiberspējas nodrošina nesalīdzināmi plašāku un masveidīgāku vārienu, nekā to ļāva līdz šim pieejamās metodes. Rietumvalstu informatīvajā telpā – interneta medijos un sociālajos tīklos – tiek iepludinātas pilnībā melīgas ziņas, kā arī ziņas un viedokļi, kur sajaukta patiesība un izdomājumi, lai manipulētu un dezorientētu noteiktas sabiedrības grupas Kremlim izdevīgā veidā. Ietekmes pasākumos tiek iesaistīti interneta “troļļi”, kas vēstījumus internetā izplata, kombinējot reālu personu un tehniski automatizētas darbības. Operācijās, kuru mērķis ir ietekmēt iekšpolitisko situāciju, nereti tiek izmantota ar kiberspigošanas metodēm iegūta amatpersonas un politiķus kompromitējoša informācija, kas pasniegta manipulatīvā veidā. Autentiskai informācija var tikt pievienoti viltoti fakti. Informācija tiek publiskota, pieskaņojot īpaši organizētas propagandas kampaņas.

Latvijā 2016. gadā SAB konstatēja vairākus ārvalstu specdienestu vai to vadītu hakeru grupu īstenotus kibernetiskus uzbrukumus, kas bija vērsti gan pret valsts institūcijām un amatpersonām, gan privātām kompānijām un medijiem. Kibernetiskus uzbrukumus mērķiem Latvijā visbiežāk tiek veikti spiegošanas nolūkā. Izplatīts paņēmieni ir pikšķerēšana (spear-phishing), kad uzbrukuma mērķim tiek nosūtīta viltota e-pasta ziņa, kas veidota tā, lai mudinātu saņēmēju atvērt vēstuli, kas savukārt inficē lietotāja datoru un uzbrucējam ļauj iegūt kontroli pār datoru un tajā esošo informāciju. Vēstuļu saturs bieži tiek īpaši izstrādāts, ņemot vērā katras konkrētās mērķa personas intereses un pieskaņojoties aktuālajai situācijai.

Piemēram, salīdzinoši apjomīgs uzbrukums vairākiem adresātiem Latvijas valsts institūcijās tika veikts 2016. gada nogalē, kad vīruss tika maskēts kā Ziemassvētku apsveikums. Skatīt piemēru:

## Merry Christmas!

**From:** Santa <nicolas@santaklausmail.com>  
**To:** xxx@xxx.gov.lv  
**Date:** 2016-12-23 22:59  
**Attachments:**  Merry\_Christmas!.docx

Ho-Ho-Ho, it's almost **Christmas!**

The elves are working very hard in the workshop to make all of the toys. **Mrs. Claus** helps to wrap the presents and we both check our list to make sure that every gift gets loaded onto the sleigh.

**Rudolph** and the other reindeers are getting very excited - they love to ride across the night sky on Christmas Eve. I expect that you have looked out of your window to look for us but, as I can only make deliveries when children are fast asleep, I have to make sure that we keep out of sight!

I hope that you will have a wonderful Christmas and that you will continue to be good next year so that I can come and visit you again.

Here you have your Christmas present in the attachment.

Love from

Santa Claus.

Santa Claus Main Post Office  
FI-96930 Arctic Circle  
FINLAND

Tel. 020 4523 120  
Fax. 016 3481 418

\*\*\*\*\*

**NOTE:** This letter has been delivered via "**Christmas Elves Mailing System**". Please don't open the attachment if you've been bad boy or girl.

\*\*\*\*\*

Viltus e-pasta vēstule var būt veidota tā, lai saņēmējam rastos iespaids, ka to sūtījusi kāda viņam zināma persona, tajā var būt ietvertas atsaucēs uz līdzšinējo sadarbību vai tikšanos. Šādos gadījumos vēstule tiek izsūtīta no adreses, kas satur pazīstamās personas vārdu, bet adreses domēns ir cits. Piemēram, ja parasti sarakste notiek, izmantojot adresi [vards.uzvards@inbox.lv](mailto:vards.uzvards@inbox.lv), viltotā vēstule tiek saņemta no adreses [vards.uzvards@yahoo.com](mailto:vards.uzvards@yahoo.com). Viens no šāda uzbrukuma piemēriem, kad uzbrukums maskēts kā ASV vēstnieces Latvijā e-pasts:

## Letter from Ambassador Nancy Bikoff Pettit to You

**From:** [Ambassador Nancy Bikoff Pettit <mypersonalmails@yahoo.com>](mailto:mypersonalmails@yahoo.com)  
**To:**  
**Reply to:** [Ambassador Nancy Bikoff Pettit <mypersonalmails@yahoo.com>](mailto:mypersonalmails@yahoo.com)

Good Evening,  
What is your mobile phone number?  
Its very urgent that we discuss privately.  
I will call you to arrange a confidential meeting.  
Warm Regards,  
Ambassador Nancy Bikoff Pettit

U.S. Embassy Riga  
1 Samnera Velsa St. (former Remtes)  
Riga LV-1510  
Latvia  
Phone: +371 6710 7000  
Fax: +371 6710 7050  
Email: [Embassy.US.Gov@usa.com](mailto:Embassy.US.Gov@usa.com)

Lai mazinātu drošības riskus, e-pasta lietotājam nav ieteicams atvērt e-pasta vēstules, kas saņemtas no nepazīstama sūtītāja. Ja rodas šaubas par vēstules autentiskumu, svarīgi nespīest uz e-pastā piedāvātām pogām, interneta adresēm un neatvērt pielikumus.

Viltus e-pasti var tikt maskēti arī kā no publisko e-pasta pakalpojumu sniedzējiem (Gmail, Yahoo u.c.) sūtīts paziņojums, piemēram, lūdzot veikt paroles maiņu. Drošības nolūkā jebkāda iestatījuma maiņa ir jāveic pakalpojuma sniedzēja iestatījumu sadaļā, neatverot atsūtītā e-pastā ietvertās aktīvās saites.

## **NATO un ES institūciju klasificētās informācijas aizsardzība**

SAB apakšstruktūra Nacionālā drošības iestāde (NDI) ir atbildīga par NATO un ES klasificētās informācijas aizsardzību. Klasificētās informācijas aizsardzība ir būtisks NATO un ES drošības aspekts un spēja to nodrošināt ir pamats tam, ka Latvija tiek uzskatīta par pilnvērtīgu partneri šajās organizācijās. Klasificētās informācijas aizsardzības pasākumi ir kopums, kas ietver personāla drošību, telpu fizisko drošību, dokumentu aprites drošību, informācijas drošību elektroniskajā vidē un industriālo drošību. NDI funkciju ietvaros SAB ir atbildīgs par visu Latvijas Republikas NATO un ES klasificētās informācijas subjektu kontroli un attiecīgu sertifikāciju. Latvijas Republikas atbilstību NATO un ES klasificētās informācijas aizsardzības standartiem veic atbildīgo NATO un ES drošības struktūru inspekcijas.

2016. gadā SAB veica pārbaudes un izsniedza 1423 sertifikātus pastāvīgam darbam ar NATO klasificēto informāciju un 1650 sertifikātus pastāvīgam darbam ar ES klasificēto informāciju. Piekļuve NATO un ES klasificētajai informācijai atteikta 10 personām.

## **Valsts noslēpuma aizsardzība**

Atbilstoši likuma "Par valsts noslēpumu" noteiktajai kompetencei SAB, līdztekus Drošības policijai un Militārās izlūkošanas un drošības dienestam, veic arī tiešus valsts noslēpuma aizsardzības pasākumus. Valsts noslēpuma aizsardzības jomā SAB veic personu pārbaudes, pirms tām izsniedz speciālo atļauju darbam ar valsts noslēpumu, kā arī pārbauda un sertificē darbā ar klasificētu informāciju izmantotas telpas. SAB veic valsts noslēpuma apstrādei paredzēto informācijas sistēmu akreditāciju.

SAB 2016. gadā sagatavoja un izsniedza 512 speciālās atļaujas darbam ar valsts noslēpumu. Procedūra paredz, ka personai ir tiesības SAB pārsūdzēt pārējo valsts drošības iestāžu (DP un MIDD) pieņemtos lēmumus atteikt pieeju valsts noslēpumam. 2016. gadā 24 gadījumos SAB atļaujas darbam ar valsts noslēpumu izsniegšanu ir atteicis, tajā skaitā izskatot DP un MIDD pieņemtos un birojam pārsūdzētos lēmumus. Kritēriji, pēc kuriem tiek izlemts par speciālās atļaujas darbam ar valsts noslēpumu piešķiršanu vai atteikšanu, ir noteikti likuma "Par valsts noslēpumu" 9. pantā.

SAB direktora lēmums par speciālās atļaujas atteikšanu ir pārsūdzams ģenerālprokuroram. 2016. gadā ģenerālprokuroram iesniegtas 13 pārsūdzības par SAB pieņemto lēmumu atteikt atļauju darbam ar valsts noslēpumu. 12 gadījumos ģenerālprokurors ir atzinis, ka SAB lēmums ir bijis pamatots un atbilstošs likuma prasībām. Vienā gadījumā ģenerālprokurors ir daļēji un uz laiku atcēlis lēmumu, kurš atbilstoši likumā noteiktajai kompetencei pārsūtīts DP tālākai izskatīšanai.

2017. gada 10. februārī Satversmes tiesa ir pasludinājusi spriedumu lietā Nr.2016-06-01 "Par likuma "Par valsts noslēpumu" 11. panta piektās daļas, 13. panta trešās un ceturtais daļas atbilstību Latvijas Republikas Satversmes 92. panta pirmajam teikumam, 96. pantam un 106. panta



pirmajam teikumam”, secinot, ka atsevišķas normas, kas nosaka speciālās atļaujas pieejai valsts noslēpumam anulēšanas kārtību, neatbilst Satversmei un no 2018. gada 1. jūlija zaudēs spēku. Vadoties no Satversmes tiesas sprieduma, ir jārada jauns regulējums, kas noteiks valsts drošības iestāžu lēmumu pārsūdzības kārtību atbilstoši leģitimētā neatkarīgā institūcijā. Jāprecizē normatīvais regulējums un likumā jānosaka noteikti gadījumi, kad pieļaujama atkārtota pretendēšana uz speciālo atļauju, vai termiņš, pēc kura beigām persona var noteiktā procedūrā atkārtoti pretendēt uz speciālo atļauju.

## **Industriālā drošība**

Industriālais drošības sertifikāts (IDS) apliecina komersantu tiesības pildīt valsts pasūtījumus, kuri saistīti ar piekļuvi valsts noslēpuma objektiem, NATO un ES klasificētajai informācijai, kā arī apliecina komersanta spēju nodrošināt šādas informācijas aizsardzību. Saskaņā ar procedūru nepieciešamās pārbaudes industriālā sertifikāta saņemšanai var veikt visas trīs valsts drošības iestādes, savukārt SAB, balstoties uz pārbaudžu materiāliem, pieņem lēmumu par sertifikāta izsniegšanu.

2017. gada sākumā spēkā esoši ir 125 SAB izsniegti IDS darbam ar valsts noslēpuma objektiem un 4 – darbam ar NATO klasificēto informāciju. Pārskata periodā SAB pieņēmis lēmumu atteikt izsniegt IDS 14 komersantiem, 6 gadījumos iepriekš izsniegtais IDS anulēts. Saskaņā ar procedūru SAB direktora pieņemtais lēmums par IDS atteikumu var tikt pārsūdzēts ģenerālprokuroram, kura lēmums ir nepārsūdzams. 2016. gadā SAB lēmums par IDS atteikumu vai anulēšanu pārsūdzēts 10 gadījumos un visos SAB lēmums atstāts negrozīts.

Lai komersants varētu saņemt IDS, ir veiktas uzņēmumu īpašnieku, amatpersonu un darbinieku pārbaudes, un 206 personām izsniegtas speciālās atļaujas darbam ar valsts noslēpuma objektiem, 6 personām izsniegti sertifikāti darbam ar NATO klasificēto informāciju, 2 personām pieeja valsts noslēpumam atteikta.

## **Mobilo telefonu kontroles iekārtas darbība**

SAB atrodas iekārta, ar kuru tiesībsargājošās un valsts drošības iestādes veic mobilo telefonu kontroli. Telefonu kontroles rezultātā iegūtie dati tiek nodoti operatīvās darbības subjektam, kas ir konkrēto telefonsarunu pārtveršanas iniciators un saņēmis Augstākās tiesas tiesneša sankciju. SAB kompetences un atbildības jomā ietilpst likumīga telefonsarunu kontrole, telefonsarunu kontroles tehnisko parametru un metodikas aizsardzība un iegūtās informācijas aizsardzība pret nesankcionētu izpaušanu līdz tās nodošanai operatīvās darbības subjektam.

Pirms telefona kontroles uzsākšanas SAB saņem operatīvās darbības subjekta lēmuma daļu, kurā norādīts:

- lēmuma reģistrācijas numurs;
- amatpersona, kura pieņēmusi lēmumu;
- iestādes vadītājs, kas to apstiprinājis;
- Augstākās tiesas tiesnesis, kas to sankcionējis;
- kontrolējamais telefona numurs;
- termiņš, līdz kādam kontrole veicama.

Uzraudzību pār sarunu operatīvās noklausīšanās atbilstību likumam veic ģenerālprokurors un viņa īpaši pilnvaroti prokurori. Parlamentāro kontroli realizē Saeimas Nacionālās drošības komisija.

2016. gadā, tāpat kā iepriekšējos gados, SAB nav pieļāvis likumpārkāpumus, nodrošinot mobilo telefonu kontroli. Mobilo telefonu kontroles izmantošanas sadalījums starp operatīvās darbības subjektiem ir redzams attēlā:

