Valsts, civilā un vides aizsardzība

juris.porozovs@lu.lv

Valsts aizsardzība

Mūsdienu drošības situācijas un Latvijas apdraudējuma raksturojums

Apdraudējums informācijas telpā, kibervidē, hibrīdapdraudējuma dažādas izpausmes formas

Literatūra

- Jemeļjanovs, V., Sulojeva, J. (2012). Civilā aizsardzība. Rīga: «RTU».
- Kusiņš, J., Kļava, G. (2011). Civilā aizsardzība. Rīga: «Drukātava».
- Kļaviņš, M. (2009). Vides piesārņojums un tā iedarbība. R.: LU Akadēmiskais apgāds.
- Kļaviņš, M., Nikodemus, O., Segliņš, V., Melecis, V., Vircavs, M., Āboliņa, K. (2008). Vides zinātne. R.: Latvijas Universitāte.
- Vide un ilgtspējīga attīstība. (2010). M. Kļaviņa un J. Zaļokšņa redakcijā. R.: LU Akadēmiskais apgāds.
- VIDES POLITIKAS PAMATNOSTĀDNES 2021.–2027. gadam.

Literatūra

- Valsts apdraudējums un tā novēršanas, samazināšanas vai seku likvidēšanas principi https://www.lai.lv/viedokli/valsts-apdraudejums-un-ta-noversanas-samazinasanas-vai-seku-likvidesanas-principi-373
- Jundzis, T. (1998). Cik maksā valsts aizsardzība? Rīga: «Junda».
- Jundzis, T. (1995). Latvijas drošība un aizsardzība. Rīga: «Junda».
- Kalniņa, A. (2005). Cilvēkdrošība Latvijā: Apdraudējumi un drošības avoti. Promocijas darba kopsavilkums. Rīga.

Literatūra

- LR Nacionālais drošības likums
- https://likumi.lv/ta/id/14011-nacionalas-drosibas-likums
- LR Civilās aizsardzības un katastrofu pārvaldīšanas likums
- https://likumi.lv/ta/id/282333-civilas-aizsardzibas-un-katastrofas-parvaldisanas-likums;
- LR likums "Par ārkārtējo situāciju un izņēmuma stāvokli" https://likumi.lv/ta/id/255713-par-arkartejo-situaciju-un-iznemuma-stavokli
- LR likums "Par radiācijas drošību un kodoldrošību" https://likumi.lv/ta/id/12484-par-radiacijas-drosibu-un-kodoldrosibu
- LR Ugunsdrošības un ugunsdzēsības likums https://likumi.lv/doc.php?id=68293

Patstāvīgo darbu tēmas kursam „Valsts, civilā un vides aizsardzība”

- Drošība valstī, iespējamiem apdraudējumi un riski, kas saistīti ar valsts drošību.
- Latvijas apdraudējuma raksturojums.
- Apdraudējums informācijas telpā un kibervidē.
- Hibrīdkarš, tā īpatnības.
- Bruņoti konflikti, to raksturojums.
- Latvijas aizsardzības un drošības politika.
- Iestāžu, amatpersonu un iedzīvotāju tiesības un pienākumi valsts aizsardzības ietvaros.
- Iedzīvotāju psiholoģiskā aizsardzība.
- Masu iznīcināšanas ieroči, to raksturojums.
- Valsts civilās aizsardzības struktūra, valsts iestāžu un pašvaldību uzdevumi civilajā aizsardzībā.
- Civilās aizsardzības pasākumu plānošana.
- Apdraudējuma riska novērtēšana.
- Civilās trauksmes un apziņošanas sistēma.
- Starptautiskās palīdzības lūgšana un sniegšana.
- Katastrofu medicīnas sistēma Latvijā.
- Psiholoģiskās palīdzības sniegšana katastrofās cietušajiem.
- Paaugstinātas bīstamības objekti, tā īpašnieka vai tiesiskā valdītāja pienākumi un tiesības.
- Bīstamās vielas, to klasifikācija. Prasības bīstamo vielu glabāšanai. Bīstamo kravu pārvadāšana.
- Valstī iespējamās dabas katastrofas un to sekas.
- Valstī iespējamās tehnogēnās katastrofas un to sekas.

Patstāvīgo darbu tēmas kursam „Valsts, civilā un vides aizsardzība”

- Preventīvie, gatavības, reaģēšanas, seku likvidēšanas un atjaunošanas pasākumi katastrofās.
- Individuālie aizsardzības līdzekļi, to pielietošana katastrofas gadījumā.
- Sabiedriskās nekārtības, to cēloņi, ierobežošana un seku likvidēšana.
- Terorisms, tā veidi un iespējamās sekas. Cīņa ar terorismu.
- Globālās vides problēmas.
- Klimata pārmaiņas un to samazināšana.
- Dabas resursi un to izmantošana.
- Vides piesārņojums.
- Vides piesārņojuma samazināšanas metodes.
- Atkritumu pārvaldība.
- Piesārņojošo vielu ietekme uz ekosistēmām.
- Toksisko vielu iedarbība uz cilvēka veselību.
- Vides monitorings.
- Urbanizācijas ietekme uz vidi.
- Bioloģiskās daudzveidības saglabāšana Latvijā.
- Ilgtspējīgas attīstības principi.
- Izglītība ilgtspējīgai attīstībai.
- Vides politikas principi un sistēma.
- Vides politika Eiropas Savienībā.
- Vides politika Latvijā.

Vērtēšanas kritēriji

- Darba saturs ir atbilstošs izvēlētajai tēmai
- Analizēti izvēlētās tēmas jautājumi
- Ir veikti apkopojoši secinājumi, kopsavilkums vai izteikts darba autoru viedoklis
- Ir izveidots izmantotās literatūras saraksts
- Spēja skaidri un uzskatāmi skaidrot prezentācijas materiālu
- Spēja atbildēt uz jautājumiem

Valsts, civilā un vides aizsardzība

- **Valsts aizsardzība**
- **Civilā aizsardzība**
- **Vides aizsardzība**
- nozīmīgi faktori mūsu valsts iedzīvotājiem un valstij kopumā, lai spētu nodrošināt savu eksistenci un valsts neatkarību, ekonomisko uzplaukumu.

Valsts aizsardzība

- Mūsdienu pasaulē robeža starp mieru un karu kļūst aizvien nenoteiktāka, jo **politisko un militāro mērķu sasniegšanai tiek izmantots integrēts militāro un nemilitāro paņēmienu lietojums**.
- Lai varētu efektīvi risināt mūsdienu drošības problēmas, ir nepieciešama **visaptveroša pieeja valsts aizsardzībai**, kas paredz visas sabiedrības iesaisti, kā arī kompleksu skatījumu uz jomām, kuras ir kritiski svarīgas sabiedrības funkcionalitātes nodrošināšanai ilgtermiņā un krīzes situācijās.
- **Visaptveroša valsts aizsardzības koncepcija** pārsniedz aizsardzības sektora robežas un prasa visas valdības, pašvaldību, uzņēmēju, nevalstisko organizāciju un citu struktūru saskaņotu darbību kopējam mērķim.

Valsts aizsardzība

- Visaptverošu valsts aizsardzību veido daudzi elementi, kurus var strukturēt četrās dimensijās: **militārajā; civilajā; informācijas un psiholoģiskajā**.
- Latvijas **militārā aizsardzība** balstās **Nacionālo bruņoto spēku (NBS**) spējā nodrošināt Latvijas neatkarību, teritoriālo nedalāmību un suverenitāti ar militārajiem līdzekļiem bruņota konflikta gadījumā.
- **Civilās aizsardzības sistēma** ir nacionālās drošības sistēmas sastāvdaļa, kas ir pamats efektīvai un visaptverošai valsts aizsardzības sistēmas funkcionēšanai, nodrošinot civilo un militāro institūciju savstarpēju koordināciju, resursu koordinēšanu un spēju harmonizāciju.

Valsts aizsardzības koncepcijas projektā norādīts, ka valsts bruņotie spēki spēs bez citu valsts palīdzības pretoties pat iebrucējiem ar skaitlisko pārsvaru

Valsts aizsardzība

- Liela nozīme ir **informācijas videi** un pasākumiem, izplatot Latvijā vienotu vēstījumu par valsts nākotni un kopīgiem mērķiem.
- Nodrošinot Latvijas **sabiedrības psiholoģisko aizsardzību,** jādomā par Latvijas iedzīvotāju noturību pret negatīvām informācijas kampaņām un psiholoģiskajām operācijām pret valsti, vispārējo lietu stāvokli valstī, atsevišķiem notikumiem utt.
- Psiholoģisko aizsardzību vairo **vienota sabiedrība** – tā spēj mazināt iekšējo konfliktu iespējamību valstī.
- Sabiedrība, kuru vieno piederība savai valstij, nevis konkrētai etniskajai grupai, spēj nepakļauties provokācijām un vairāk fokusēties visas valsts aizsardzībai, neļaujoties pretnostatījumam starp nacionalitātēm.

Globālie konflikti

- Pasaulē ir vismaz kādas septiņas vai astoņas lielas civilizācijas, kuras vieno kopīgas kultūras vērtības un intereses. Viens no civilizāciju raksturojošiem elementiem ir reliģija, nozīmīgas ir arī kultūras tradīcijas, valoda u.c.
- Par tādām varētu uzskatīt Ķīnas, Japānas, Indijas, islāma, rietumu (Rietumeiropas, Ziemeļamerikas, arī Austrālijas un Jaunzēlandes), ortodoksālās pareizticības (kas centrējas Krievijā), latīņamerikas, iespējams, Āfrikas civilizāciju (Semjuels Hantigtons «Civilizāciju sadursme»).
- Vēsturiski raugoties, rietumu civilizācija ir Eiropas civilizācija, tomēr 20. gs. Amerika ir pieteikusi sevi kā plašākas identitātes «Rietumu» līderi.
- Pēdējos gadu desmitos rietumu civilizācijas globālā ietekme ir mazinājusies.
- Konfliktiem starp civilizācijām var būt dažādas formas.
- **Lokālajā jeb mikrolīmenī** tie parādās starp kaimiņvalstīm no divām civilizācijām, starp grupām no civilizācijām valsts iekšienē.
- Lokālie konflikti, kas izvēršas plašākos karos, lielākoties ir kari starp atšķirīgu civilizāciju valstīm un grupām.

Globālie konflikti

- **Globālajā jeb makrolīmenī** vadošo valstu konflikti notiek starp dažādo civilizāciju lielākajām valstīm.
- Šo konfliktu tēmas ir klasiskas starptautiskajā politikā, piemēram:
- **Relatīvo globālo organizāciju**, piemēram, ANO, SVF un Pasaules Banka, NATO, **darbība un ietekme uz globālajiem procesiem**.
- **Relatīvais militārais potenciāls**, domstarpības jautājumos par ieroču izplatīšanu un bruņojuma kontroli, kā arī bruņošanās sacensību.
- **Domstarpības ekonomikas jautājumos**, kas atklājas strīdos par tirdzniecību, investīcijām un citiem jautājumiem.
- **Vērtības un kultūra**, kas izraisa konfliktus, ja valsts mēģina veicināt vai uzspiest savas vērtības citas civilizācijas cilvēkiem.
- Dažreiz **teritorijas**, kad vadošā valsts kļūst par līdzdalībniecēm lūzuma līniju konfliktos.

- Konflikti notiek arī civilizāciju iekšienē (īpaši islāmā, piemēram starp šiītiem un sunnītiem).

Globālie konflikti

- Daudzas valstis ir heterogēnas – tās ietver divas vai vairākas etniskās, rasu un reliģiskās grupas.
- Ir valstis, kas ir sašķeltas, jo to politikā liela nozīme ir atšķirībām un konfliktiem starp iedzīvotāju grupām.
- Dziļa šķelšanās var izraisīt vardarbību vai apdraudēt valsts pastāvēšanu.
- Piemēram, Sudānā desmitiem gadu ilga pilsoņu karš starp musulmaņiem ziemeļos un lielākoties kristiešiem dienvidos.
- Padomju Savienības laikā Krievija bija atšķirīga no rietumiem, bet tomēr arī veidoja saikni ar rietumiem. Lai gan komunistiskā ideoloģija un liberālā demokrātija būtiski atšķīrās, abas puses tomēr runāja savā starpā.
- V. Putina valdīšanas laikā Krievijā sāka dominēt nacionālistiskas intereses.
- Krievijas agresija Ukrainā ir satricinājusi Eiropas drošību un globālo starptautisko kārtību.
- Krievijas rīcība ir likusi visām Eiropas valstīm pārvērtēt attieksmi pret drošību.

Valsts apdraudējums un tā novēršana

- **Draudi Latvijas nacionālajai drošībai** ir saistīti ar Krievijas militārajām aktivitātēm Latvijas robežu tuvumā un citur, situācijas attīstību starptautiskajā drošības vidē, kā arī ļaunprātīgām kiberaktivitātēm un starptautiskā terorisma tendencēm.
- Jau ilgstoši, bet it īpaši kopš 2014. gada Krievijas iebrukuma Ukrainā un Krimas aneksijas drošības situāciju Baltijas jūras reģionā ietekmē Krievijas agresīvās militārās un hibrīdās aktivitātes.
- Krievija 2022. gada 24. februāra rītā pēc Krievijas prezidenta Vladimira Putina pavēles uzsāka iebrukumu Ukrainā jeb Krievijas—Ukrainas kara plaša mēroga militāra operācija, ko veica Krievijas Bruņotie spēki.
- Operāciju ievadīja Krievijas Bruņoto spēku atklāta ievešana pašpasludināto Doņeckas un Luhanskas tautas republiku teritorijā 2022. gada 21. februārī un to neatkarības atzīšana visa Doņeckas un Luhanskas apgabala robežās 2022. gada 22. februārī.

Karš Ukrainā

- Ukrainas bruņotie spēki un iedzīvotāji sīvi pretojās iebrucējiem.
- Krievijas uzbrukums Ukrainai izraisījis vispārēju starptautiskās sabiedrības nosodījumu.
- Pret Krieviju daudzas pasaules un Eiropas valstis ieviesa arvien jaunas sankcijas.

Karš Ukrainā

- Krievijai zibenskarš neizdevās, ukraiņi stāvēja stingrāk nekā daudziem tas šķita iespējams.
- Sākās sarunas starp Krievijas un Ukrainas delegācijām, bet tās nedeva rezultātus.
- 2023. gada 24. februārī apritēja gads, kopš pilna mēroga kara sākuma Ukrainā.

Bruņots konflikts

- **Militārs (bruņots) konflikts** ir bruņota, organizēta, bieži iepriekš plānota sadursme, kas radusies dažādu nesaskaņu rezultātā.
- Bruņotu konfliktu iemesli:
- Politiskās un etniskās problēmas.
- Stratēģiski, ar teritoriju saistīti iemesli.
- Ekonomiskās nesaskaņas.
- Reliģiskās problēmas.
- Sociālās problēmas.
- Ideoloģiskas nesaskaņas.

Ženēvas konvencijas

- **Ženēvas konvencijas** ir četri miera līgumi ar trim papildprotokoliem, kas nosaka starptautisko tiesību standartu humanitārai attieksmei pret kara upuriem.
- Termins izmantots vienskaitlī (*Ženēvas konvencija*) pārsvarā norāda uz nolīgumiem, kas tika parakstīti pēc Otrā pasaules kara 1949. gadā, kad tika papildināti pirmie trīs miera līgumi un pievienots ceturtais.
- Valstu valdību pilnvarotie pārstāvji, piedalījās diplomātiskajā konferencē, kas notika Ženēvā no 1949.gada 21.aprīļa līdz 12.augustam ar nolūku radīt Konvenciju par civilpersonu aizsardzību kara laikā.

Ženēvas konvencijas

- Pirmā Ženēvas konvencija — “Par ievainoto un slimo stāvokļa uzlabošanu karojošajās armijās” (1864)
- Otrā Ženēvas konvencija — “Par ievainoto un slimo kā arī jūras kara flotes kuģu katastrofās cietušo stāvokļa uzlabošanu” (1906)
- Trešā Ženēvas konvencija — “Par izturēšanos pret karagūstekņiem” (1929)
- Ceturtā Ženēvas konvencija — “Par civiliedzīvotāju aizsardzību kara laikā” (1949)
- 1. papildprotokols — “Par cietušo aizsardzību starptautiskajos bruņotajos konfliktos” (1977)
- 2. papildprotokols — “Par cietušo aizsardzību nestarptautiskajos bruņotajos konfliktos” (1977)
- 3. papildprotokols — “Par papildu atšķirības emblēmu apstiprināšanu” (2005)

Kara noziegums

- **Kara** noziegumi ir starptautiskajās tiesībās definēti karošanas likumu pārkāpumi.
- Tie ir nopietni Ženēvas Konvenciju 3. panta pārkāpumi, kā arī citu normu, kas aizstāv bruņoto konfliktu upurus, un pamatnormas, kas regulē karadarbības metodes, pārkāpumi.
- Kara noziegumi ir piemēram:
- Padevušos kaujinieku nogalināšana.
- Miera karoga ļaunprātīga izmantošana.
- Ķīmisko un gāzu ieroču izmantošana.
- Kara noziegumu ir sodāmi. Lai saņemtu krimināLsodu, jebkurš kara nozieguma gadījums ir jāiesniedz Starptautiskajā Krimināltiesā.
- Piemēram, Hāgā bāzētais Kara noziegumu tribunāls bijušās Dienvidslāvijas jautājumos piesprieda 22 gadus cietumā Bosnijas serbiem: bijušajam iekšlietu ministram Miko Staņišičam un Stojanam Župļaņinam.

Valsts apdraudējums un tā novēršana

- **Drošības vides izmaiņu rezultātā Latvija kopā ar sabiedrotajiem pievērš pastiprinātu uzmanību drošības politikai un aizsardzības spēju stiprināšanai** kā nacionālajā, tā arī starptautiskajā līmenī.
- Latvijas skatījumā efektīvas atturēšanas politikas sastāvdaļa ir sabiedroto militārā klātbūtne Latvijā.
- Latvijas dalībai NATO ir svarīga nozīme valsts aizsardzības stiprināšanā un nodrošināšanā. Vienlaikus būtisks ir arī Latvijas ieguldījums visas alianses kolektīvajā aizsardzībā. Latvija piedalās NATO operācijās, nodrošina uzņemošās valsts atbalstu sabiedroto karavīriem Latvijā, kā arī iegulda aizsardzībā 2% no IKP.
- 2022. gada 1. janvārī stājoties spēkā likumam "Par valsts budžetu 2022. gadam", aizsardzības nozarei paredz piešķirt ne mazāk kā divus procentus no iekšzemes kopprodukta.
- **2023.gadā aizsardzības budžets tiek plānots 2.07% no IKP un paredzēts to palielināt līdz 2.5% no IKP 2025. gadā.**

Valsts apdraudējums un tā novēršana

- Ziemeļatlantijas līguma (NATO) 5.pants nosaka: **puses vienojas, ka bruņotu uzbrukumu vienai vai vairākām no tām Eiropā vai Ziemeļamerikā uzskatīs par uzbrukumu visām dalībvalstīm.**
- Piebilde: **līguma dalībvalstis šāda uzbrukuma gadījumā veic "pasākumus, kurus tās uzskata par nepieciešamiem, ieskaitot bruņota spēka pielietošanu, lai atjaunotu un saglabātu Ziemeļatlantijas reģiona drošību".**
- NATO ir dibināta kā militāra kolektīvās aizsardzības organizācija, un savstarpējā palīdzība starp tās dalībvalstīm ir militāra.
- Militārās palīdzības apjoms un veids var būt atkarīgs no konkrētās situācijas.

Nacionālās drošības koncepcija

- **Nacionālā drošība** ir valsts un sabiedrības īstenotu vienotu, mērķtiecīgu pasākumu rezultātā sasniegts stāvoklis, kurā ir garantēta valsts neatkarība, tās konstitucionālā iekārta un teritoriālā integritāte, sabiedrības brīvas attīstības perspektīva, labklājība un stabilitāte.
- Nacionālās drošības garantēšana ir valsts pamatpienākums (Nacionālais drošības likums, 2001) .
- https://likumi.lv/ta/id/14011-nacionalas-drosibas-likums
- **Nacionālās drošības sistēmu** veido valsts varu un pārvaldi realizējošās institūcijas un Latvijas pilsoņi, kam likums deleģē pienākumus un tiesības nacionālās drošības jomā noteiktas kompetences ietvaros

Valsts aizsardzība

- **Valsts nacionālā drošības plānošana** sākas ar **valsts apdraudējuma (risku) analīzi**, izvērtējot galvenos iespējamos draudus.
- **Valsts apdraudējuma analīze** ir visaptverošs izvērtējums, kura rezultātā tiek noteikti esošie un potenciālie specifiskie nacionālās drošības apdraudējumi vai riska faktori.
- Valsts apdraudējuma analīzi:
- 1) izstrādā Satversmes aizsardzības birojs sadarbībā ar Valsts drošības dienestu un Militārās izlūkošanas un drošības dienestu ne retāk kā reizi četros gados;
- 2) saskaņo Valsts drošības iestāžu padome;
- 3) izskata Ministru kabinets un Nacionālās drošības padome.

Valsts aizsardzība

- Uz valsts apdraudējuma analīzes pamata Saeima pieņem **Nacionālās drošības koncepciju**, kas deklarē nacionālās intereses un nosaka konkrētu darbību valsts institūcijās.
- **Nacionālās drošības koncepcija** ir uz Valsts apdraudējuma analīzes pamata sagatavots dokuments, kurā noteikti **valsts apdraudējuma novēršanas stratēģiskie pamatprincipi un prioritātes**, kas jāņem vērā, izstrādājot jaunus politikas plānošanas dokumentus, tiesību aktus un rīcības plānus nacionālās drošības jomā.

Nacionālās drošības koncepcija

- **Nacionālās drošības koncepcijā** atbilstoši katrai apdraudējuma jomai tiek noteiktas vispārējās prioritātes šo apdraudējumu novēršanai.
- Nacionālās drošības likums nosaka, ka Nacionālās drošības koncepcijas izpilde ir **obligāta visām valsts institūcijām.**
- Saskaņā ar Nacionālās drošības likumu **Aizsardzības ministrija sagatavo Valsts aizsardzības koncepciju.**
- **Valsts aizsardzības koncepcija** ir uz Militāro draudu analīzes pamata sagatavots dokuments, kurā noteikti **valsts militārās aizsardzības stratēģiskie pamatprincipi, prioritātes un pasākumi** miera, valsts apdraudējuma un kara laikā.
- Valsts aizsardzība tiek plānota ņemot vērā Ziemeļatlantijas līguma organizācijas (NATO), kolektīvās aizsardzības politiskās garantijas un militārās aizsardzības plānus.

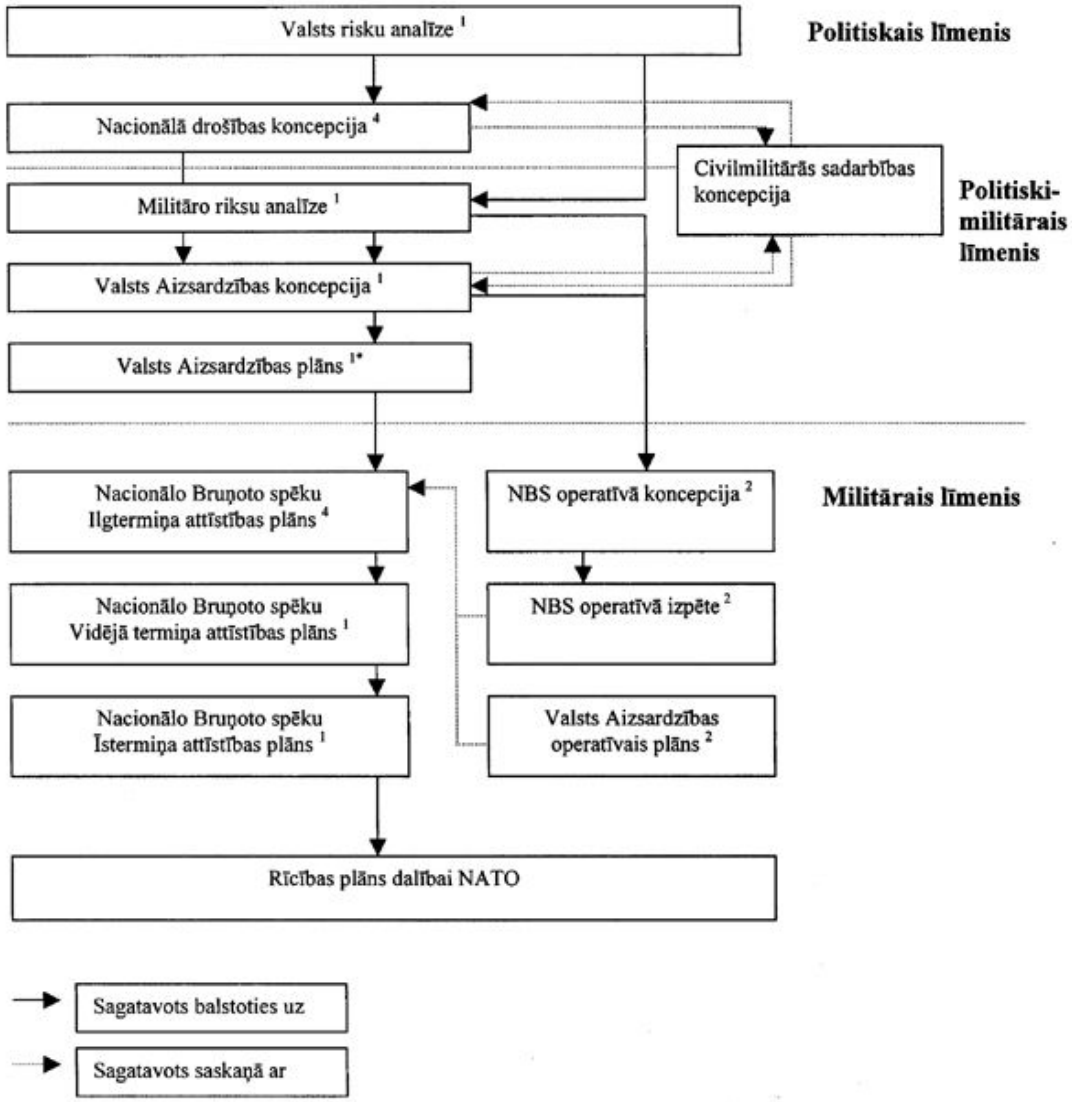
Valsts aizsardzības koncepcija

- Ministru kabinets, balstoties uz **Nacionālās drošības koncepcijā** noteiktajām prioritātēm un **Valsts aizsardzības koncepciju**, izstrādā **Valsts aizsardzības plānu**, kurā ietverti konkrēti valsts apdraudējuma neitralizācijas un novēršanas pasākumi un līdzekļi.
- **Valsts aizsardzības plānu** izstrādā, pamatojoties uz **Militāro draudu analīzi** un **Valsts aizsardzības koncepcijā** noteiktajiem principiem.
- **Militāro draudu analīze** ir pret Latviju vērsta militāra iebrukuma iespējamības izvērtējums, kurā tiek noteikti esošie un potenciālie apdraudējumi un riska faktori, kā arī to iespējamā izpausme un ietekme.

Valsts aizsardzības koncepcija

- **Valsts aizsardzības plāns** balstās uz Nacionālās drošības koncepcijā noteikto stratēģiju un principiem.
- **Valsts aizsardzības operatīvais plāns** ietver operatīvās situācijas izvērtējumu, Nacionālo bruņoto spēku operatīvās kaujas gatavības izvērtējumu un darbības plānu.
- **Nacionālo bruņoto spēku attīstības plānu**, ievērojot militārās plānošanas procedūras, izstrādā Aizsardzības ministrija, pamatojoties uz Valsts aizsardzības koncepciju, Valsts aizsardzības operatīvo plānu un Nacionālo bruņoto spēku komandiera priekšlikumiem.
- Nacionālo bruņoto spēku attīstības plānu veido ilgtermiņā (līdz 12 gadiem), vidējā termiņā (uz četriem gadiem) un īstermiņā.
- **Nacionālo bruņoto spēku mobilizācijas plānu** sagatavo izņēmuma stāvokļa vai kara laika gadījumam.

Ar Aizsardzības ministrijas kompetenci saistīto svarīgāko plānošanas un konceptuālo dokumentu hierarhiskā struktūra



[1] – precizē un apstiprina vienu reizi gadā;
[2] – precizē un apstiprina vienu reizi divos gados;
[4] – precizē un apstiprina vienu reizi četros gados;
[1*] – precizē un apstiprina vienu reizi gadā ja izraisītas radikālas pārmaiņas

Valsts apdraudējums un tā novēršana

- **Būtiskākais apdraudējuma novēršanas stratēģiskais pamatprincips** Nacionālās drošības koncepcijā ir:
- novērst militāro apdraudējumu,
- ārvalstu izlūkošanas un drošības dienestu radīto apdraudējumu,
- kiberapdraudējumu,
- iekšējai drošībai un konstitucionālajai iekārtai radīto apdraudējumu,
- Latvijas informatīvajai telpai radīto apdraudējumu,
- Latvijas ekonomikai radīto apdraudējumu,
- starptautiskā terorisma radīto apdraudējumu.

Valsts apdraudējuma pārvarēšana

- Atkarībā no valsts apdraudējuma veida, tā intensitātes un rakstura, kā arī apdraudētās teritorijas lieluma nosaka atbilstošu terorisma draudu līmeni, kā arī likumā noteiktajā kārtībā var izsludināt **ārkārtējo situāciju vai izņēmuma stāvokli**.
- Ārkārtējās situācijas un izņēmuma stāvokļa gadījumā var izsludināt mobilizāciju, lai risinātu ar nacionālo drošību un valsts aizsardzību saistītos uzdevumus, kā arī likvidētu ārkārtējās situācijas un to sekas.
- **Kara laiks** iestājas, ja ārējs ienaidnieks ir izdarījis militāru iebrukumu vai citādi vērsies pret valsts neatkarību, tās konstitucionālo iekārtu vai teritoriālo integritāti.

Valsts apdraudējuma analīze

- Pirmais jautājums valsts apdraudējuma analīzē ir**: kas ir kādas nedraudzīgas kaimiņvalsts mērķis - panākt ierobežotu mērķi vai pilnu valsts pārņemšanu.**
- Viena šādas analīzes svarīga sastāvdaļa ir jautājums par apdraudētās valsts ekonomisko suverenitāti – vai nedraudzīgā kaimiņvalsts jau kontrolē valsts stratēģisko infrastruktūru – ostas, dzelzceļu, bankas, lidostu, lielos ekonomiskos uzņēmumus.
- Analīzē iekļauj arī izvērtējumu par valstij nedraudzīgu organizāciju mērķiem, plāniem, spējām un vadību.
- Pastāv jautājums, vai NATO, aizstāvot apdraudētas valsts neatkarību, spēj to veikt ierobežojot savu militāro darbību tikai apdraudētās valsts teritorijā un kādas varētu būt militārās, politiskas, un ekonomiskas sekas, ja tā pārplūst uz nedraudzīgās valsts vai citas NATO valsts teritoriju.

Valsts apdraudējuma novēršanas preventīvie pasākumi un nepieciešamā darbība

- Apdraudētai valstij ir jāizstrādā **vienots darbības plāns ar skaidri noteiktām atbildībām, lai apdraudējumu novērstu, samazinātu vai likvidētu tā sekas.**
- Preventīvajos pasākumos iekļaujas **visu starptautisko līgumu izpēte**, policijas speciāla apmācība demonstrantu kontrolē.
- Pārvietojamu slepenu sakaru tīklu izveidošana, plāni iespējamai valdības dislokācijai, plāni Saeimas locekļu sanāksmei, ja demonstranti okupējuši Saeimu.
- Nepieciešamas arī visaugstāko valsts amatpersonu mācības.

Valsts apdraudējuma novēršanas preventīvie pasākumi un nepieciešamā darbība

- Militāro draudu novēršanā liela lomau var būt gudras aizsardzības sistēmas izveidošanai.
- Nepieciešams izveidot tādu aizsardzības sistēmu, kur uzbrukums par daudz politiski, ekonomiski un morāli maksātu agresoram.
- Bruņotiem spēkiem jāveic ļoti precīza analīze, **cik ilgi paietu pirms, piemēram, NATO bruņotie spēki spētu reāli piedalīties valsts aizsardzībā un tad jāplāno, kā nepieļaut valsts militāro pārņemšanu līdz tam brīdim.**
- Valstij arī ļoti rūpīgi jāizlemj par izņēmuma stāvokļa vai kara pasludināšanu.

Latvijas prioritātes ES drošības un aizsardzības sadarbībā

- Latvija atbalsta ciešāku un koordinētāku **Eiropas Savienības (ES) drošības un aizsardzības sadarbību**, jo mūsu interesēs ir vienotāka, drošības un aizsardzības jomā spējīgāka Eiropa.
- Latvijai īpaši svarīga ir **ES militāro un civilo spēju attīstīšana, ES un tās partnervalstu noturības veicināšana pret hibrīdo apdraudējumu, stratēģiskās komunikācijas spēju stiprināšana, kiberdrošības stiprināšana, kā arī civilo spēju attīstība.**
- Latvijai būtiska ir **ES un NATO ciešākas sadarbības veicināšanā** gan politiskā, gan operacionālā līmenī, abām organizācijām papildinot vienai otras spējas.
- Latvija iestājas **par transatlantisko saišu stiprināšanu un ciešāku sadarbību drošības un aizsardzības jomā starp ES un NATO valstīm**, īpaši ASV, Kanādu un Apvienoto Karalisti.

Nacionālās drošības koncepcija

- **Latvijas nacionālajai drošībai** ir **militārā, ārpolitiskā un iekšējās drošības dimensija**, kas ir savstarpēji saistītas.
- **Militāro dimensiju** raksturo Krievijas militārās aktivitātes Baltijas reģionā un pret Latviju vērstie arī citi militārie un hibrīda rakstura drošības riski un apdraudējumi.
- **Ārpolitisko dimensiju** raksturo pašreizējā starptautiskā drošības vide, izmaiņas tajā un ārējie draudi.
- **Iekšējās drošības** dimensiju raksturo Latvijas Republikas Satversmē noteikto pamatvērtību nodrošināšana no valsts puses. Iekšējās drošības pamatā ir saliedēta pilsoniskā sabiedrība ar vienotu izpratni par pamatvērtībām un vēlmi redzēt Latviju kā neatkarīgu, demokrātisku, tiesisku un Rietumu pasaulei piederīgu valsti.
- Jo stiprāka Latvija būs iekšpolitiski, jo efektīvāk tā spēs reaģēt un mazināt ievainojamību no ārējiem apdraudējuma faktoriem.

Informācijas drošība

- Informācijas drošību Latvijā **regulē Informācijas tehnoloģiju drošības likums.**
- https://likumi.lv/ta/id/220962-informacijas-tehnologiju-drosibas-likums
- Lai raksturotu i**nformācijas drošības** saturu, par standarta modeli bieži tiek izmantots konfidencialitātes, integritātes, pieejamības modelis:
- **Konfidencialitāte** – informācijas pieejamība tikai noteiktai lietotāju grupai (sankcionētiem lietotājiem);
- **Integritāte** – informācijas nemainīguma nodrošināšana (nesankcionētas informācijas modifikācijas nepieļaujamība);
- **Pieejamība** – piekļuve informācijai definētajā laikā un apjomā.

Informācijas drošība

- Ar **informācijas drošību** saprot tādu pasākumu kopumu, kas īstenots ar mērķi nodrošināt datu aizsardzību pret nesankcionētu piekļuvi un izmaiņām, glabājot vai pārsūtot datus no vienas vietas uz citu.
- Informācijas tehnoloģiju drošības incidents ir kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte.

Informācijas drošība

- Informācijas drošību dala virzienos:
- **organizatoriskais virziens** – informācijas sistēmu izmantošanas organizācija iestādēs vai uzņēmumos, personāla un lietotāju apmācība, vadība un uzraudzība;
- **tehniskais virziens** – (tehniskā drošība) tehnisko iekārtu, aparatūras un tīklu nepārtrauktas darbības nodrošināšana, bojājumpiecietības uzlabošana, informācijas nesēju uzglabāšana un saudzēšana;
- **tehnoloģiskais virziens** – (informācijas tehnoloģiju un informācijas sistēmu drošība) visa veida programmatūras un informācijas sistēmu konfidencialitātes, integritātes un pieejamības nodrošināšana un dažāda veida ievainojamību identificēšana un novēršana.

Informācijas drošība

- **Organizatoriska rakstura apdraudējumi:**
- **informācijas sistēmu personāla pārstāvju brīvprātīga vai piespiedu atteikšanās no lojalitātes** (nodevība) politiskas pārliecības, materiālas ieinteresētības vai citu faktoru rezultātā;
- **ļaunprātīga uzticības izmantošana** jeb sociālā inženierija, kas tiek izmantota, lai cilvēki labprātīgi atklātu viņiem uzticētu svarīgu informāciju, piemēram, lietotāja vārdus un paroles sistēmās, personas datus un citu sensitīvu informāciju. Datortīklos plaši izmanto sociālās inženierijas metodi pikšķerēšanu (phishing), kas ir sensitīvas informācijas izvilināšana, uzdodoties par personu vai organizāciju, kam šī informācija var tikt sniegta. Dažreiz šī informācija tiek izvilināta, izmantojot speciāli pielāgotus un konkrētai personai adresētus pieprasījumus – mērķētā pikšķerēšana;
- **identitātes zādzība**, kad kaut kādā veidā uzzinātos datus par personu izmanto, lai izdarītu kādu noziegumu, piemēram, šīs personas vārdā paņemot aizdevumu kādā ātro kredītu firmā;
- **dažāda veida krāpšana**, piemēram, viltus vēstuļu izsūtīšana darbiniekiem it kā no priekšniekiem.

Informācijas drošība

- **Tehniskā rakstura apdraudējumi:**
- tīši vai netīši aparatūras vai informācijas nesēju bojājumi;
- elektrības traucējumi;
- elektroniski (elektromagnētiski) uzbrukumi.

Informācijas drošība

- **Tehnoloģiskā rakstura apdraudējumi** ir ļoti daudzveidīgi un atkarīgi no izmantotās tehnoloģijas. Svarīgākie no tiem pašlaik saistīti ar datoru izmantošanu:
- ļaunatūra (malware) – **programmatūra, kas izveidota ar mērķi traucēt datoru darbību**, ievākt informāciju, piekļūt īpaši aizsargātām sistēmām, uzbrukt citām sistēmām, izplatīt mēstules vai reklāmas, vai jebkādā citā veidā nesankcionēti ietekmēt datoru darbību. Ļaunatūrai ir dažādi paveidi – vīrusi, u.c. Tā var tikt veidota specifiskiem uzdevumiem, piemēram, mērķētiem uzbrukumiem vai spiegošanai, kā arī inficēto datoru failu šifrēšanai, prasot maksu par atšifrēšanas atslēgu;
- **piekļuves lieguma uzbrukumi** tiek izmantoti, lai pārslogotu sistēmas un tās nebūtu spējīgas atbildēt uz leģitīmiem pieprasījumiem. Izkliedēto piekļuves lieguma uzbrukumu organizēšanai parasti tiek izmantoti robotu tīkli;
- **robotu tīkli ir inficētu datoru un citu ierīču kopums**, kas tiek centralizēti vai decentralizēti kontrolēts, lai uzbruktu citiem datoriem, izmantojot piekļuves lieguma vai cita veida uzbrukumus, izsūtītu mēstules, inficētu jaunas ierīces.

Informācijas drošības apdraudētāju mērķi un motīvi

- **Informācijas apdraudētāju motīvi un mērķi** ir daudzveidīgi un var būt saistīti ar:
- ziņkārību vai pašapliecināšanos, kas bija raksturīga galvenokārt hakeriem datortīklu pirmsākumos;
- politisko vai reliģisko pārliecību, kas tiek pausta ziņojumos, kuri tiek atstāti uzlauztajās sistēmās;
- finansiāliem ieguvumiem, kas ir šīs – skaitliski lielākās – noziedznieku grupas stimuls;
- konkurences cīņu, kaitējot konkurentu vai politisko pretinieku darbībai vai reputācijai;
- terorismu, kas var tikt vērsts uz dažādiem kritiskās infrastruktūras objektiem ražošanā, transportā, sakaru sistēmā, elektroapgādē, veselības aizsardzībā u.c.;
- spiegošanu, gan izmantojot tradicionālas metodes, gan kibervidi apsteidzošas informācijas iegūšanai politiskā vai ekonomiskā kontekstā;
- militāra rakstura uzbrukumiem, apdraudot militāros datortīklus vai iesaistoties hibrīdkara aktivitātēs.

Informācijas drošības aizsardzība

- **Informācijas drošības aizsardzībai ir komplekss raksturs un tā aptver daudzpusīgus pasākumus.**
- **Organizatoriskie pasākumi** ir pats konservatīvākais pasākumu veids, kuru būtība ir maz atkarīga no izmantotajām tehnoloģijām:
- **informācijas drošības dokumentācijas izstrāde** valsts iestāžu un uzņēmumu līmenī, kas satur drošības noteikumus, risku analīzi, darbības nepārtrauktības plānu un vajadzīgās instrukcijas;
- **darbinieku atlase**, uzturot pielaižu sistēmu valsts līmenī, ietverot prasības par konfidencialitāti uzņēmumu darbinieku darba līgumos vai noslēdzot atsevišķu vienošanos u.c.
- **autorizācijas sistēmas**, darbinieku atbildības noteikšana, lai katram darbiniekam būtu pieejama tikai tā informācija, kas nepieciešama viņa pienākumu veikšanai, šo darbinieku kontrole;
- **nepārtraukta darbinieku apmācība** par vispārīgām tēmām un informācijas drošības jautājumiem;
- **izmaiņu pārvaldība**, visām izmaiņām ir jābūt rūpīgi pārbaudītām, tām jānotiek savlaicīgi informējot un apmācot visas iesaistītās puses.

Informācijas drošības aizsardzība

- **Tehniskie pasākumi:**
- nepārtrauktā elektropiegāde, kas tiek nodrošināta ar nepārtrauktās barošanas sistēmām un rezerves sprieguma ģeneratoriem;
- rezerves serveri vai cita aparatūra, kas var būt izvietota arī attālināti citā lokācijā vai citā valstī;
- profilaktiskās pārbaudes atbilstoši tehniskajiem noteikumiem;
- savlaicīgs remonts vai bojāto mezglu nomaiņa, kas ir jāparedz un attiecīgās detaļas un mezgli ir jātur rezervē;
- fizisko piekļuvi regulējošie līdzekļi – atslēgas (arī elektroniskās), speciālas telpas un durvis, video reģistrācija.

Informācijas drošības aizsardzība

- **Tehnoloģiskais virziens:**
- vīrusus un citu ļaunatūru apkarojošie līdzekļi, piemēram, antivīrusu un pretspiegošanas programmas;
- ugunsmūris datoram, kas nodrošina kontrolētu piekļuvi sistēmām tīkla līmenī;
- kriptogrāfiskie līdzekļi, digitālais paraksts, kas galvenokārt tiek lietoti, lai nodrošinātu informācijas konfidencialitāti un integritāti;
- savlaicīga operētājsistēmas un citas programmatūras ievainojamību novēršana, regulāri atjaunojot programmatūru;
- rezerves kopēšana lokāli vai arī attālinātā datu glabātuvē (mākonī);
- informatīvo datu bāzu veidošana gan par aizdomīgām vietnēm un lietotnēm, gan par neapšaubāmi uzticamām (melnie un baltie saraksti);
- autentifikācijas sistēmas (paroles, atslēgas, sertifikāti, biometrija);
- ielaušanās kontroles sistēmas, kas seko aktivitātēm tīklā vai sistēmā, lai fiksētu aizdomīgas darbības vai drošības politikas pārkāpumus;
- konfidenciālās informācijas noplūdes novēršanas programmatūra, kas seko sensitīvās informācijas izmantošanai un pārsūtīšanai ar mērķi fiksēt un novērst nesankcionētas darbības.

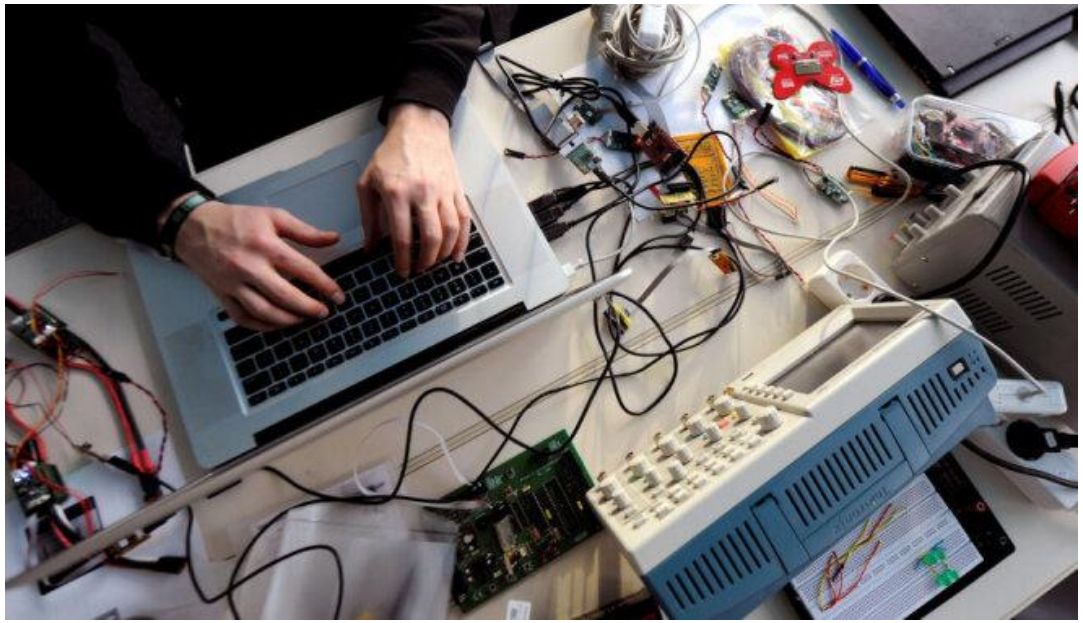
Informācijas drošības militārais aspekts

- Pasaulē informācijas drošība kļūst arvien nozīmīgāka arī militārajā kontekstā.
- **NATO kibertelpu ir pasludinājis par piekto cīņas telpu līdzās zemei, gaisam, ūdenim un kosmosam.**
- 10.05.2010. tika izveidota **ASV kiberdrošības pavēlniecība** (United States Cyber Command, USCYBERCOM) kā ASV Stratēģiskās pavēlniecības (United States Strategic Command) vienība. Tā centralizē militārās operācijas kibertelpā un sinhronizē militāro tīklu aizsardzību.
- Krievijā ir izveidotas jaunas bruņoto spēku vienības – **informācijas operāciju spēki**, kas sastāv no karaspēka daļām kara apgabalos un flotēs un tiek komplektētas no ar matemātiķiem, programmētājiem, inženieriem, kriptogrāfiem, sakarniekiem, radioelektroniskās cīņas virsniekiem, tulkiem u.c. To uzdevums ir veikt kiberkaujas operācijas un aizsargāt militāros datortīklus.

Kiberapdraudējuma novēršana

- **Kiberapdraudējums** Latvijai ir uzskatāms par būtisku nacionālās drošības apdraudējumu, kas sistemātiski pieaugs, jo IT nozīmei un lomai ir pieaugoša tendence globālā mērogā, kā arī valsts pārvaldes, sabiedrības un ekonomikas funkcionēšanā.
- Valsts un sabiedrības izdzīvotspēja paliek aizvien vairāk atkarīga no IT.
- Lai īstenotu valsts pamatfunkcijas, ir nepieciešami risinājumi, kas nodrošina valsts kontroli pār svarīgo IT infrastruktūru.
- Kiberapdraudējumi nav nodalāmi no politiskajiem, ekonomiskajiem, militārajiem un sociālajiem notikumiem un ģeopolitiskās situācijas kopumā un tie ir vērtējami nedalīti no vispārējā apdraudējuma.

Kiberuzbrukums ir rīcība, kad nelikumīgā veidā mēģina ietekmēt citu cilvēku vai citas puses spēju darboties kibervidē, viņu datu integritāti, kā arī viņa identitātes integritāti.
Kiberuzbrukumu mērķis ir sabojāt vai iegūt kontroli vai piekļuvi svarīgiem dokumentiem un sistēmām uzņēmuma vai personālo datoru tīklā.



Kiberapdraudējuma novēršana

- Joprojām aug valstu skaits, kam ir ievērojamas spējas veikt kiberizlūkošanu, informācijas operācijas sabiedrības un lēmēju viedokļa ietekmēšanai un destruktīvas darbības kibertelpā (pakalpojumu bloķēšana, IT iekārtu bojāšana, fiziskās infrastruktūras bojāšana).
- Apdraudējumu kibertelpā var radīt **ārvalstu specdienesti, bruņoto spēku paspārnē izvietotas kibervienības, kā arī atsevišķi haktīvistu grupējumi,** kas darbojas saskaņā ar valsts institūciju uzdevumiem, vai pēc savas iniciatīvas, **kiberhuligāni un kibernoziedznieki.**
- Kibertelpu savu interešu īstenošanai izmanto arī teroristiski grupējumi, kas lielākoties kibertelpā izplata propagandu un vervē kaujiniekus.
- IT infrastruktūra savstarpēji savieno institūcijas un uzņēmumus gan Latvijā, gan ārvalstīs. Attiecīgi, iespējamie apdraudējumi vienai institūcijai var radīt riskus citām, tāpat apdraudējumi vienā valstī var ietekmēt citu valstu kibertelpas drošību.
- Hakeru uzbrukums ASV informācijas tehnoloģiju kompānijai "Kaseya" varētu būt ietekmējis līdz pat 1500 uzņēmumu pasaulē, teikts kompānijas publiskotajā paziņojumā.

Kiberapdraudējuma novēršana

- Kiberapdraudējuma kontrole un samazināšana ir iespējama tikai sasaistē ar **efektīvi īstenotu valsts kiberdrošības politiku,** kas ilgtermiņā un sistemātiski nodrošinātu rīcībspēju krīzes situācijās, attīstītu informācijas un tehnoloģiju jomas tiesisko regulējumu, izglītotu sabiedrību, kā arī mērķtiecīgi strādātu pie atbildīgo institūciju spēju attīstīšanas un cilvēkresursu nodrošinājuma nozarei.
- Lai veiktu jomas uzlabojumus, ir izstrādāti un pieņemti vairāki dokumenti, kas tiešā veidā ietekmē kibervides jautājumus, piemēram, **Latvijas kiberdrošības stratēģija 2019.-2022. gadam**.
- **"Latvijas kiberdrošības stratēģija 2023.–2026. gadam"** ir izstrādāta, pamatojoties uz Informācijas tehnoloģiju drošības likuma 11. panta otro daļu. Tā raksturo Latvijas kiberdrošības situāciju, identificē nākotnes izaicinājumus un definē galvenos nacionālās kiberdrošības politikas rīcības virzienus laika periodam līdz 2026. gadam (ieskaitot).

Latvijas kiberdrošības stratēģija

- **Kiberdrošības politikas vīzija ir droša, atvērta, brīva un uzticama kibertelpa,** kurā ir garantēta valstij un sabiedrībai būtisku pakalpojumu droša, uzticama un nepārtraukta saņemšana un sniegšana un indivīda cilvēktiesības tiek ievērotas kā fiziskajā, tā virtuālajā vidē.
- **Kiberdrošības politikas mērķis** ir stiprināt un attīstīt kiberaizsardzības spējas, paaugstinot noturību pret kiberuzbrukumiem un veicinot sabiedrības izpratni par draudiem kibertelpā. Īstenojot kiberdrošības politiku iek definētas šādas prioritātes: **aizsardzība, atturēšana un attīstība.**
- **Nacionālās kiberdrošības politikas rīcības virzieni ir**
- "Kiberdrošības pārvaldības pilnveidošana".
- "Kiberdrošības veicināšana un izturētspējas stiprināšana".
- "Sabiedrības izpratne, izglītība un pētniecība".
- "Starptautiskā sadarbība un tiesiskums kibertelpā.
- "Kibernoziedzības novēršana un apkarošana".

Hibrīdkarš

- Ar **hibrīdkaru** saprot jebkuru darbību, ko pret savu pretinieku īsteno agresora valsts, lai panāktu sev labvēlīgu iznākumu konfliktā.
- Atšķirība starp nosacīti "parastu" jeb konvenciālu karu un hibrīdkaru:
- „Ja konvencionālajā karadarbībā galvenā cīņa notiek starp valstu karaspēkiem, starp dažādiem militāriem grupējumiem, tad hibrīdkarā primāri cīņa tiek vērsta vai iedarbība tiek īstenota pret citas valsts sabiedrību un lēmumu pieņēmējiem. Tas arī nozīmē, ka instrumentu klāsts, kas tiek izmantots, ir daudz plašāks" (Austrumeiropas politikas pētījumu centra pētnieks Māris Cepurītis).
- Tātad hibrīdkarš ir nevis tikai cīņa karavīram pret karavīru, bet arī pretinieka sabiedrības psiholoģiska ietekmēšana un spiediens uz politisko eliti.

Hibrīddraudu izpausmes

- Hibrīddraudu izpausmes ir daudzpusīgas, un tās var ietvert gan **militārus līdzekļus un to izmantošanas draudus, gan plaša spektra nemilitāru līdzekļu pielietošanu, sākot ar izlūkošanas un drošības dienestu operācijām, kiberuzbrukumiem, plašām informācijas kampaņām un dezinformācijas izplatīšanu, pretrunu un konflikta potenciāla izmantošanu sabiedrībā un beidzot ar ekonomisko spiedienu un terorismu.**
- Hibrīddraudu izpausmes tiek īstenotas sinhroni, vienai otru papildinot, turklāt to būtība ir maksimāli slēpt jebkādu saikni ar attiecīgo aktivitāšu plānotājiem, tāpat arī to īstenotājus daudzos gadījumos var nojaust, taču precīzi noteikt un pierādīt to iesaisti ir ļoti grūti.

Hibrīddraudu izpausmes

- Informatīvais karš
- Piemēram, informatīvajās kampaņās vai informācijas karā agresora valsts savai sabiedrībai iestāsta "pareizo" situācijas interpretāciju, bet pretinieka valstī izplata nomelnojošu un provocējošu informāciju. Mērķis ir saliedēt savu un šķelt pretinieka sabiedrību, diskreditēt otras valsts varu vietējā un starptautiskā līmenī. Efektīvs var izrādīties arī spiediens uz pretinieka politisko eliti.
- „Zaļie cilvēciņi"
- „Zaļie cilvēciņi" jeb "zaļie vīriņi" karo kādā no iesaistītajām pusēm, taču oficiāli nepieder nevienai no armijām. Viņu mērķis ir radīt apjukumu. „Zaļajiem cilvēciņiem" parasti nav atšķirības zīmju, kas padara daudz sarežģītāk identificēt šo agresoru. Ja tiek radīts apjukums, tad zināma neuzticība var izplatīties konkrētās valsts bruņotajos spēkos, lēmumu pieņemšanas struktūrās, kas var arī sarežģīt tālāko valsts rīcību.
- **Hibrīddraudiem, tostarp kiberdrošības riskiem, arī turpmāk būs pieaugoša tendence, īpaši ņemot vērā informācijas tehnoloģiju (IT) attīstību.**