Komisjoni metoodika ning tuvastatud valimiste tehnoloogiate ohtude tutvustus

Dan Bogdanov, PhD

Dan Bogdanov, akadeemik ja
küberturvalisuse komisjoni esimees

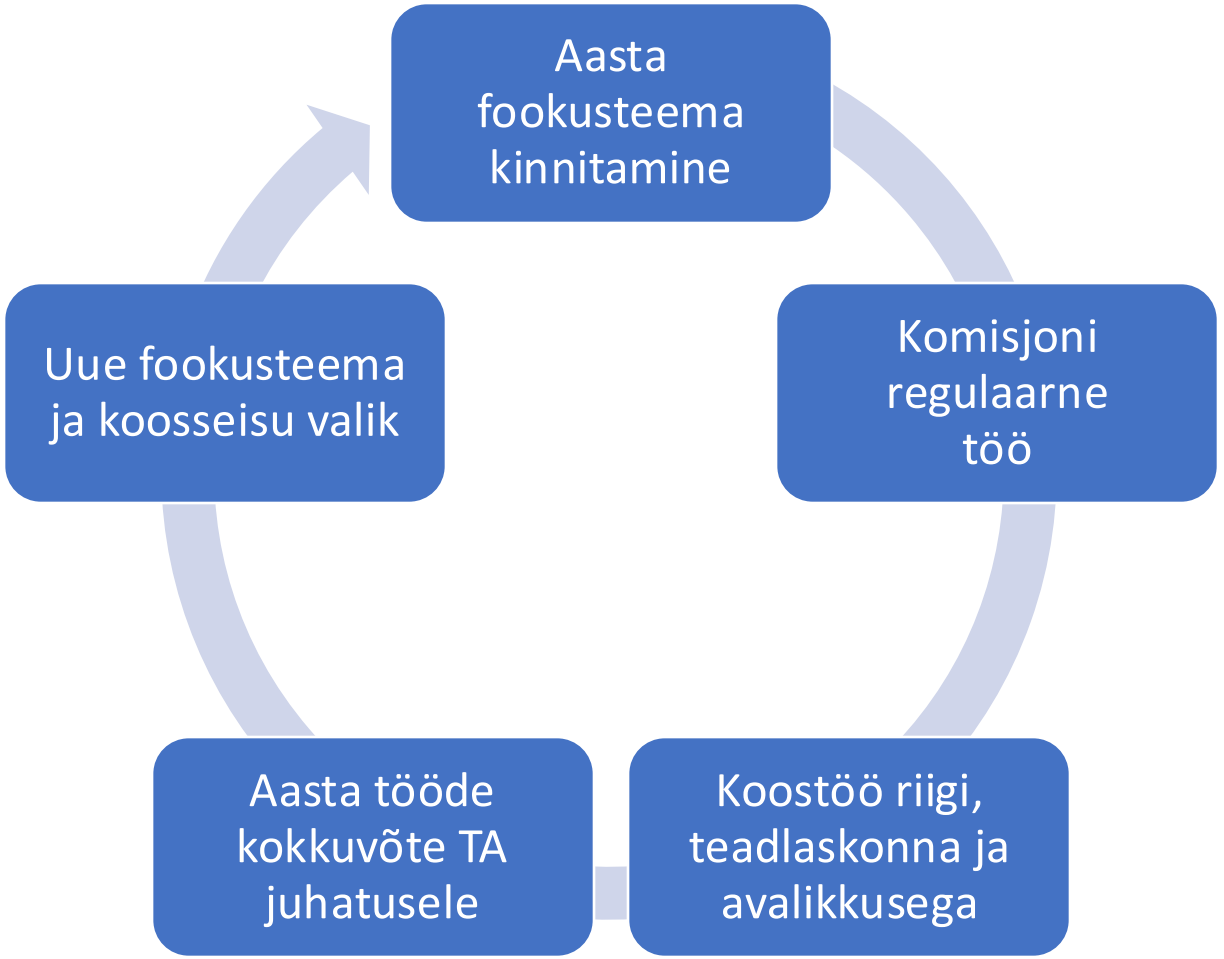
Ajaloost ja uuest mandaadist

- TA küberkaitse komisjon loodi 2012. aastal (juht Leo Mõtus), kuid see ei olnud mitmeid aastaid enam aktiivne
- 15. detsembril 2022 andis akadeemia juhatus akad Bogdanovile ülesandeks komisjon taaskäivitada
- 20. juunil 2023 kinnitas akadeemia juhatus uue küberturvalisuse komisjoni koosseisu
- Uus küberturvalisuse komisjon kohtus esimest korda 14. augustil 2023

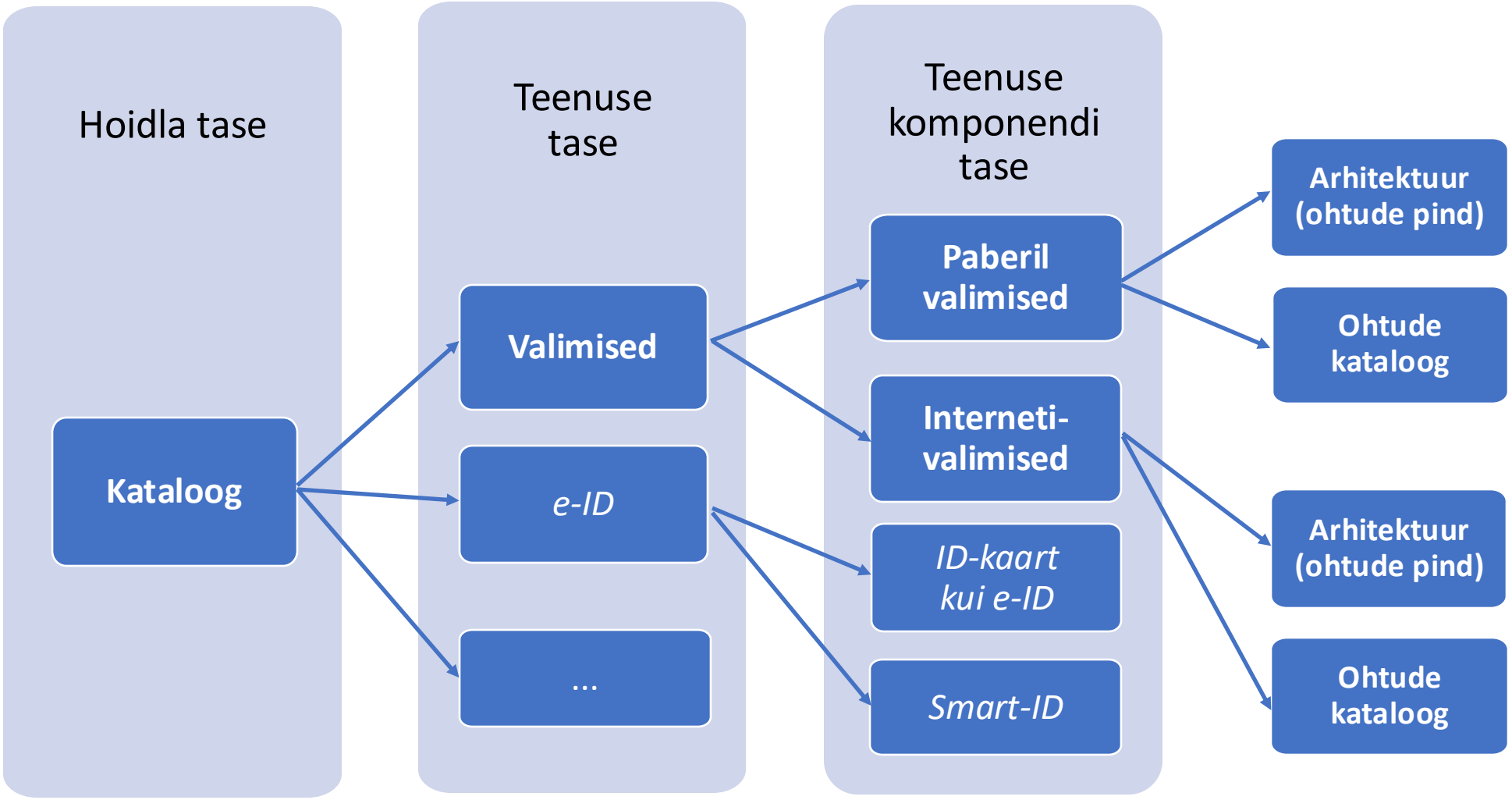
Komisjoni peamine eesmärk:
ühtlustatud turbeohtude kataloog ja riskianalüüsi metoodika

Komisjoni tsükkel on ühe aasta pikkune

- Komisjoni mandaat on uurida digitaalsete teenuste riskide analüüsi metoodikaid
- Uurimisobjektid valitakse Eesti e-riigi teenuste seast (digitaalne identiteet, valimised, andmepõhised teenused)



Riskianalüüsi kavandatav infoarhitektuur



Ohtude analüüsi metoodika

1. Komisjoni liige pakub välja ohusündmuse, mida uurida
2. Komisjoni liige kirjeldab ohusündmust ja meetmeid
3. Komisjoni istungil loetakse ja täpsustatakse kirjeldust, luuakse ühtne arusaam ohu olemusest
4. Seejärel annab iga istungil osalev komisjoni liige enda hinnangu ohu sagedusele ja mõjule skaalal 1-5.
5. Komisjoni esimees salvestab hinded ja keskmistab need, saades ohu sageduse ja mõju ühe hinnangu
6. Sageduse ja mõju hinnangu korrutis annab selle riskiklassi.

Metoodika kasutamise näidis

Olgu meil hüpoteetiliselt istungil 7 osalejat (tavaliselt on rohkem).

Olgu ohu pealkiri: “Võib juhtuda, et TA küberturvalisuse komisjoni istung läheb kauem, kui ajakavas ette nähtud”.

	Liige 1	Liige 2	Liige 3	Liige 4	Liige 5	Liige 6	Liige 7	Keskmine
Sagedus	4	4	3	2	4	4	4	**3,57**
Mõju	3	3	5	1	4	4	3	**3,29**

Ohu riskiklassi leiame, korrutades 3,57 ja 3,29 ning saame 11,74.

11,74 annab ohule riskiklassiks “Keskmine”

Kuidas saaks kataloogi kasutada?

- Kui teenuse omanik teeb ise turvaanalüüsi, või tellib seda teadlastelt või turbeteenuse andjatelt, palutakse võtta aluseks kataloog ning esitada töö selle täiendusena.
- Kui teenuse omanikul on vaja vastata nt avalikkuse päringutele, teeb ta seda kataloogile tuginedes.
- Kui tekib päring, mille kohta kataloogis sissekannet pole, siis küsimusele vastamise käigus täiendatakse kataloogi (nii et järgmine kord oleks vastamine kiirem).
- Teenuse omanik võib otsustada kataloogis enda teenuse turvaanalüüsi ka kasutada arendusotsuste tegemiseks.

Komisjoni 2023-2024 töö
31 valimiste tehnoloogia ohu analüüs

Komisjoni koosseis 2023–2024

- Esimees: Dan Bogdanov (akadeemik, Cybernetica AS teadusdirektor)
- Alo Einla (RIA valimiste osakonna juht)
- Arne Koitmäe (Riigi valimisteenistuse juht)
- Kristjan Krips (Cybernetica AS teadur)
- Ivo Kubjas (ConsenSys vanemteadusinsener)
- Liisa Past (MKM riikliku küberturvalisuse osakonna juhataja)
- Teet Raidma (VVK liige, IS Audit OÜ juhtaudiitor, RIA vanemekspert)
- Mihkel Solvak (Tartu Ülikooli tehnoloogiauuringute kaasprofessor)
- Ahto Truu (Guardtime tarkvaraarhitekt)
- Tarmo Uustalu (akadeemik, Reykjaviki ülikooli professor, TalTech juhtivteadur)
- Priit Vinkel (e-Riigi Akadeemia SA vanemekspert e-valitsemise alal)
- Jan Willemson (Cybernetica AS vanemteadur)

Mõju ja võimalikkuse skaalad

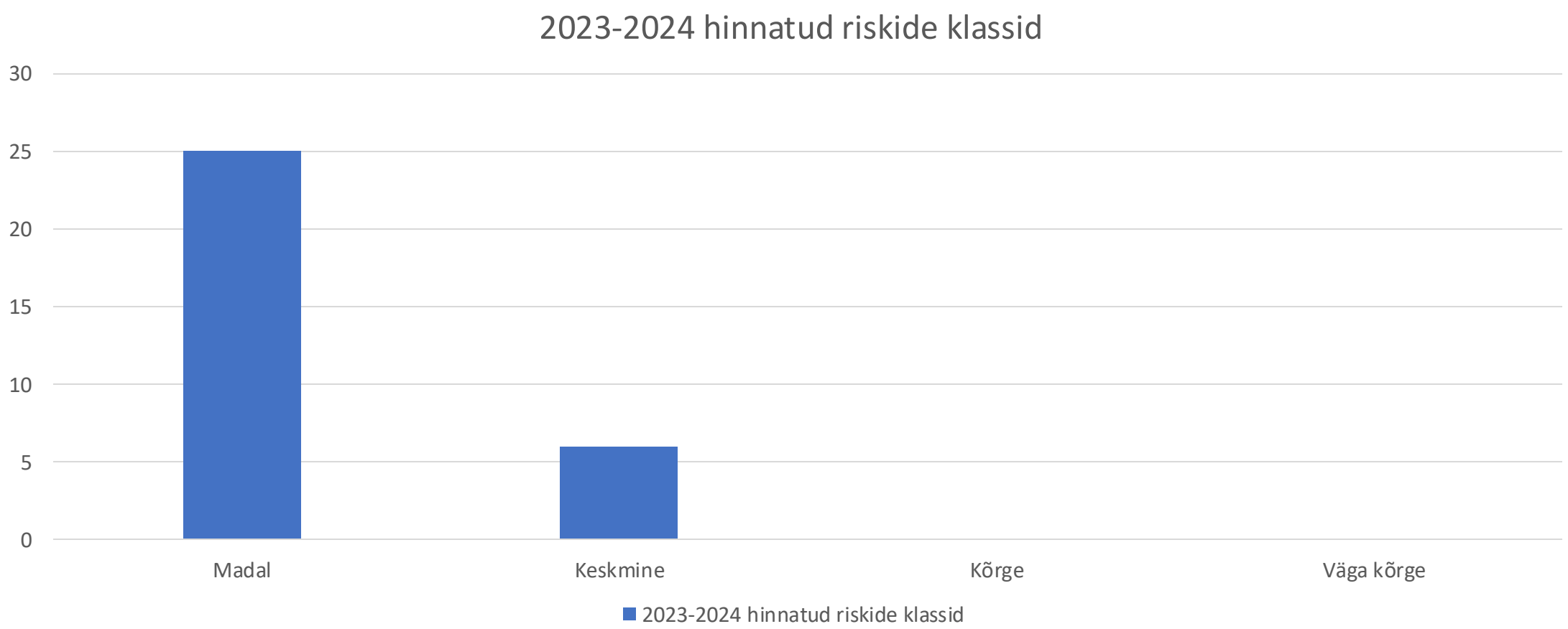
Mõju skaala

- 5 – kriitiline mõju konkreetsetele valimistele, võib mõjutada valimisi tulevikus
- 4 – kriitiline mõju konkreetsetele valimistele, võib mõjutada valimistulemusi
- 3 – märkimisväärne mõju valimiste läbiviimisele
- 2 – intsidendi mõju on väike
- 1 – mõju puudub, intsident on
- lihtsasti lahendatav

Võimalikkus skaala

- 5 - (peaaegu) kindel
- 4 – tõenäoline
- 3 – võimalik
- 2 – vähetõenäoline
- 1 – väga harv

Hinnatud riskide klassid



M-hääletamise rakenduste autentsus ja terviklus võib olla tõendatavalt auditeerimata (1)

- **Ohusündmuse kirjeldus**: M-hääletamise rakendusi võidakse hakata levitama läbi Google Play Store'i ja Apple App Store’i. Need kanalid kasutavad sisulevivõrke (CDN) ja pakendavad rakendusi ka pärast üleslaadimist ringi. Vaja on uusi juhendeid, kuidas kontrollida valimisrakenduste terviklust
- **Mõjutatud objekt**: Apple/Google sisulevivõrgu kaudu levitatav m-hääletamise rakendus.
- **Ohu ulatus**: ülemaailmne, rakenduste levituskanaliga seotud ohud on globaalsed ja mõjutavad ka teisi iOS/Androidi rakendusi
- **Ohuagendi tüüp**: riikliku taustaga ründaja

M-hääletamise rakenduste autentsus ja terviklus võib olla tõendatavalt auditeerimata (2)

- **Olemasolevad kaitsemeetmed**
  1. E-hääletuse organisatsiooni kirjelduses määratakse audiitori roll ja selle rolliga seotud tegevused.
  2. E-hääletuse käsiraamatus kirjeldatatakse detailsemalt, mida audiitor peab hindama ning millistes protseduurides audiitor osaleb.
  3. Audiitor peab vastama nõuetele (kogemused, sertifikaadid jne).
- **Võimalikud lisakaitsemeetmed**
  1. M-valimiste audiitori juhendi loomine. M-hääletus kui selline pole käsiraamatus lahti kirjutatud, seega pole hetkel ka kirjeldatud m-hääletuse auditeerimise protseduure.

M-hääletamise rakenduste autentsus ja terviklus võib olla tõendatavalt auditeerimata (3)

- **Hinnangu aeg**: 16. jaanuar 2024
- **Mõjuhinnang**: 3,55 (komisjoniliikmete hinnete keskmine)
  - Selgitus: kriitiline mõju valimiste läbiviimisele, sest ei ole võimalik tagada valimiste terviklust.
- **Võimalikkuse hinnang**: 4 (komisjoniliikmete hinnete keskmine)
  - Selgitus: 2024. aasta kevadel olemasoleva info põhjal on riski avaldumine lähitulevikus kindel, kuna praegu pole piisavalt infot Apple/Google sisulevivõrkude kohta ning ühiskonda on teavitatud, et m-hääletamine kavataksetakse kasutusele võtta. Samuti puudub praegu detailne auditeerimisjuhend.
- **Riskiklass**: 14,18 (keskmine risk)

Demokraatlike valimiste vastane (vale)infokampaania võib kahjustada nende usaldusväärsust (1)

- **Ohusündmuse kirjeldus:** valimiste usaldusväärsust rünnatakse valeinfokampaaniaga. Kannatab valimiste usaldusväärsus ning koormatakse valimiste läbiviijat.
- **Mõjutatud objekt**: valimised ja selle läbiviija
- **Ohu ulatus**: võib olla nii Eesti-keskne kui ülemaailmne
- **Ohuagendi tüüp**: motiveeritud subjekt (nii siseriiklik kui välismaine, nii eraalgatuslik kui riiklikult toetatud organisatsioon)

Demokraatlike valimiste vastane (vale)infokampaania võib kahjustada nende usaldusväärsust (2)

- **Olemasolevad kaitsemeetmed**
  1. Avalik kommunikatsioon.
  2. Efektiivne klienditugi.
  3. Koostöö strateegilise kommunikatsiooni osas (Riigikantselei, RIA, RVT, VVK).
- **Võimalikud lisakaitsemeetmed**
  1. Varajane, ennetav ja strateegiliselt planeeritud kommunikatsioon, sh valimiste toimimise ja riskihalduseks ette võetud sammude osas. Koordineeritud ja erinevaid sihtgruppe ning ohustsenaariume arvestavad sõnumid ja kõneisikud (laiapõhiselt üle riigi, kodanikuühiskonna, teadlaskonna).
  2. Kõikide uuenduste ja muudatuste teavitus tehakse piisavalt varakult. Näiteks, m-hääletamine võetakse eeldatavalt kasutusele 2025. aasta oktoobris, vastavat kommunikatsiooniplaani tuleks ette valmistada juba 2024. aastal.
  3. Valimiste ning selle tehnoloogia ja protsesside läbipaistvuse ja mõistetavuse suurendamine, et selle selgitamine oleks lihtsam erinevatele sihtrühmadele ja kõneisikutele.

Demokraatlike valimiste vastane (vale)infokampaania võib kahjustada nende usaldusväärsust (3)

- **Hinnangu aeg**: 3. juuni 2024
- **Mõjuhinnang**: 3 (komisjoniliikmete hinnete keskmine)
  - Selgitus: Kui väärinfokampaania käigus edastatav sõnum on efektiivselt sihitud ja atraktiivne, siis on mõju käimasolevatele valimistele märkimisväärne. Kui kampaania on sihitud hääletamisperioodi algusele, võib see halvemal juhul kaasa tuua hääletamistoimingute peatamise.
- **Võimalikkuse hinnang**: 3,7 (komisjoniliikmete hinnete keskmine)
  - Selgitus: Sarnaste uudiste ja sõnumitega puutuvad valimiste korraldajad kokku pea igal korral. Niisiis on tegu väga realistliku stsenaariumiga. M-valimiste sisseviimine laiendab võimalike argumentide valikut veelgi.
- **Riskiklass**: 11,1 (keskmine risk)

Mõned e-hääletamise etapid võivad jääda auditeerimata või vaatlemata, sest tänane protokoll seda ei võimalda (1)

- **Ohusündmuse kirjeldus:** Internetihääletamise protsesside ja protokolli keerukuse ning väliste osapoolte (usaldusteenuste pakkujad, sisulevivõrgud jt tootmis- ja tarneahela osapooled) olemasolu tõttu pole võimalik kõiki valimiste etappe auditeerida.
- **Mõjutatud objekt**: kogumisteenus, elektrooniline urn
- **Ohu ulatus**: Eesti-keskne, kuna küsimus on Eestis kasutusel oleva hääletussüsteemi ja valimissüsteemi auditeerimises.
- **Ohuagendi tüüp**: valimisi ette valmistava või läbi viiva asutuse töötaja

Mõned e-hääletamise etapid võivad jääda auditeerimata või vaatlemata, sest tänane protokoll seda ei võimalda (2)

- **Olemasolevad kaitsemeetmed**
  - *Mitmeid, vt aruandest*
- **Võimalikud lisakaitsemeetmed**
  1. Vähendame väliseid osapooli, kus see on otstarbekas ning ei tõsta muid riske.
  2. Võtame kasutusele tehnilised lahendused serverite kaughaldamise auditeerimise võimaldamiseks.
  3. Toome ohuhinnangutes konkreetselt välja sõltuvused välistest osapooltest.
  4. Võimaldame audiitoril taristut võimalikult suures ulatuses auditeerida.
  5. Süsteemi protokollide ja protsesside uuesti kavandamine auditeerimise ulatuse ja lihtsuse tõstmiseks (nt andmeauditeeritavate protokollide kasutamine).

Mõned e-hääletamise etapid võivad jääda auditeerimata või vaatlemata, sest tänane protokoll seda ei võimalda (3)

- **Hinnangu aeg**: 27. mai 2024
- **Mõjuhinnang**: 3,11 (komisjoniliikmete hinnete keskmine)
  - Selgitus: Käesolev oht ei kirjelda konkreetset rünnet, vaid kirjeldab eeldusi muude rünnete läbiviimiseks ja õnnestumiseks. Hinnatud on tervikmõju.
- **Võimalikkuse hinnang**: 3,9 (komisjoniliikmete hinnete keskmine)
  - Selgitus: Teada on alametappe, millele valimiste audiitor juurde ei saa. Vaatlejatel puudub ülevaade, millised valimiste protokolli ja protsessi osad on milliste auditite ga või ülevaatustega kaetud.
- **Riskiklass**: 12,3 (keskmine risk)

Komisjoni tulevikuplaanid

- 2024-2025 hooajal tegeleb komisjon valimiste tehnoloogiaga.
- Eesmärgid:
  - Katta ohud, mida avalikkus, uued komisjoniliikmed ja arenevad teadus ja tehnoloogia välja toovad
  - Kus vaja, hinnata üle esimese tööaasta ohte
  - Pakkuda välja kestlik lahendus valimiste tehnoloogiate riskide analüüsiks
- 2025-2026 hooajal jätkab komisjon uue teemaga.