# EESTI TEADUSTE AKADEEMIA
## KÜBERTURVALISUSE KOMISJON

Koosolek nr. 6

Tallinnas, 20. veebruaril 2024

Koosolek kestab kl 10.30-14.00

Osalevad: komisjoni esimees akadeemik Dan Bogdanov, Jan Willemson, Kristjan Krips, Priit Vinkel, Ahto Truu ja Ivo Kubjas.
Külalisena Indrek Leesi ja Kati Ambo-Vaher Vabariigi valimiskomisjonist ja Priit Parmakson RIAst.
Puuduvad Mihkel Solvak, Liisa Past, Alo Einla, Teet Raidma ja akadeemik Tarmo Uustalu.

PÄEVAKORD:

1) Komisjoni liikmed teavitavad teisi komisjoni liikmeid uudistest, mis võivad mõjutada komisjoni tööd.
2) Komisjoni esimees esitleb ettepanekut paberhääletamise, e-hääletamise ja m-hääletamise võrdlevaks riskianalüüsiks. Järgneb arutelu.
3) Töötame läbi kodutöödena tehtud riskianalüüse.

PROTOKOLL:

1) Komisjoni liikmete teavitus teistele uudistest, mis võivad mõjutada komisjoni tööd. Komisjoni liikmed arutavad olulist infot, mis on laekunud eelmisest koosolekust alates.
    a. ERRis ilmus akadeemik Dan Bogdanovi artikkel, mis oli suunatud valimiste turvalisuse alase diskussiooni arendamisele.
    b. Lühidat käsitlust leidis põhiseaduskomisjoni käsitletud pöördumine valimiste vaadeldavuse tõstmise teemal. Järgnenud arutelu käigus

nentisid mitmed komisjoni liikmed, et Eestis puudub hea ametlik kanal valimiste tehnoloogia arenduse ja uuenduse aruteluks ning see tekitab arusaadavalt rahulolematust. Komisjoni juht akadeemik Bogdanov nõustus ning lisas, et TA küberturvalisuse komisjonil pole selleks tegevusest otsest mandaati, kuid komisjon on valmis oma võimete mahus sellist algatust toetama.

c. Jätkuteemana arutleti veel RVT kommunikatsioonitegevusi, sh välismaistel üritustel esitatud kriitikale vastamist. Kati Ambo-Vaheri sõnul on RVT www.valimised.ee lehel avaldatud materjalid, kus kirjeldatakse e-valimiste kohta levivaid müüte ja tegelikkust. Erinevate küsimuste käsitlemine aitab vältida ebaõiget arusaama e-hääletamisest, vähendada kaebuste hulka ja lahendada juba esitatud kaebusi.
d. Üheskoos teadvustati, et m-valimiste lahendus on endiselt arenduses.

2) Ettepanekud paberhääletamise, e-hääletamise ja m-hääletamise võrdlevaks riskianalüüsiks.
   a. Komisjoni esimees akadeemik Dan Bogdanov teavitab komisjoni, et senistel istungitel on läbi käidud üksikuid ohte. On näha, et hoidlasse on tekkinud mitmete ohtude kirjeldused, aga natuke on dubleerimist. Kaugem eesmärk on, et tekiks riskide võrdlemise tabel kõigi kolme hääletamisviisi kohta. Kus võimalik, võrreldaks sarnast riski valimistele sõltuvalt hääletusviisist. Lisaks toodaks eraldi välja hääletusviisi iseärasustest lähtuvad riskid.
   b. Ahto Truu leidis, et esitletu on hästi hea ülevaatetabel. Keerukust tekitab, kuidas see tabel kokku panna täna planeeritavast hoidlast, kus ohud on jaotatud hääletusviiside järgi. Peame leidma viisi, kuidas märkida hääletusviisist sõltumatuid riske, samuti riske, mis rakenduvad kolmest hääletusviisist kahele.
   c. Järgnes arutelu, kuidas hoidlas märgendada riske, mis rakenduvad mitmele hääletusviisile (seni oli jaotus kaustapõhine).
   d. Arutelu käigus jõuti ideele, et selline analüüs oleks tulevikus kasutatav ka arendustööde prioriteedi seadmiseks – kõrgemate riskide kahandamine on hea põhjendus täiendavateks protsessi ja tehnoloogiate arenduseks.
   e. Kristjan Krips tõstatas küsimuse, kas tuleks esile tõsta riskid, mis on kriitilise mõjuga, aga väga vähetõenäolised? On ka kriitilisi riske, mille mõju on tänase tehnoloogiataseme juures väga madal, aga see võib tehnoloogia arenedes kiirelt muutuda. Akadeemik Bogdanov nõustus ning tõi näitena Eesti e-riigi täna kasutusel olevat krüptograafiat ohustava võimaliku kvantarvuti ehitamise, mida oodatakse mitte enne 20 aastat, aga näiteks internetivalimiste

viimine uhiuuele protokollile ja krüptograafiale on vähemalt 4-5 aastat kestev protsess, sest vajab läbipaistvust.

3) Komisjoni liikmed arutavad ja hindavad riske enda püstitatud ohustsenaariumite korral.
    a. Läbi vaadati seitse riski. Tehti täiendusi ning anti üheskoos hinnanguid mõjule ja sagedusele. Harjutuse eesmärk oli uurida, milliste riskide puhul ekspertpaneeli hinnangud erinevad ja kus on ühtsed.
    b. Akadeemik Bogdanov tänas osalejaid ning tegi ettepaneku, et järgmiseks istungiks peaks komisjoni liikmetele andma täpsemad ülesanded. Nendest teavitab Dan komisjoni peatselt.

Komisjoni esimees: Dan Bogdanov

Protokollis: Ülle Sirk