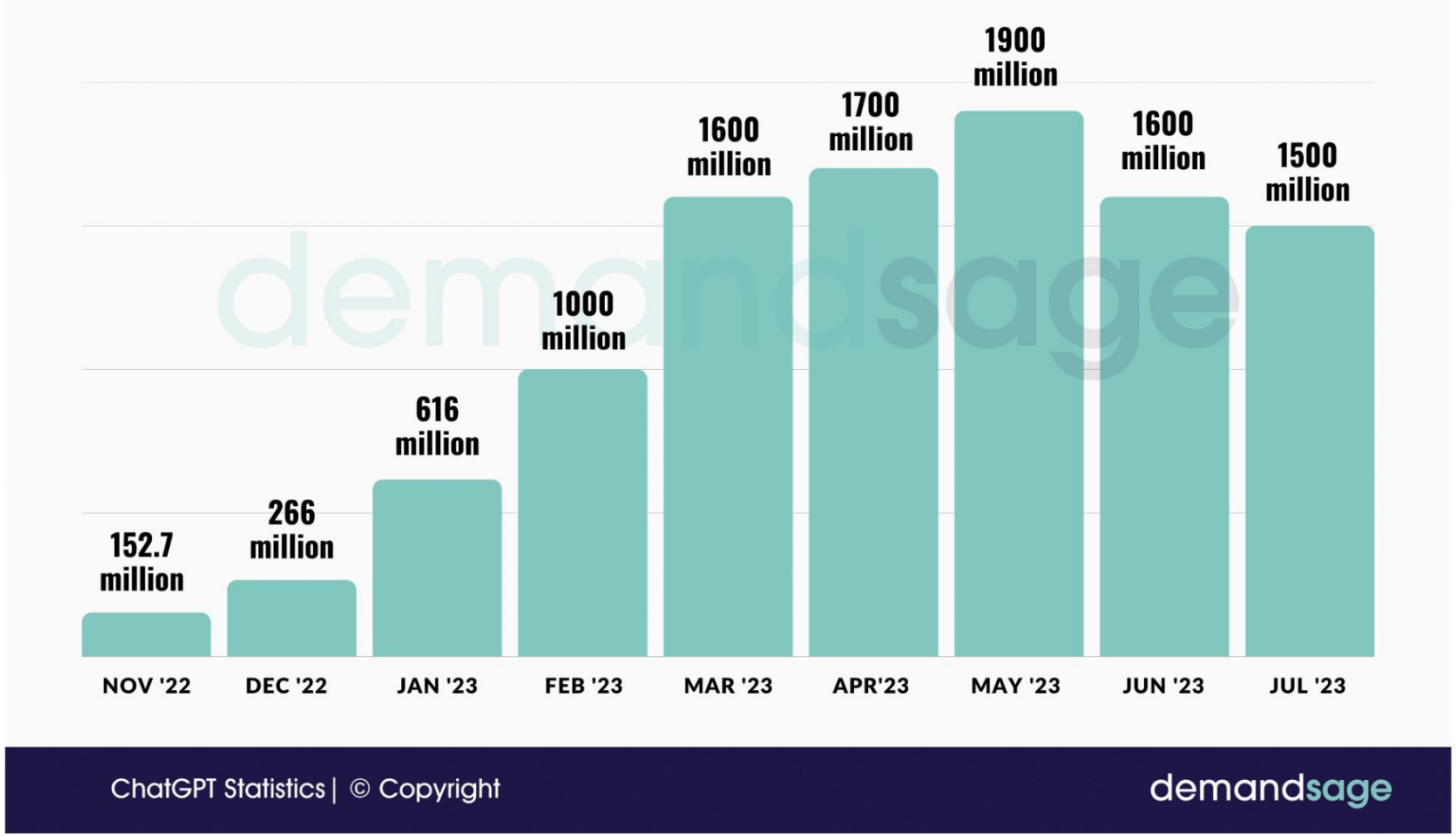
Kuidas saame tehnoloogia abil riske leevendada?

Liina Kamm, PhD
Cybernetica AS vanemteadur
liina.kamm@cyber.ee

CYBERNETICA

Tulevikku tagasi hoida on keeruline

- Läbimurdelised tehnoloogiad võetakse kasutusele ka ilma regulatsiooni toeta
- ChatGPT vestlusrobot jõudis 100 miljoni kasutajani kahe kuuga ning kasvas edasi



Allikas: https://www.demandsage.com/chatgpt-statistics/ (9. oktoober 2023)

Tehisintellekti ja andmetehnoloogiate riskid

- Risk 1: tehisintellekti mudelite treeningandmeid ja sisendandmeid (isikuandmed, ettevõtete andmed) ei osata piisavalt kaitsta.
  - Kahju: andmed töödeldakse ebaseaduslikult, rikutakse õiguseid või ärisaladust
- Risk 2: tehisintellekti mudel ei ole kvaliteetne ning annab vigast väljundit
  - Kahju: loodud süsteem ei anna soovitud efekti, diskrimineerib või kahjustab isikuid, kelle kohta see ennustusi teeb
- Risk 3: tehisintellekti mudelis on andmekaitse, ärisaladuse või autoriõigusega kaitstud andmed, mille töötlemiseks kasutajal õigust ei ole
  - Kahju: teiste poolt treenitud mudeli kasutuselevõtja rikub mudeli loomisel kasutatud andmete või teostega seotud õiguseid

Teadlased on neid riske ette näinud

- Privaatsuskaitse tehnoloogiad aitavad kaitsta inimeste ja ettevõtjate andmeid andmete töötlemise.

- Nii Euroopa Komisjon kui ka Ameerika Ühendriikide teadusagentuurid (DARPA, NIH, NSF, ONR) on rahastanud privaatsuskaitse tehnoloogiate uurimist viimase 15 aasta jooksul sadade miljonite eurode ja dollaritega.

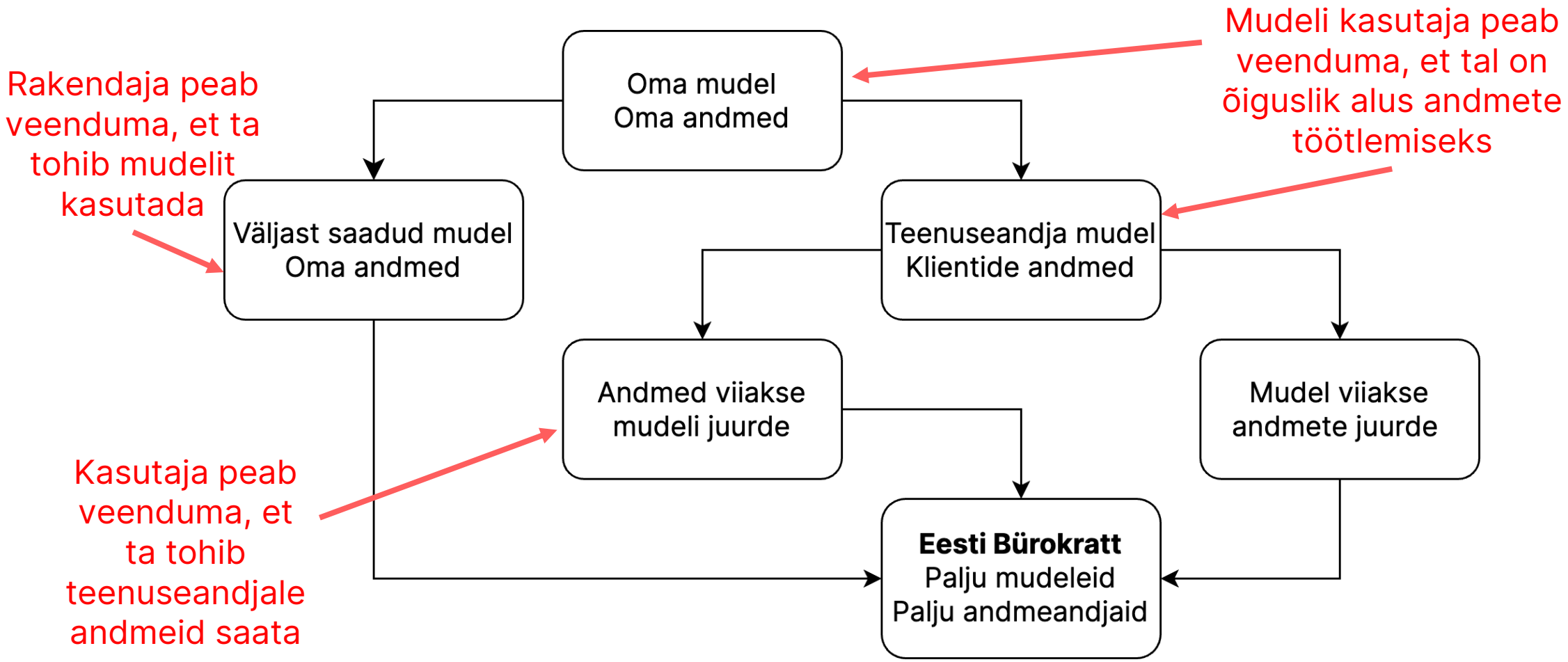
- Edukaid pilootprojekte on palju, aga tehnoloogiate juurutamisega on viivitatud.

Kaks värsket uuringut Eestis

- Privaatsuskaitse tehnoloogiate uuring (november 2022 - märts 2023)
  - Tellija: Majandus- ja Kommunikatsiooniministeerium
  - Täitja: Cybernetica AS infoturbeinstituut
  - Tulemid: Privaatsuskaitsetehnoloogiate kontseptsioon, kataloog ja teekaart
  - Avaldatud: https://www.kratid.ee/analuusid-ja-uuringud

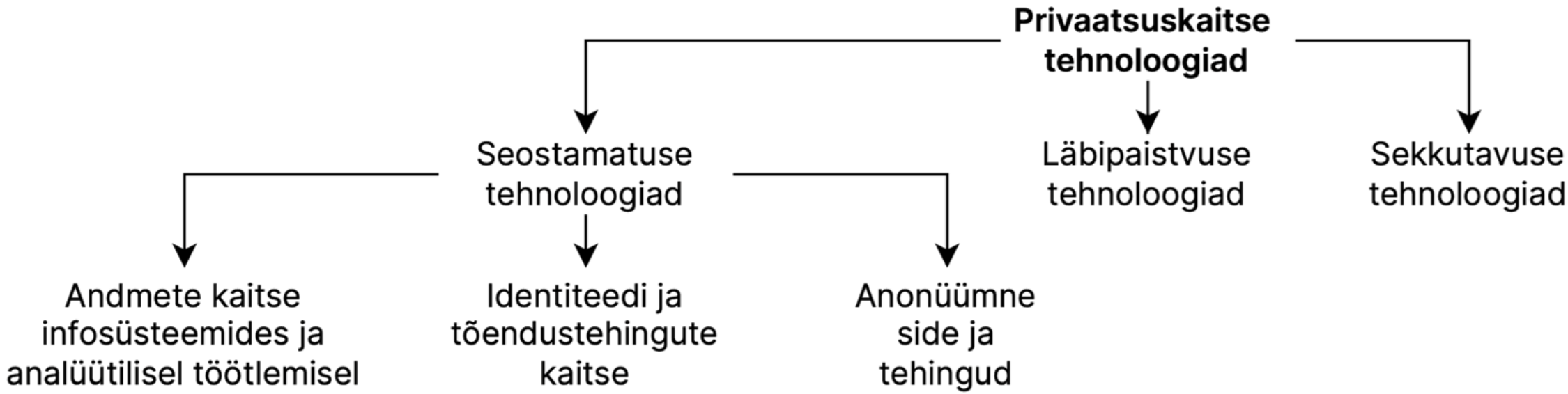
- Tehisintellekti ja masinõppe tehnoloogia riskide ja nende kahandamise võimaluste uuring ja õppevideod (august 2023 – juuni 2024)
  - Tellija: Riigi Infosüsteemi Amet
  - Täitja: Cybernetica AS infoturbeinstituut
  - Uuring on veel käimas, tulemused avaldatakse 2024. aastal

AI-teenuste lihtsustatud hierarhia



CYBERNETICA

Privaatsuskaitse tehnoloogiad



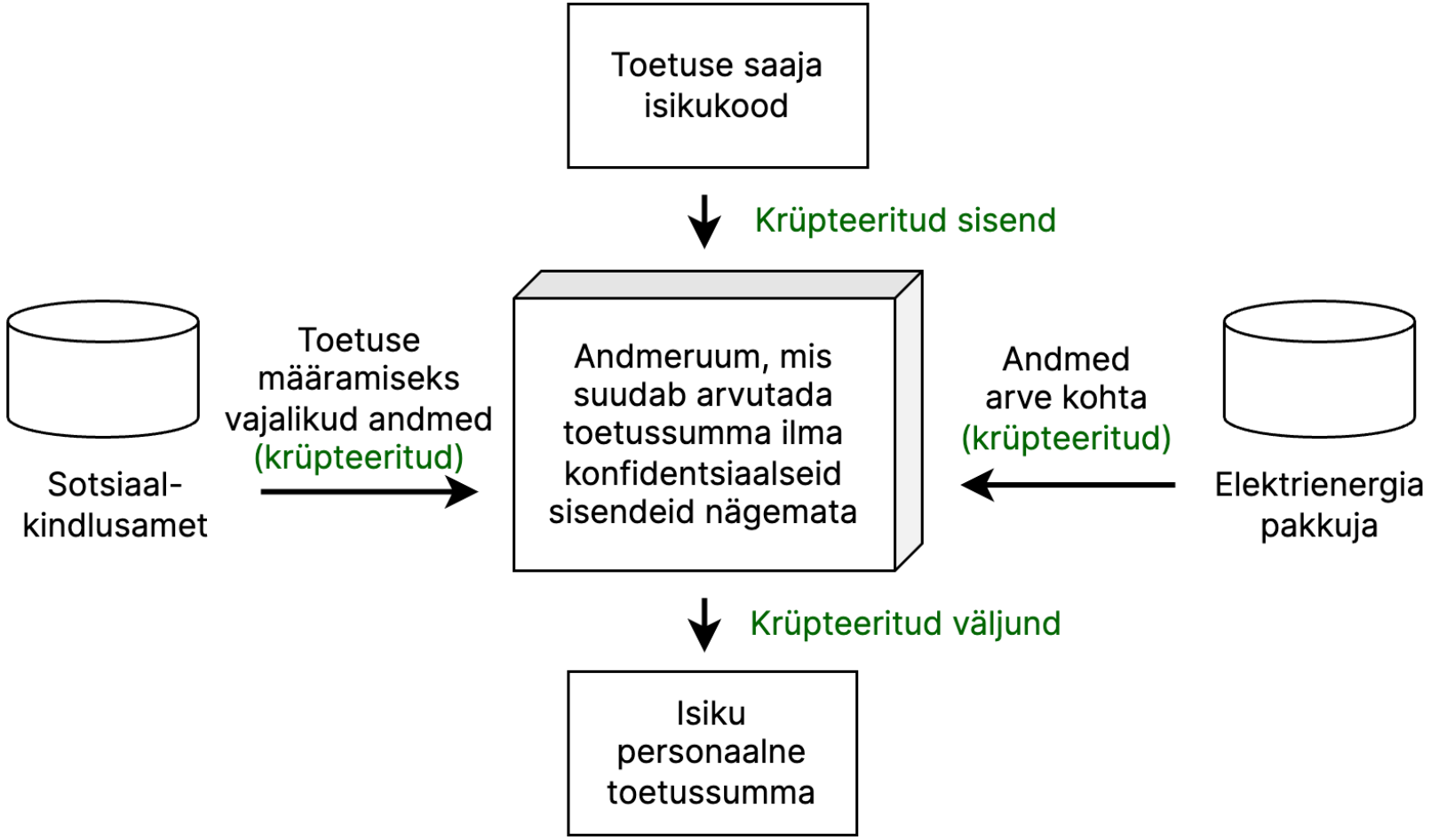
CYBERNETICA

Privaatsuskaitse tehnoloogiate uuring

Kontseptsioon:
- tehnoloogiate ülevaade ja lühikirjeldus,
- ülevaade riikide kogemusest,
- e-riigi kasutusjuhtude kirjeldus.

Teekaart:
- õigusmaastik,
- Eesti kogemused privaatsuskaitse tehnoloogiatega,
- Eesti riigiasutuste privaatsuskaitse-alased vajadused,
- poliitikasoovitused,
- rakendamise arendusplaan.

Personaalne ja privaatne toetuste määramine



CYBERNETICA

Aitäh!

Liina Kamm, PhD
liina.kamm@cyber.ee

https://cyber.ee/
info@cyber.ee
cybernetica
CyberneticaAS
cybernetica_ee
Cybernetica

CYBERNETICA