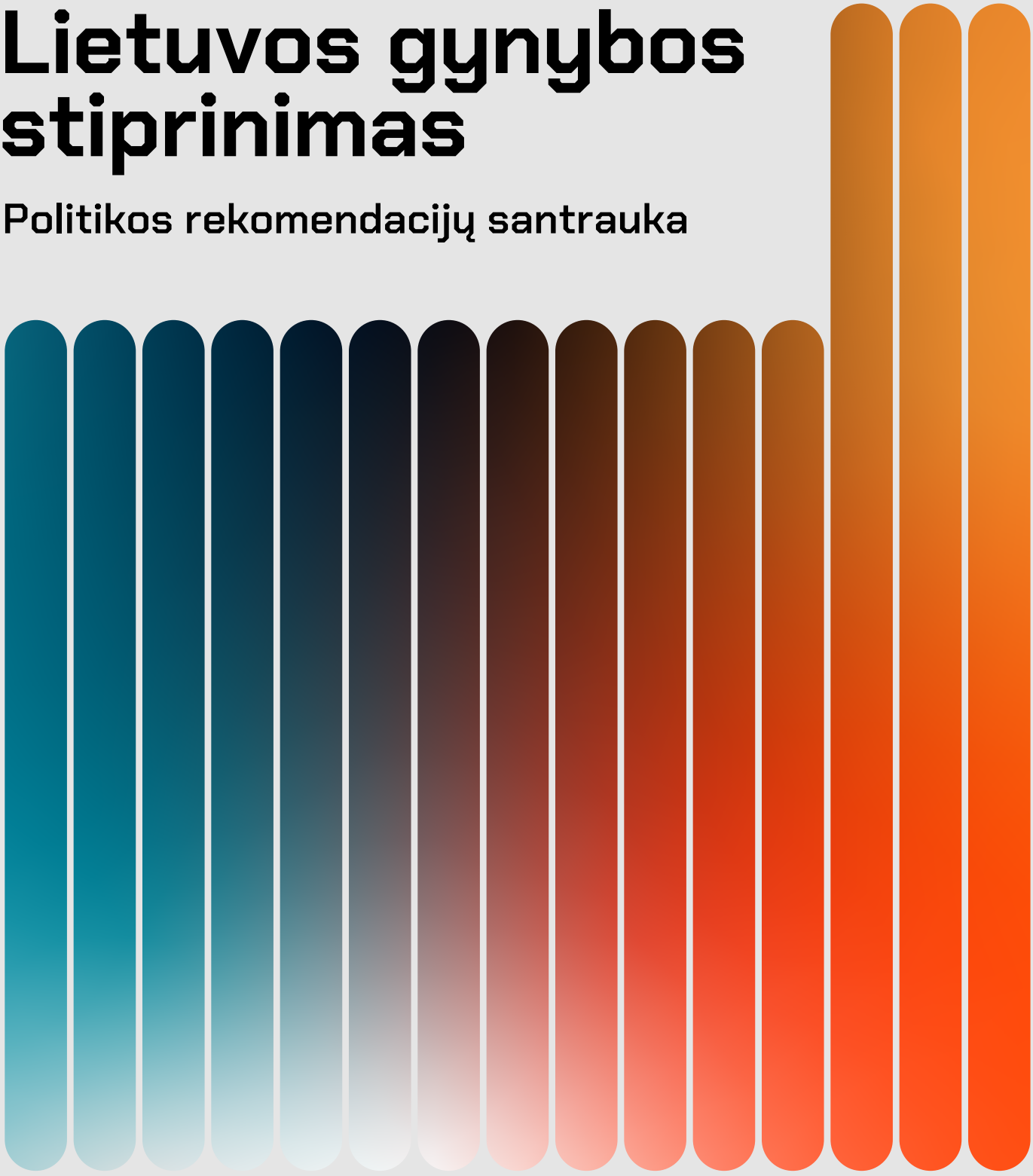
Human and More-Than-Human Futures: Innovating Technologies for Coexistence

Kartu su MISTI Lithuania

ktu 1922

Lietuvos gynybos stiprinimas

Politikos rekomendacijų santrauka



Parengė „MISTI Lithuania“ konsorciumas Lietuvos bendradarbiavimui su MIT, dalyvaujant Lietuvos verslo, akademijos, rizikos kapitalo ir viešojo sektoriaus atstovams

SITUACIJOS APŽVALGA

Lietuvos gynybos **inovacijų ekosistema yra fragmentuota** – tarp ministerijų, agentūrų, akademijos ir pramonės trūksta koordinacijos, bendros vizijos, pasitikėjimo ir sąveikumo. Finansavimo ir pirkimų srityje nėra nuoseklaus nuo idėjos iki diegimo vedančio finansavimo ciklo. Aukšti technologinės parengties reikalavimai (TRL 5+) gynybos ir dvejopos paskirties projektams reiškia, kad daug perspektyvių ankstyvos stadijos idėjų taip ir nepasiekia prototipų kūrimo etapo. Realios karo lauko patirtys nėra pakankamai integruotos į inovacijų kūrimo ekosistemą.

Karas Ukrainoje atskleidė **gamybos pajėgumų trūkumo problemą** visose NATO / ES šalyse ir aiškiai parodė, kad labai svarbu ne tik aukštų technologijų produktai ir sprendimai, bet ir sugebėjimai juos gaminti greitai, laiku ir atitinkamais mastais už prieinamą kainą. Reikia išmokti sąveikauti su jau esama inžinerine ir technologijų pramone, kad ji galėtų įsilieti į gamybos potencialo vystymą bei tiekimo grandines.

Lietuvos informacinių technologijų (IT) ir operacinių technologijų (OT) **infrastruktūros veikia nuolatinio spaudimo sąlygomis** – daugėja kibernetinių ir informacinių atakų, ypač kriziniu laikotarpiu. Didžiausi pažeidžiamumai kyla jungčių tarp IT ir OT sistemų, programinės įrangos tiekimo grandinių ir duomenų dalijimosi barjerų srityse.

Lietuvos **susisiekimo ir energetikos infrastruktūra** – keliai, geležinkeliai, elektros ir ryšių tinklai – išlieka nepakankamai pralaidi, patikima ir tvari, vertinant pagal Vakarų Europos standartus. Ypatingai pažeidžiami yra bevielio ryšio sistemos ir telekomunikaciniai tinklai, kurie karo metu galėtų būti lengvai sutrikdomi ar neutralizuojami elektroninės kovos metodais, o energetikos tinklas nėra parengtas dirbti mažuose lokaliuose potinkliuose.

Lietuvos visuomenės **atsparumas krizėms išlieka menkas** – tik 14 proc. gyventojų žino artimiausius evakuacijos kelius, vos trečdalis supranta, kaip paruošti namus ekstremaliai situacijai. Hibridinis šiuolaikinio karo pobūdis, įtraukiantis tiek fizines ginkluotąsias pajėgas, tiek kibernetines atakas, tiek informacinės erdvės užvaldymą kenkėjiška informacija, rodo, kad būtina keisti mąstymo kryptį – nuo atgrasymo link puolimo, nuo reaktyvaus **link proaktyvaus elgesio modelio**.

REKOMENDACIJOS

Esminiai sprendimai trumpuoju laikotarpiu (12–18 mėn.)

Gynybos inovacijų ekosistemos vystymas

- Artimiausiu laikotarpiu Lietuvai būtina sukurti „vieno langelio“ idėjų pateikimo ir finansavimo, įskaitant žemo TRL idėjų vystymo ir prototipų testavimo mechanizmų, diegimą.
- Būtina remti MSI, mažąsias ir vidutines įmones, suteikiant joms galimybę gauti finansavimą jau nuo ankstyvųjų technologinės parengties stadijų (pavyzdžiui, nuo TRL2-3).
- Kartu būtina užtikrinti sistemingą karybos patirties ir ekspertinių žinių grąžinimą į inovacijų kūrimo ciklą, aktyviai įtraukiant atsargos karininkus, gynybos ekspertus ir kitus praktinės karybos patirties turinčius profesionalus.

Kritinių technologijų ir infrastruktūros vystymas

- Bepiločių platformų ir jų kontrpriemonių sprendimai, optoelektronika, mechatronika ir biotechnologijos galėtų tapti „greito starto“ sritimis, kuriose Lietuva turi realų potencialą tapti lydere per specializaciją ir fokusą.
- Būtina transformuoti geležinkelius ir kelius į multimodalinius susisiekimo koridorius, išplečiant jų zonose elektros skirstymo, ryšių (optikos, mobiliojo ryšio bazinių stočių) tinklus ir logistinės paramos pajėgumus.
- Reikia pradėti kurti testavimo poligonus oro gynybos, bepiločių platformų ir sistemų vidutinių ir ilgų nuotolių technologijoms, nes šių galimybių šiandien Europoje beveik nėra.
- Reikia skatinti alternatyviomis medžiagomis iš vietinių žaliavų ir naujausiomis gamybos technologijomis grįstas inovacijas gynybos produktams, kad į tiekimo grandines įsitrauktų daugiau regioninės pramonės ir būtų plečiami gamybos pajėgumai ir jų mastas.

Kibernetinio saugumo stiprinimas

- Kibernetinio saugumo srityje metu siūloma sukurti sektorinį „mesh“ tipo saugos operacijų centrą energetikos ir transporto sektoriuose.

- Būtina įdiegti hibridinės debesijos „landing zone“ aplinką su atsparaus atkūrimo testais.
- Reikia sukurti eID sąveikos su stipraus šifravimo gairėmis modelį ir atlikti šifravimo migracijos bandymus.

Informacinės gynybos stiprinimas

- Būtina kurti nacionalinę informacinės erdvės stebėsenos ir greito reagavimo sistemą tiek Lietuvoje, tiek diasporoje.
- Turi būti suformuotos faktų tikrinimo ir kontrnaratyvo komandos krizių ir rinkimų laikotarpiams.
- Reikalingas koordinuotas komunikacijos mechanizmas vyriausybės lygiu su socialinių tinklų platformomis.

GAIRĖS ILGAJAM LAIKOTARPIUI (5–10 METŲ)

Strateginė ambicija – sukurti europinio masto integruotą gynybos inovacijų ekosistemą, kurioje nauji sprendimai galėtų būtų perkelti iš ankstyvos idėjos į lauko bandymus ne per metus, o **per kelis mėnesius**.

Ilgalaikis gynybos pajėgumų stiprinimas turėtų remtis **valstybės ir privataus sektoriaus partnerystėmis**, kuriose valstybė prisiima reikšmingą (apie 50 proc.) kapitalo dalį dvejopos paskirties technologijų ir gamybos pajėgumams plėtoti. Būtina išryškinti ir sustiprinti **Lietuvos inžinerinės ir technologijų pramonės** – mechanikos, elektronikos, optikos, mašinų ir transporto priemonių gamybos, mechatronikos – vaidmenį, ypač perimant šios pramonės patirtį efektyvinant ir skaitmeninant gamybą.

Ilguoju laikotarpiu Lietuvai būtina užtikrinti **saugų jūrų kelią į Vakarus**. Ypač perspektyvus sprendimas – autonominių ir nuotoliu valdomų stebėjimo ir puolamųjų **bepiločių platformų** integravimas šio kelio apsaugai bei logistikos organizavimui.

Be to, Lietuva turi vystyti bent vidutinio nuotolio **puolamąsias technologijas**, nes dėl sąlyginai nedidelio strateginio gylio reikalingi gynybiniai pajėgumai leidžiantys efektyviai kontratakuoti ir perkelti veiksmų teatrą į priešininko teritoriją.

Kibernetinio saugumo srityje iki 2030 m. numatoma pasiekti visuotinio SOC tinklo padengimą, integruoti OT įvykių stebėseną ir tamsiojo interneto žvalgybą, užtikrinti, kad visos kritinės sistemos naudotų NIST, ISO ir ETSI standartais paremtus **šifravimo algoritmus**.

Informacinėje erdvėje ilgalaikis siekis – pasiekti visuotinę informacinę brandą, kur informacinis raštingumas ir kritinis mąstymas būtų **integruoti į švietimo sistemą visais lygiais**. Lietuva turėtų sukurti tvirtą **demokratinių procesų apsaugos** sistemą, audituojamą prieš rinkimus, bei **civilinio ir karinio bendradarbiavimo** modelį.

STRATEGINIS BENDRADARBIAVIMAS IR KOORDINACIJA

Siūloma įkurti **Kariuomenės inovacijų biurą (KIB)** į kurio pagrindines funkcijas įeitų tarpžinybinė koordinacija efektyviai komunikacijai tarp ministerijų, mokslo institucijų, verslo ir pramonės įmonių. KIB sistemingai rinktų realius operacinius poreikius, juos verstų aiškiais technologiniais uždaviniais ir perduotų pramonei bei tyrėjams. Toks biuras atliktų centrinio mazgo funkciją nacionalinėje inovacijų grandinėje, užtikrindamas, kad inovacijų vystymas prasidėtų nuo mūšio lauko patirties – technologijų, kurios realiai didina išlikimą, mobilumą ir efektyvumą. Tai yra praktika, paplitusi pažangiose gynybos ekosistemose (Izraelis, Suomija, JAV), kur inovacijų ciklas grindžiamas grįžtamuoju ryšiu iš karių ir karininkų.

Kariuomenės inovacijų biuras padėtų išspręsti gynybos inovacijų ekosistemos fragmentacijos iššūkį bei palengvintų komunikaciją su partnerių organizacijomis, tokiomis kaip NATO DIANA, pagrindinėmis ginkluotės darbo grupėmis NAAG, NNAG, NAFAG, COE bei STO ir NIAG. Be to, NATO Inovacijų fondas (NIF) bei Europos gynybos fondas (EDF) finansuoja būtent tas ekosistemas, kurios geba veikti kartu, kaip platformos, o ne pavienės institucijos. Lietuva turi unikalią galimybę tapti tokio modelio dalimi, bet tam reikalingas **nacionalinis koordinatorius**, gebantis integruoti Lietuvos MTEP potencialą į NATO inovacijų tinklus.

Regioninis bendradarbiavimas yra kitas kritinis komponentas. Bendri pilotiniai projektai su Estija, Latvija, Lenkija ir Suomija leistų spartinti testavimą, mažinti vieneto savikainą ir kurti Baltijos gynybos inovacijų klasterį – praktika, kurią jau taiko Šiaurės šalys ir Izraelis. Taip pat mokslo, inovacijų ir pramonės bendradarbiavimas gali paskatinti ir gilesnį bendradarbiavimą vystant gynybos technologijas ir gynybos pajėgumus bei vykdant bendrus įsigijimus.

AUTORIAI IR EKSPERTAI

Prof. Dr. Edita Gimžauskienė	Kauno technologijos universiteto Strateginių partneryščių prorektorė
Prof. Dr. Monika Petraitė	Kauno technologijos universiteto Ekonomikos ir verslo fakulteto Inovacijų ir antreprenerystės tyrimų grupės pagrindinė tyrėja
Prof. Dr. Šarūnas Grigaliūnas	Kauno technologijos universiteto Kibernetinio saugumo kompetencijų centro vadovas
Dr. Artūras Medeišis	Vilniaus Gedimino technikos universiteto Elektronikos fakulteto dekanas
Dr. Andrius Vilkauskas	Kauno technologijos universiteto Mechanikos inžinerijos ir dizaino fakulteto vyr. tyrėjas
Paulius Vaitkevičius	„Novian“ programavimo srities inovacijų ir produktų vadovas
Peter Nielsen	AB „Lietuvos geležinkeliai“ nepriklausomas valdybos narys
Dr. Simona Pūkienė	LR Krašto apsaugos ministerijos mokslo ir inovacijų patarėja
Tadas Gudėnas	Lietuvos kariuomenės inovacijų ekspertas
Una-May O'Reilly	MIT Informatikos ir dirbtinio intelekto laboratorijos (CSAIL) ALFA tyrėjų grupės vadovė
Dr. Kevin P. O'Brien	MIT elektros inžinerijos ir kvantinių technologijų ekspertas