TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Karistusõiguse osakond

Priit Pruks

# TÖÖSTUSSPIONAAŽI-VASTASED MEETMED KAITSETÖÖSTUSE KAITSEL

Magistritöö

Juhendaja
*mag. iur.* Andres Parmas

Kaasjuhendaja
*mag. iur.* Martin Purre

Tartu
2025

# Sisukord

# Sissejuhatus

„Uus külm sõda“ [1] on käes. Autokraatiad vastanduvad demokraatiatele[2], maailmamajandus lõheneb[3], valitsevad riiklikud huvid ja väheneb vabakaubandus[4], toodetakse tuumarakette[5] ja ähvardatakse neid kasutada[6], kruvitakse pingeid mere-, õhu- ja maailmaruumis[7], sõditakse

[1] George Kennan 1998. aastal pärast NATO laienemist: Friedman, T. L. Foreign Affairs; Now a Word From X. The New York Times 02.05.1998. – https://www.nytimes.com/1998/05/02/opinion/foreign-affairs-now-a-word-from-x.html (25.10.2024). [Tsitaat: *"I think it is the beginning of a new cold war," said Mr. Kennan from his Princeton home. "I think the Russians will gradually react quite adversely and it will affect their policies. I think it is a tragic mistake. There was no reason for this whatsoever. No one was threatening anybody else. This expansion would make the Founding Fathers of this country turn over in their graves. We have signed up to protect a whole series of countries, even though we have neither the resources nor the intention to do so in any serious way.“*]; Ivo H. Daalder ja James M. Lindsay pärast 2001. aasta terrorirünnakuid: Daalder, I. H., Lindsay, J. M. The New Cold War. Brookings 30.09.2001. – https://www.brookings.edu/articles/the-new-cold-war/ (25.10.2024). [Tsitaat: *„The post-Cold War era abruptly ended the morning of Sept. 11, 2001. From the moment terrorists turned passenger airplanes into weapons of mass destruction, the United States was inescapably engaged in a new “war” against global terrorism. […]This struggle is—instead—much more like the Cold War of the past century.“*]; Edward Lucas 2008. aastal enne Gruusia sõda: Lucas, E. The New Cold War: Putin’s Russia and the threat to the West. Palgrave Macmillan 2008; Robert D. Kaplan 2019. aastal keset USA-Hiina rivaalitsemist: Kaplan, R. D. A New Cold War Has Begun. Foreign Policy 07.01.2019. – https://foreignpolicy.com/2019/01/07/a-new-cold-war-has-begun/ (25.10.2024); Niall Ferguson ja Condolezza Rice 2023. aastal pärast täiemahulise sõja algust Ukrainas: Ferguson, N., Rice, C. Niall Ferguson and Condolezza Rice on the new cold war. The Economist 13.11.2023. – https://www.economist.com/the-world-ahead/2023/11/13/niall-ferguson-and-condoleezza-rice-on-the-new-cold-war (25.10.2024). Termini „*new Cold War*“ kasutamine on kasvanud jõudsalt alates 2016. aastast, kui Ameerika Ühendriikide presidendiks valiti Donald Trump. Vt lähemalt järgneva artikli *Supplementary Information 1*: Schindler, S., DiCarlo, J., Paudel, D. The new cold war and the rise of the 21st-century infrastructure state. – Transactions of the Institute of British Geographers 2022/47 (2), lk 331–346.

[2] McFaul, M. Autocrats vs. Democrats: China, Russia, and the New Global Order. Mariner Books 2025; Applebaum, A. Autocracy, Inc. The Dictators Who Want to Run the World. Doubleday 2024; Kroenig, M.The Return of Great Power Rivalry: Democracy versus Autocracy from the Ancient World to the U.S. and China. Oxford University Press 2020.

[3] Ferragamo, M. What is the BRICS Group and Why is it Expanding? Council on Foreign Relations 18.10.2024. – https://www.cfr.org/backgrounder/what-brics-group-and-why-it-expanding (14.11.2024).

[4] President Donald. J. Trump. Regulating Imports with a Reciprocal Tariff to Rectify Trade Practices that Contribute to Large and Persistent Annual United States Goods Trade Deficits. Executive Orders. The White House 02.04.2025. – https://www.whitehouse.gov/presidential-actions/2025/04/regulating-imports-with-a-reciprocal-tariff-to-rectify-trade-practices-that-contribute-to-large-and-persistent-annual-united-states-goods-trade-deficits/ (03.04.2025).

[5] Kristensen, H. jt. Status of World Nuclear Forces. Federation of American Scientists 29.03.2024. – https://fas.org/initiative/status-world-nuclear-forces/ (14.11.2024).

[6] Valiarenko, Y. Nuclear Blackmail of the Russian Federation. Ukrainian PRISM. Foreign Policy Council, 10.04.2024. – https://prismua.org/en/english-nuclear-blackmail-of-the-russian-federation/ (14.11.2024); Freedman, L. Putin Keeps Threatening to Use Nuclear Weapons. The New York Times 03.10.2024. – https://www.nytimes.com/2024/10/03/opinion/putin-russia-nuclear-weapons.html (14.11.2024); Williams, H. Why Russia Is Changing Its Nuclear Doctrine Now. Center for Strategic & International Studies, 27.09.2024. – https://www.csis.org/analysis/why-russia-changing-its-nuclear-doctrine-now (14.11.2024).

[7] Kube, C., Gains, M. China has increased military flights near Taiwan by 300%, U.S. general says. NBC News. – https://www.nbcnews.com/politics/national-security/china-increased-military-flights-taiwan-300-us-general-says-rcna179184 (14.11.2024); Jordan, D. China and Philippines trade blame as ships collide. BBC 13.08.2024. – https://www.bbc.com/news/articles/cx2erwedxz5o (14.11.2024); Vene hävitaja narris Alaska kohal pilooti. Helsingin Sanomat/Postimees 02.10.2024. – https://maailm.postimees.ee/8107175/video-vene-havitaja-narris-alaska-kohal-nato-pilooti (14.11.2024); McCarthy, S. China is practicing ’dogfighting’ with satellites as it ramps up space capabilities: US Space Force. CNN. (21.03.2025). – https://edition.cnn.com/2025/03/21/china/china-space-force-dogfighting-satellites-intl-hnk/index.html (11.04.2025).

pingekolletes [8], laiendatakse luure- ja mõjutustegevust [9], vallutatakse kosmost [10], konkureeritakse sõjaliselt olulistes teadus- ja tööstusvaldkondades[11] ning suurendatakse kaitse-eelarveid[12]. Raha otsib innovatsiooni ja kaitsetööstuse ülesandeks on seda pakkuda.

Uue külma sõja valguses tuleb ka Eestil otsustada, kas ja mis ulatuses arendada välja enda kaitsetööstus. Mõistagi on teadus- ja arendustegevusest kasu ainult siis, kui suudetakse, esiteks, arendada välja uued materjalid, tooted ja teenused ning, teiseks, takistada teistel riikidel nende materjalide, toodete ja teenuste aluseks olevat intellektuaalset vara ebaseaduslikult omandamast. Õigusteadus saab kaasa rääkida mõlema probleemi lahendamisel. Õigusreeglitega on võimalik nii tõhustada teadus- ja arendustegevust kui ka kaitsta loodavaid hüvesid.

Loodud hüvesid aitavad eelkõige kaitsta intellektuaalomandiõigus ning ärisaladuse kaitset sätestavad õigusreeglid. Kuid eraõiguslik kaitse eeldab, et rikkuja näol on tegemist isikuga, kes rikkumise korral on valmis osalema vaidluses ning kaotuse korral on valmis ka kahju hüvitama. Nii toimivad suured tehnoloogiaettevõtted, mis lahendavad kohtutes omavahelisi keerulisi intellektuaalomandivaidlusi[13]; või väikesed tehnoloogiaettevõtted, mis käivad kaitsmas end suuremate eest.[14]

---

[8] Venemaa sõda Ukrainas alates 2014. aastast. Hamasi rünnak Iisraeli vastu 7. oktoobril 2023, mis kasvas üle sõjaks Iisraeli ja Hamasi vahel.

[9] Jones, S. G. Russia's Shadow War Against the West. CSIS Briefs. (18.03.2025). – https://www.csis.org/analysis/russias-shadow-war-against-west (11.04.2025); Lawless, J. MI5 spy chief says Russia and Iran are behind a 'staggering' rise in deadly plots. Associated Press 09.10.2024. – https://apnews.com/article/uk-intelligence-mi5-threats-russia-iran-936d7c24d303ffea41f6b1cef7c7b814 (14.11.2024); Frenkel, S., Bergman, R., Saad, H. How Israel Built a Modern-Day Trojan Horse: Exploding Pagers. The New York Times (20.09.2024). – https://www.nytimes.com/2024/09/18/world/middleeast/israel-exploding-pagers-hezbollah.html (18.11.2024); Thibaut, K. Effective US goverment strategies to address China's information influence. Atlantic Council (30.07.2024). – https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/effective-us-government-strategies-to-address-chinas-information-influence/ (11.04.2025); Joske, A. Spies and Lies. How China's Greatest Covert Operations Fooled the World. Hardie Grant Books 2022.

[10] Marshall, T. The Future of Geography: How Power and Politics in Space Will Change Our World. Elliott & Thompson 2023; 2021. aastal ületas kosmoselendude arv 1967. aasta kõrgpunkti: https://spacestatsonline.com/launches. Ameerika Ühendriikide ja Hiina kosmoselennud moodustasid kokku 86% kogu 2024. aasta kosmosemissioonidest. Muuhulgas asutasid Ameerika Ühendriigid 2019. aastal Kosmosejõud (*United States Space Force*). – https://www.spaceforce.mil/About-Us/About-Space-Force/History/.

[11] Miller, C. Chip War: The Fight for the World's Most Critical Technology. Simon & Schuster 2022.

[12] Stockholm International Peace Research Institute. Global military spending surges amid war, rising tensions and insecurity. (22.04.2024). – https://www.sipri.org/media/press-release/2024/global-military-spending-surges-amid-war-rising-tensions-and-insecurity (14.11.2024).

[13] Vogelstein, F. Dogfight: How Apple and Google Went to War and Started a Revolution. Sarah Crichton Books 2013.

[14] Michel, P. R. Big Tech Has a Patent Violation Problem. Harvard Business Review 05.08.2022. – https://hbr.org/2022/08/big-tech-has-a-patent-violation-problem (14.11.2024).

Olukord on aga sootuks teine, kui äriühingu ärisaladusi ohustab mitte avalikult ja seaduslikult tegutsev äriühing, vaid hoopis võõrriik või võõrriigi variettevõte, mis tegutseb salaja ja õiguskorda hülgavalt. Sel juhul läheb käiku kogu eriteenistuste arsenal: töötajaid jälitatakse, äriühingut jälgitakse, ning selleks, et saada, mida vaja, tehakse täpselt seda, mida vaja.[15] Selliste isikute heidutamiseks ei piisa eraõigusest. Tõtt-öelda ei pruugi piisata isegi haldusõigusest. Nimelt kasutab KAPO riigi vastu suunatud luuretegevuse ennetamiseks ja tõkestamiseks mittesõjalisi ennetavaid vahendeid[16], mis võivad seisneda koormavates haldusõiguslikes meetmetes nagu teabehange[17], väljasaatmine[18], sissesõidukeeld[19] või julgeolekukontroll[20], aga ka täiesti tavalises silmast-silma vestluses. Kui haldusõiguslikest meetmest ei piisa, tuleb kasutada õigussüsteemi *ultima ratio*'t: karistusõigust.

KAPO sõnul on kriminaalmenetluse näol tegemist efektiivse meetmega, mille tähtsust on tajutud viimastel aastatel lääneriikides laiemalt. Kriminaalmenetlust kasutavad spionaaži tõkestamiseks Eesti, Läti ja Leedu, aga ka Ameerika Ühendriigid ja Ukraina. Ka riikides, kus varasemalt püüti tekkinud olukordi lahendada mitteavalike meetmetega[21], on hakatud riigireetureid ja agente aina enam vangistama. KAPO järeldab, et praegusel hetkel pole lääneriikides kriminaalmenetlus spionaažis vahelejäänu jaoks enam „hüpoteetiline võimalus, vaid pigem oodatav reaalsus".[22]

---

[15] Mõningad näited Hiina näited on leitavad magistritöö tööstusspionaaži meetodite alapeatükist.
[16] JAS§ 2 lg 1, § 6 p 2; Julgeolekuasutuste seadus (JAS). – RT I, 14.03.2023, 25.
[17] Teabehanke mõiste tuleneb JAS § 9 lg-s 2 kasutatavast mõistest „riigi julgeolekuteabe hanke ja analüüsi kava". Põhiõiguste piiramise alused on sätestatud JAS §-des 25 ja 26. Meetodid ja vahendid kehtestab JAS § 28 alusel asjaomane minister. KAPO puhul: Siseministri 6. juuni 2001 määrus nr 76 „Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord". – RT I, 02.08.2017, 7.
[18] VSS § 5;Väljasõidukohustuse ja sissesõidukeelu seadus (VSS). – RT I, 06.07.2023, 125.
[19] VSS § 6 lg 1.
[20] RSVS § 47 jj; Riigisaladuse ja salastatud välisteabe seadus (RSVS). – RT I, 12.12.2024, 11; Seonduvalt tööstusspionaažiga: Hollandi valitsus käis hiljuti välja idee kohaldada julgeolekukontrolli tundlikes valdkondades tegutsevatele teadlastele: Cokelaere, H. Dutch government plans to screen scientists for national security risks. Politico 07.04.2025. – https://www.politico.eu/article/dutch-government-scientists-tech-national-security-espionage/ (09.04.2025). Mõned päevad enne Politico artikli ilmumist astus Hollandis kohtu ette Venemaa kodanik, keda kahtlustatakse ärisaladuste varguses Hollandi ettevõttest ASML, mis on üks maailma juhtivaid kiipide tootmisaparatuuri valmistajaid: van der Klundert, M. jt. AIVD: opgepakte werknemer ASML had contact met Russische geheime dienst. NOS 06.02.2025. – https://nos.nl/nieuwsuur/artikel/2554733-aivd-opgepakte-werknemer-asml-had-contact-met-russische-geheime-dienst (09.04.2025); Thomson, I. Ex-ASML, NXP staffer accused of stealing chip secrets, peddling them to Moscow. The Register 04.04.2025. – https://www.theregister.com/2025/04/04/amsl_russian_spy/ (09.04.2025).
[21] Vt Viini konventsiooni Art 9 lg 1, mille alusel on võimalik kuulutada välisriigi diplomaat vastuvõetamatuks ehk *persona non grata*'ks: Diplomaatiliste suhete Viini konventsioon. – RT II 2006, 16, 0.
[22] Klemm, J. (koost). KAPO aastaraamat 2022–2023, lk 20.

Võttes arvesse, et tööstusspionaaž on üks spionaaži liike, tekib küsimus, kas ka tööstusspioonide heidutamiseks oleks tarvis kasutada karistusõiguslikke meetmeid? Just sellisele järeldusele on jõudnud Ameerika Ühendriikide[23] ja Suurbritannia[24] seadusandjad, kuivõrd tööstusspionaaž on nendes õiguskordades sõnaselgelt kriminaliseeritud.[25] Võrdlusena, Eesti seadusandja pole sätestanud ei majandus- ega ka tööstusspionaaži legaaldefinitsiooni. Tõsi, Mandri-Euroopa kontekstis ei ole selline seis sugugi anomaalne. S. Carl jt on täheldanud, et ainult nelja Euroopa Liidu liikmesriigi (Leedu, Holland, Poola ja Ungari) õiguskorras on tööstusspionaaži legaaldefinitsioon ning ainult kolmes riigis (Leedu, Holland ja Ungari) majandusspionaaži legaaldefinitsioon.[26] Majandus- ja tööstusspionaaži legaaldefinitsioonid puuduvad isegi Saksamaa õiguskorrast. Mis muidugi ei tähenda, et Saksamaal ei pandaks toime kõnealuseid kuritegusid või et toimepanijaid poleks võimalik vastutusele võtta.[27]

Karistusseadustikus[28] puudub tööstusspionaaži koosseis, mistõttu püstitan hüpoteesi, et tööstusspionaaž ei ole Eesti õiguskorras karistatav.

Et hüpoteesi ümber lükata tuleks eelkõige teha selgeks, mis on tööstusspionaaž? See aga eeldab, et sisustame luuretegevuse mõiste, eristame luuretegevust spionaažist ning tööstusspionaaži majandus- ja ärispionaažist. Samuti tuleks uurida, milliseid esemeid ja millistel meetoditel tööstusspioonid ründavad, ning milliseid õigushüvesid nad selle käigus ohustavad: kas kollektiivseid õigushüvesid nagu riigi julgeolek? Või hoopis individuaalseid õigushüvesid nagu omand, ettevõtlusvabadus jt põhiõigused? Ebaselgust suurendab fookus kaitsetööstusel, kus avalik huvi ja erahuvi on omavahel tihedalt läbipõimunud. Mõistmaks kaitsetööstusega kaasnevaid omapärasid tuleks sisustada ka kaitsetööstuse mõiste.

---

[23] Economic Espionage Act of 1996. Public Law 104–294 (11.10.1996).
– https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf (15.11.2024).
[24] National Security Act 2023, Section 2. (11.07.2023).
– https://www.legislation.gov.uk/ukpga/2023/32/section/2 (15.11.2024).
[25] Tõsi, *Economic Espionage Act* kasutab mõistet majandusspionaaž. *National Security Act 2023* kasutab üldmõistet *espionage* eristades erinevaid ründeobjekte: *protected information*, *trade secrets*. Mõisteline arutelu jätkub magistritöö kolmandas peatükis.
[26] Carl, S., Kilchling, M., Knickmeier, S., and Wallwaey, E. (2017). Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa. Schriftenreihe Forschung aktuell des Max-Planck-Instituts für ausländisches und internationales Strafrecht Band 49, lk 95. (Viidatud: Button, M., Knickmeier, S. Economic and Industrial Espionage: Characteristics, Techniques and Response. – The Handbook of Security (ed. M. Gill) Springer 2022).
[27] Näiteid Hiina spionaažist Saksamaal: Deutsche Welle. Chinese cyberattacks hit nearly half of German firms, study. (28.08.2024). – https://www.dw.com/en/chinese-cyberattacks-hit-nearly-half-of-german-firms-study/a-70070417 (10.02.2025). Asjakohastest sätetest Saksa õiguskorras: vt käesoleva magistritöö majandus-, tööstus- ja ärispionaaži mõistete alapeatükk.
[28] Karistusseadustik (KarS). – RT I, 12.12.2024, 6.

Kui leiame, et tööstusspionaaži ründeobjektide hulka ei kuulu ainult riigisaladus, vaid ka selle eraõiguslik analoog ärisaladus, tekib küsimus, kas karistusseadustik kaitseb ka ärisaladust? Ja kui, kas kaitse on võrreldav salastatud teabe kaitsega? Ärisaladuse karistusõiguslik kaitse on oluline, kuna mitte kõik kaitsetööstuse ettevõtjad ei vaja või soovi juurdepääsu salastatud teabele.

Eesti Kaitse- ja Kosmosetööstuse Liitu (EKTL) kuuluva äriühingu CybExer Technologies[29] juhatuse liige ja endine kaitseministeeriumi kantsler Lauri Almann on teadlikult vältinud kokkupuudet salastatud teabega.[30] Esiteks kulutab salastatud teabe kaitsmine ja töötlemine aega ja raha, mis ei ole kooskõlas kiiresti kasvava äriühingu vajadustega.[31] Teiseks tähendab kokkupuude salastatud teabega piiranguid, mis vähendavad ettevõtte turuväärtust. [32] Kolmandaks, kuna riigisaladusega kaitstakse[33] julgeolekut kui avalikku hüve, võib riigisaladus muutuda survevahendiks; juhul kui avaliku hüve asemel asuvad domineerima erahuvid, nt võimupartei soov nõrgestada poliitilisi vastaseid.[34] Võttes arvesse piirangutega kaasnevat kulu ei pruugi olla kasu väidetavast konkurentsieelisest, mida annab võimalus osaleda hangetel, mis nõuavad kokkupuudet salastatud teabega, nagu väidab KAPO.[35]

Veel: kaitsetööstuses arendatakse aina enam kahesuguse kasutusega tooteid ehk tooteid, mida kasutatakse nii tsiviil- kui ka sõjalisel otstarbel. K. Tammai sõnul on tegemist äristrateegiaga, mille raames arendatakse esmalt toode tsiviilkasutuseks ja seejärel üritatakse seda müüa

[29] CybExer Technologies. – https://cybexer.com/ (08.02.2025).
[30] Priit Pruksi intervjuu Lauri Almanniga, 27.01.2025. L. Almanni seisukohtadega nõustuvad suures osas kõik intervjueeritud kaitsetööstuse äriühingute esindajad.
[31] Samas.
[32] Samas.
[33] KAPO 2016. aasta aastaraamatus (lk 16) väidetakse „Riigisaladus kuulub alati riigile“. Endine riigiprokurör I. Ombler: „Kõigile riigisaladusega kokkupuutujatele väärib siinkohal meeldetuletamist tõsiasi, et riigisaladus kuulub alati riigile.“ [Prokuratuuri aastaraamat 2017. Inna Ombler: on spioone, kes kinnipidamisest kergendust tunnevad. – https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2017/inna-ombler-spioone-kes-kinnipidamisest-kergendust-tunnevad (04.03.2025)] Kaitsepolitseinik K. Virks: „Võib-olla ta on muutunud liiga mugavaks, arvab, et tema on selle teabe ka koostanud, järelikult on ka teabe omanik. Tegelikult ei ole, riigisaladuse omanik on alati riik.“ (Pihl, K. „Pealtnägija“: miks ja milliseid riigijuhtide saladusi kaitsepolitsei kogub? ERR 13.03.2019. – https://www.err.ee/919467/pealtnagija-miks-ja-milliseid-riigijuhtide-saladusi-kaitsepolitsei-kogub (06.05.2025)) Juriidiliselt ei ole see päris korrektne. Tegemist ei ole tähenärimisega, vaid see on oluline ka magistritöö raames. Isik, kes leiutab riigikaitselise leiutise (RSVS § 7 p 6), või kaitsetööstuse äriühing, kes arendab välja sõjalise otstarbega asja (RSVS § 7 p $6^1$), säilitab isegi pärast mainitud esemete salastamist oma omandiõiguse. Ehk siis: salastatus ei mõjuta omandiõigust. Riigisaladus ei kuulu alati riigile.
[34] Priit Pruksi intervjuu Lauri Almanniga.
[35] Kaitsepolitseiamet. Mida peaks teadma tööstusspionaažist? – https://web.archive.org/web/20191103141731/https:/www.kapo.ee/et/content/mida-peaks-teadma-t%c3%b6%c3%b6stusspionaa%c5%beist.html (08.02.2025).

riikidele.[36] Selle valdkonna teerajajaks on endise Ameerika Ühendriikide kaitseministri Ashton Carteri initsiatiivil loodud *Defense Innovation Unit*, mis hangib kaitseministeeriumile innovatsioonikeskustest (nt Silicon Valley) tsiviil- ja kahesuguse kasutusega tooteid lahendamaks julgeolekuga seonduvaid väljakutseid.[37] Kahesuguse kasutusega toodete arendamine on ka NATO ja Euroopa Liidu üks eesmärkidest.[38] Eesti kaitsetööstusest võiks esile tuua aktsiaselts Cybernetica mereseiretehnoloogiad, mis äriühingu juhatuse liikme Oliver Väärtnõu sõnul on liikunud ajapikku tsiviilkasutusest sõjalisse kasutusse.[39] Kuigi kahesuguse kasutusega tooteid arendavad äriühingud ei pruugi puutuda kokku salastatud teabega, vääriksid nad siiski võrdväärset karistusõiguslikku kaitset kaitsetööstuse äriühingutega, mis töötlevad salastatud teavet.

Seetõttu tuleb küsida: millise karistusseadustiku koosseisu kaitsealasse kuulub kaitsetööstuse äriühingu ärisaladus? Kas KarS § 377, millega kaitstakse „äriühingute majandustegevust“[40]? Või hoopis KarS § 234[2], millega kaitstakse „Eesti Vabariigi julgeolekut“[41]?

KarS § 234[2] lg 1 tõlgendamist raskendab asjaolu, et kõik kohtumenetlused[42] kõnealuse sätte alusel – peale ühe[43] – on lõppenud kokkuleppemenetlusega, kus kohtunik on KrMS[44] § 408[1] lg 4 alusel avalikustanud otsuse jõustumisel vaid lahendi sissejuhatuse ja resolutiivosa. Ainukesed

[36] Martinson, A., Tammai, K., Mikheim, V. The Reality and Challenges of Building Defense Technologies. Startup Day, Tartu, 30.01.2025.
[37] Defense Innovation Unit. – https://www.diu.mil/ (10.02.2025). Vt ka: Shah, R. M; Kirchhoff, C. Unit X: How the Pentagon and Silicon Valley Are Transforming the Future of War. Scribner 2024.
[38] Baldwin, H. Critical Dual-Use Technologies: Commercial, Regulatory, Societal and National Security Challenges. General Report. NATO Parliamentary Assembly 26.08.2024. – https://www.nato-pa.int/download-file?filename=/sites/default/files/2024-12/051%20ESC%2024%20E%20rev.2%20fin%20-%20CRITICAL%20DUAL-USE%20TECHNOLOGIES%20-%20BALDWIN%20REPORT.pdf (10.02.2025); NATO. Emerging and disruptive technologies. (08.08.2024).
– https://www.nato.int/cps/fr/natohq/topics_184303.htm?selectedLocale=en (10.02.2025); NATO DIANA. – https://www.diana.nato.int/ (10.02.2025); European Commission. On options for enhancing support for research and development involving technologies with dual-use potential. White Paper. (24.01.2024) – https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec_rtd_white-paper-dual-use-potential.pdf (10.02.2025).
[39] Priit Pruksi intervjuu Oliver Väärtnõuga, 09.04.2025.
[40] Vutt, A. KarS komm § 377, p 1. – Karistusseadustik. Komm vlj. 5. vlj. Tallinn: Juura 2021.
[41] Kiris, R., Kärner, M. KarS komm § 234[2], p 1.
[42] Harju Maakohtu lahendid: 1-24-2828/10, 1-24-2627/6, 1-24-2429/9, 1-21-1256, 1-19-6812.
[43] Prokuratuur taotles ka selle kohtumenetluse raames avalikkuse piirangut ja otsuse jõustumisel vaid lahendi sissejuhatuse ja resolutiivosa avalikustamist (RKKKo 1-21-1421, p 27). Riigikohus aga leidis: „G. Mutso süüdimõistmise põhjuste täielik varjamine riivaks siiski liiga suurel määral PS § 24 lg-st 4 tulenevat kohtuotsuse avalikkuse põhimõtet. Kohtuotsuse avaldamispiirangute üle otsustamisel ei saa jätta arvesse võtmata, et käesoleva kriminaalasja vastu on õigustatud avalik huvi (vrd ka RKKKm 04.12.2020, 1-17-9149/626, p 12).“ (RKKKo 1-21-1421, p 144)
[44] Kriminaalmenetluse seadustik (KrMS). – RT I, 12.12.2024, 7.

suunanäitajad mõiste „teave“ sisustamisel on 642 SE seletuskiri[45], RKKKo 1-21-1421, ning Saksamaa karistusseadustiku (sks *Strafgesetzbuch*, StGB[46]) § 99, mis oli aluseks[47] KarS § 234[2] vastuvõtmisel.

S. Hegmann ja F. Stuppi möönavad, et piir StGB § 99 ja „konkurentsispionaaži“ (sks *Konkurrenzspionage*) koosseisu – ehk Eesti näitel KarS § 234[2] ja § 377 – vahel on hägune.[48] Autorite sõnul on puutumus riigi julgeolekuga tugev muuhulgas kõrgtehnoloogia ülekande ja relvakaubanduse valdkondades.[49]

642 SE seletuskirja järgi on teabe mõistega KarS § 234[2] tähenduses hõlmatud „nii avalik teave, asutusesiseseks kasutamiseks mõeldud teave kui ka riigisaladus ja salastatud välisteave“[50]. Seletuskiri täpsustab, et sätte eesmärk on kriminaliseerida olukorrad, kus „välisriigi luure- või julgeolekuteenistus või selle huvides või ülesandel tegutsev isik kogub infot mittesalajaste valdkondade kohta“[51]. Seletuskiri tugineb KAPO aastaraamatus kajastatud juhtumitele, millest ilmneb, et „välisluure huvi võib seisneda ka Eesti riigi otsuste ja siinse olukorra mõjutamises ja seaduse mõttes mittesalajase või asutusesiseseks kasutamiseks mõeldud teabe või avaliku teabe hankimises (nt krediidiasutuste andmebaasid, töötamise registri andmed, isikute taustaandmed, isiklikud ja tööalased e-kirjad või suhtlusringkond, teatud objektide asukohad, sõjaväekolonnide liikumised, elutähtsate teenuste toimepidavus jne)“[52].

Seletuskirjast nähtub, et teabe mõistega on püütud hõlmata võimalikult laia esemete ringi. Ainuke kriteerium on, et teabe kogumine oleks „Eesti Vabariigi julgeoleku vastane tegevus“. Mainitud mõistet ei ole seletuskirja kohaselt „võimalik ammendavalt defineerida ning see on ajas muutuv mõiste, mis sõltub riiki ähvardavatest julgeolekuohtudest ning riigi julgeolekupoliitikast“[53].

[45] 642 SE. Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (terrorismivastase võitluse direktiivi ülevõtmine) eelnõu seletuskiri. Vastu võetud 19.12.2018. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/af992ccb-58f7-4a6e-bef5-d8f82772b3b7/karistusseadustiku-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus-terrorismivastase-voitluse-direktiivi-ulevotmine/ (09.04.2025).
[46] Strafgesetzbuch (StGB). BGBl. 2024 I Nr. 109.
[47] 642 SE seletuskiri, lk 6.
[48] StGB-MK, § 99 vnr 22. – Münchener Kommentar zum StGB. 4. Auflage. München: Beck 2021.
[49] Samas.
[50] 642 SE seletuskiri, lk 6.
[51] Samas, lk 4.
[52] Samas. Viidatakse KAPO 2013. ja 2014. aastaraamatu välisluure peatükkidele.
[53] Samas.

Eelnevale tuginedes sõnastan magistritöö teise hüpoteesi järgmiselt: kaitsetööstuse äriühingu ärisaladus on teave KarS § 234[2] lg 1 mõttes.

Väitele saab vastu vaielda kolmel põhjusel. Esiteks, ärisaladust ei mainita kordagi seletuskirja näidisloetelus.[54] Teiseks, seletuskirja mittesalajase teabe näidisloetelu iseloomustab riigikeskne käsitlus. Sellest annavad märku teabe jagamine avalikuks teabeks, asutusesiseseks kasutamiseks mõeldud teabeks, riigisaladuseks ja salastatud välisteabeks.[55] Kõik need on terminid, mis tulenevad haldusõiguslikest õigusaktidest. Täpsemalt, avaliku teabe seadusest[56] (§§ 3, 34 jj) ning riigisaladuse ja salastatud välisteabe seadusest (§ 3 p 1-2). Kolmandaks, KarS § 234[2] asub karistusseadustiku riigivastaste süütegude peatüki Eesti Vabariigi vastaste süütegude jaos. R. Kirise ja M. Kärneri järgi on KarS §-ga 234[2] kaitstav õigushüve Eesti Vabariigi julgeolek.[57]

KarS § 234[2] eesmärk on kaitsta riiki ja täpsemalt Eesti Vabariigi julgeolekut, mistõttu on põhjus küsida, miks peaks ärisaladus kuuluma KarS § 234[2] kaitsealasse? Sest tegutseb äriühing kui eraõiguslik juriidiline isik ju erahuvides (TsÜS[58] § 25 lg 1, ÄS[59] § 2 lg 1). Samuti on ärisaladuse üheks olemuslikuks tunnuseks „kaubanduslik väärtus oma salajasuse tõttu“ (EKTÄKS[60] § 5 lg 2 p 2). Miks peaks Eesti Vabariigi julgeolekut kaitsev karistusõiguslik norm kaitsma äriühingule kuuluva eseme kaubanduslikku väärtust?

Tõsi, 642 SE seletuskirja näidisloetelus mainitakse ka „krediidiasutuste andmebaase“, „tööalaseid e-kirju“ ja „elutähtsate teenuste toimepidevust“, mis annab märku, et seadusandja on tajunud, et ka äriühingute valduses võib olla võõrriigile huvipakkuvat teavet, mis väärib riigipoolset kaitset.[61] Samuti ligendab era- ja avalikku huvi magistritöö teise hüpoteesi rõhuasetus kaitsetööstusele. Seda põhjusel, et kaitsetööstuse äriühingu klientideks on eranditult riigid.[62] G. Allen ja D. Berenson väidavad, et Ameerika Ühendriikide kaitsetööstusbaas

[54] 642 SE seletuskiri, lk 4.
[55] Samas, lk 6.
[56] Avaliku teabe seadus (AvTS). – RT I, 30.12.2024, 5.
[57] Kiris, R., Kärner, M. KarS komm § 234[2], p 1; 642 SE seletuskiri, lk 4.
[58] Tsiviilseadustiku üldosa seadus (TsÜS). – RT I, 31.12.2024, 48.
[59] Äriseadustik (ÄS). – RT I, 06.07.2023, 131.
[60] Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus (EKTÄKS). – RT I, 07.12.2018, 2.
[61] 642 SE seletuskiri, lk 4.
[62] Nicastro, L.A. The U.S. Defense Industrial Base: Background and Issues for Congress. Congressional Research Service. Summary. Uuendatud 23.09.2024, lk 6 – https://crsreports.congress.gov/product/pdf/R/R47751 (15.01.2025). Tsitaat: „*Compared to other parts of the U.S. economy, the commercial defense industry is unique in several important ways. Because the federal government is effectively the only buyer for most defense products*

(*Defense Industrial Base, DIB*) on sisuliselt isoleeritud ülejäänud majandusest, kuivõrd sinna kuuluvate äriühingute kliendiks on ainult riik.[63] Ühtlasi on maailmapraktikas – kuid mitte Eestis[64] – levinud riigi osalusega kaitsetööstuse äriühingud.[65]

Kuigi määratlemata õigusmõistete nagu „Eesti Vabariigi julgeolek" ja „teave" kasutamine ei väära riigikohtu käsitluse[66] kohaselt kooskõla määratletuspõhimõttega, on õigusselguse ja laiemalt õigusriikluse huvides, et ka valgustkartvates valdkondades nagu seda on riigivastaste kuritegude menetlemine säiliks akadeemiline huvi sõnade tähenduse vastu. KarS § 234[2] asetseb riigivastaste süütegude peatükis, mistõttu kui asjaomase normiga kaitstakse ka äriühingu ärisaladust peab olema selge, milline on seos äriühingu ärisaladuse ja riigi julgeoleku vahel. Teisisõnu, KarS § 234[2] kaitsealasse peaks kuuluma ainult selline teave, mille sattumine võõrriigi valdusesse kujutab selget ohtu Eesti Vabariigi julgeolekule.

Hüpoteesi kinnitamine või ümberlükkamine nõuab arusaama, mida peab õiguskord ärisaladuseks ja mida peetakse praktikas kaitsetööstuse äriühingu ärisaladuseks. Seejärel tuleb luua tõsikindel seos kaitsetööstuse äriühingu ärisaladuse ja riigi julgeoleku mõistete vahel.

Esimese hüpoteesi käsitlemisel kasutan kvalitatiivset, empiirilist ja võrdlevat meetodit, et selgitada välja tööstusspionaaži mõiste sisu ja seostada mõiste asjakohase karistusseadustiku normiga. Allikate osas tuginen: 1) ajakirjandusväljaannetele; 2) riigiasutuste pressiteadetele, aastaraamatutele, uuringutele ja muudele dokumentidele; 3) teaduskirjandusele; 4) Eesti, Ameerika Ühendriikide ja Saksamaa õigusaktidele ning Ameerika Ühendriikide kohtupraktikale. Ajakirjanduse kaasamine on vajalik, kuna spionaaži puudutav faktoloogia ei pruugi alati jõuda kohtulahenditesse või julgeolekuasutuste avalikesse materjalidesse.[67]

---

*and services, the commercial DIB may be described as a monopsony market.*" Vt ka: Carril, R., Duggan, M. The Impact of Industry Consolidation on Government Procurement: Evidence from Department of Defense Contracting. – National Bureau of Economic Research, October 2018, lk 28;

[63] Allen, G.; Berenson, D. Why is the U.S. Defense Industrial Base So Isolated from the U.S. Economy. CSIS (August 20, 2024). – https://www.csis.org/analysis/why-us-defense-industrial-base-so-isolated-us-economy (22.04.2025).

[64] Hiljuti andis valitsus rahandusministrile volituse luua äriühing, mis hakkab tootma sõjalist lõhkeainet: ERR. Riik asutab põlevkivist lõhkeaine tootmiseks ettevõtte Hexest. (24.04.2025). – https://www.err.ee/1609673597/riik-asutab-polevkivist-lohkeaine-tootmiseks-ettevotte-hexest (24.04.2025). Kuna tegemist on võrdlemisi diferentseerimata tootega on tööstusspionaaži oht sellises ettevõttes võrdlemisi väike.

[65] Priit Pruksi intervjuu Kalev Koidumäega, 01.04.2025.

[66] RKKKo 1-22-3155, p 40; RKKKo 1-16-10888/62, p 48.

[67] Minu hinnangul ei jää julgeoleku teemadele spetsialiseerunud ajakirjanike kirjutised kvaliteedi poolest alla teadusartiklitele ning võivad olla ühiskonnale isegi väärtuslikumad kui kitsale ringile suunatud teadusartiklid. Näiteks, Venemaa sõjaväeluure tegevust uuriv Ameerika ajakirjanik Michael D. Weiss sai 2025. aastal president Alar Kariselt teenetemärgi. Eesti ajakirjanikest on julgeolekualaste kirjutistega silma paistnud Holger Roonemaa.

Ameerika Ühendriikide kohtupraktika kaasamise eesmärk on anda võimalikult lühike ent laiapõhjaline ülevaade tööstusspionaaži meetoditest ja nende meetodite rakendamise käigus täidetavatest karistusõiguslikest koosseisudest. Ameerika Ühendriikide õigusaktide ja kohtupraktika kasutamist õigustab asjaolu, et Ühendriigid on sõnaselgelt kriminaliseerinud ärisaladuse varguse (*theft of trade secrets*) ja majandusspionaaži (*economic espionage*).[68] Samuti on Ühendriikide näol tegemist maailma võimsaima (kaitse)tööstusriigiga, mis on olnud tööstusspioonide sihtmärk alates vähemalt teisest maailmasõjast.[69] Mäletatavasti hukati külma sõja ajal Julius ja Ethel Rosenberg, kes mõisteti süüdi vandenõus panna toime spionaažikuritegu. Nimelt aitasid Rosenbergid edastada tuumarelvaga seotud salastatud teavet Nõukogude Liidule.[70] J. J. Fialka eristab kolme Ameerika Ühendriikide vastast tööstusspionaaži lainet vahemikus 1950–1996: Venemaa, Jaapan ja Hiina.[71] Seega on Ameerika Ühendriikide julgeolekuasutustel selles vallas laialdased teadmised.[72]

Teise hüpoteesi käsitlemisel kasutan samuti kvalitatiivset, võrdlevat ja empiirilist meetodit. Eesti Vabariigi julgeoleku, kaitsetööstuse ja ärisaladuse mõistete avamisel kasutan kõiki ülalmainitud allikaid ning poolstruktureeritud[73] intervjuusid EKTL-i ja kaitsetööstuse äriühingute[74] esindajatega. Samuti aitavad intervjuud mõista kaitsetööstuse eripärasid ning seostada ärisaladuse ja julgeoleku mõisteid. Äriühingute valikul lähtusin valdkondadest, millel on minu hinnangul kõige tugevam seos Eesti Vabariigi julgeolekuga: 1) eelhoiatus; 2) vastuluure; 3) otsene sõjaline tegevus; 4) piirivalve; 5) küberkaitse ja küberturvalisus.

---

Veel mainin isiklikku tähelepanekut, et luure- ja vastuluurealaseid teadusartikleid tükivad kirjutama pigem analüütikud kui need, kes tegelevad operatsioonidega. Eriteenistuste ametnikud, kes tegelevad operatsioonidega, kirjutavad pigem memuaare või astuvad üles taskuhäälingutes. Seetõttu olen erandkorras viidanud mõningates kohtades ka mitteteaduslikele materjalidele, nt taskuhäälingutele.

[68] 18 U.S. Code § 1831-39.

[69] USA vastu suunatud tööstusspionaaži kohta vt lähemalt: Lotrionte, C. Countering State-Sponsored Cyber Economic Espionage Under International Law. – North Carolina Journal of International Law 2017/40, No 2, lk 467 jj.

[70] U.S. Department of Energy. The Manhattan Project. Espionage and the Manhattan Project (1940–1945). – https://www.osti.gov/opennet/manhattan-project-history/Events/1942-1945/espionage.htm (06.03.2025); FBI. Atom Spy Case/Rosenbergs. – https://www.fbi.gov/history/famous-cases/atom-spy-caserosenbergs (06.03.2025).

[71] Fialka, J. J. War by Other Means: Economic Espionage in America. W W Norton & Co 1997, lk 9–13. (Viidatud: Lotrionte, C., nr. 86)

[72] Suurenenud majandus- ja tööstusspionaaži ohu tõttu on Föderaalne Juurdlusbüroo (FBI) laiendanud teavitustööd, sh valmistanud tõestisündinud juhtumi põhjal lühikese linateose nimega „*The Company Man: Protecting America's Secrets*". Vt lähemalt: FBI. Economic Espionage. FBI Launches Nationwide Awareness Campaign (23.07.2015). – https://www.fbi.gov/news/stories/economic-espionage (04.02.2025).

[73] Virkus, S. Intervjuu, vaatlus ja sisuanalüüs. Intervjuu liigid. Tallinna Ülikool (2016). – https://www.tlu.ee/~sirvir/Intervjuu_vaatlus_ja_sisuanals/intervjuu_liigid.html (03.04.2025).

[74] Cybernetica, CybExer Technologies, Defsecintel, Defensphere, Milrem ja Sensus Septima.

Äriühingute valimi piiratus on tingitud ajalistest piirangutest ning asjaolust, et kõigi soovitud äriühingutega ei olnud võimalik vestelda.

KarS § $234^2$ lg-s 1 sätestatud teabe mõiste sisustamisel kasutan Eesti kohtupraktikat. Mõnede julgeolekualaste teemade käsitlemisel tuginen poolstruktureeritud intervjuudele endise KAPO peadirektori Arnold Sinisaluga ja struktureerimata intervjuule anonüümseks jääva endise luureametnikuga. Ettepanekute tegemisel karistusseadustiku täiendamiseks viitan ka Taiwani õiguskorrale. Seda põhjusel, et Hiina tööstusspionaaži-kampaania[75] ohjeldamiseks on Taiwan karmistanud tööstusspionaaži koosseisu sätestades „riikliku võtmetehnoloogia“ [76] (*national core key technology*) mõiste.[77]

Magistritöö on jaotatud neljaks osaks. Esimeses osas selgitatakse tööstusspionaaži uurimise hetkeseisu ja tähtsust. Teises osas avatakse kaitsetööstuse mõiste. Kolmandas käsitletakse tööstusspionaaži mõistet ning tuvastatakse karistusseadustikust õigusnormid, mille alusel on võimalik karistada isikuid tööstusspionaaži kuriteo eest. Neljandas osas otsitakse vastust küsimusele, kas kaitsetööstuse äriühingu ärisaladus on teave KarS § $234^2$ lg 1 tähenduses.

Magistritöö eesmärgiks on parandada ühiskonna luurealast haritust ning edendada eestikeelset julgeolekualast õigusteadust.

Magistritööd iseloomustavateks märksõnadeks on kaitsetööstus, tööstusspionaaž, vastuluure, riigivastased süüteod, julgeolek.

[75] Lotrionte, C., lk 451 jj.
[76] National Security Act. Executive Yuan. (08.06.2022). – https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030028 (05.03.2025);
[77] Seda enam, et endise CIA direktori William Burnsi väitel kinnitab USA luureinfo Xi Jinpingi juhist Hiina rahvaarmeele olla valmis Taiwani vallutamiseks 2027. aastal: Brennan, M. Transcript: CIA director William Burns on „Face the Nation“, Feb. 26, 2023. CBS News. – https://www.cbsnews.com/news/william-burns-cia-director-face-the-nation-transcript-02-26-2023/ (06.03.2025). Tsitaat: *„We do know, as has been made public, that President Xi has instructed the PLA, the Chinese military leadership, to be ready by 2027 to invade Taiwan, but that doesn't mean that he's decided to invade in 2027 or any other year as well.“*

# 1. Tööstusspionaaži uurimise hetkeseis ja tähtsus

Tööstusspionaaži ei ole Eesti õigusteaduses varem uuritud. Ainukese tööstusspionaaži-alase mitte-õigusteadusliku magistritöö on kirjutanud Erkki Koort, aga seda enam kui kakskümmend aastat tagasi ning fookusega riigisaladuse kaitsel.[78] Tartu Ülikooli õigusteaduskonnas ei ole kaitstud mitte ühtegi magistri- või doktoritööd, mille märksõnade hulka kuuluks tööstusspionaaž või tööstusluure.[79] Küll aga on Eestis kaitstud kaks magistritööd, mis käsitlevad spionaažikuritegusid laiemalt.[80]

Põgusalt käsitleb tööstusspionaaži Marta Mägi 2017. aasta magistritöös „Ärisaladuse kaitse karistusõigusliku regulatsiooni efektiivsus kehtivas õiguses“[81]. Kuid õigem oleks öelda, et M. Mägi magistritöö käsitleb ärispionaaži ehk olukorda, kus ärisaladuse omandamises ei osale võõrriigi eriteenistus.[82] Ühtlasi on magistritöö kirjutatud ajal, mil oht Venemaalt ja Hiinast oli oluliselt väiksem ning Eesti kaitsetööstuse areng oluliselt tagasihoidlikumas järgus. Seda näitab julgeolekukaalutluste puudumine Mägi töös ning rõhuasetus ettevõtjate ja töötajate õiguste tasakaalul.[83] Lisaks sellele, et vahepeal on tunnistatud kehtetuks tööstusspionaaži alapeatüki arutelu suunav seadusesäte Saksa õiguskorras (UWG[84] § 17 lg 2 p 1), puudus M. Mägi magistritöö avaldamise hetkel Eesti õiguskorrast KarS § $234^2$, mistõttu ei saanud üldse tekkida küsimust puutumusest KarS §-iga 377.

Põhjalikuma käsitluse ärisaladuse mõistest KarS § 377 lg 1 tähenduses annab Kertu Kirsipuu 2020. aasta magistritöös „Ärisaladuse mõiste KarS § 377 lg 1 sätestatud kuriteokoosseisu tunnusena“[85]. Mõnes kohas mainitakse ka selles töös tööstusspionaaži, kuid taaskord on

[78] Koort, E. Riigisaladus ja tööstusjulgeolek. Tallinna Tehnikaülikool 2004.
[79] University of Tartu. Digital Archive ADA. – https://dspace.ut.ee/browse/subject?scope=581ec471-a7cb-494a-a576-095050b702a4&bbm.page=1&startsWith=spionaa%C5%BE (10.02.2025).
[80] Purre, M. Riigireetmise ja salakuulamise regulatsioon Eesti karistusõiguses. Magistritöö. Tallinna Tehnikaülikool 2014; Võsaste, S. Kuriteo matkimise kasutamine riigivastaste süütegude ennetamisel. Magistritöö. Tartu Ülikool 2024.
[81] Mägi, M. Ärisaladuse kaitse karistusõigusliku regulatsiooni efektiivsus kehtivas õiguses. Magistritöö. Tartu: Tartu Ülikool 2017.
[82] Ärispionaaži mõiste kohta vt lähemalt käesoleva magistritöö alapeatükk 3.2.
[83] Mägi, M., lk 7.
[84] *Gesetz gegen den unlauteren Wettbewerb – UWG*. – https://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html (10.02.2025). Saksamaa õiguskorras on ärispionaaži karistusõiguslik kaitse nüüd GeschGehG §-s 23: https://www.gesetze-im-internet.de/englisch_geschgehg/englisch_geschgehg.html (10.02.2025).
[85] Kirsipuu, K. Ärisaladuse mõiste KarS § 377 lg 1 sätestatud kuriteokoosseisu tunnusena. Magistritöö. Tartu Ülikool 2020.

käsitlus napp ning põhineb ainult ühel allikal: KAPO.[86] Kuid ka selle töö puhul oleks õigem öelda, et käsitletakse ärispionaaži.

Isegi KAPO aastaraamatutes ja kodulehel leidub üllatavalt vähe teavet tööstusspionaaži kohta. Tõsi: 2021. aasta 18. jaanuarini oli KAPO kodulehel seda teavet oluliselt rohkem.[87] Selleks hetkeks oli tööstusspionaaži üksikasjalik käsitlus püsinud KAPO kodulehel vähemalt alates 2011. aastast.[88] Pärast 2021. aasta 18. jaanuari teave aga kadus. Võttes arvesse, et lisaks aastaraamatutele on koduleht teine foorum, kus Eesti tähtsaim vastuluureasutus suhtleb avalikkusega, võib spekuleerida, et ehk tähistab muutus kodulehe sisus ka muutust asutuse prioriteetides. Eraldi küsimus on, kas tööstusspionaaži-alase materjali kadumine tähendab, et võitlus tööstusspioonide vastu on muutunud vähem või rohkem tähtsaks?[89]

KAPO 2021–2022 aastaraamatu alapeatükk „Vaenulik huvi ärisaladuse vastu kasvab“ toetab viimast alternatiivi. KAPO kirjutab: „2021. aasta jooksul on kaitsepolitsei ka Eestis täheldanud võõrriikide kasvavat huvi tehnoloogilise oskusteabe vastu eelkõige strateegilistes ja kasvava nõudlusega kaupade tootmise sektoris. Huvipakkuvale infole juurdepääsuks kasutatakse nii tehnilisi vahendeid kui ka töötajaid.“[90]

Viimases aastaraamatus tunnistab KAPO, et „Eesti ettevõtete süvenev huvi panustada julgeoleku-, teadus- ja arendusprojektidesse [...] [on] Eesti ametkondadele [...] väljakutse“[91]. KAPO sõnul on Eestil vähe kogemust tööstusjulgeolekuga ehk „riiklikult oluliste hangete ja projektide süsteemse riskihaldusmudeliga“.[92] KAPO lisab, et Eestis tuleks „üle hinnata [...] kehtiv õiguskord, et ettevõtetel oleks selge ülevaade oma õigustest, kohustustest ja vastutusest“[93] ning et „[v]ajadus võib olla ka selgema raamistiku järele, mille alusel hinnata,

[86] Kirsipuu, L., lk 28.
[87] Võrdle: 18. jaanuar 2021: https://web.archive.org/web/20201021122615/https://www.kapo.ee/et/content/majandusjulgeolek.html ja https://web.archive.org/web/20191103141731/https://www.kapo.ee/et/content/mida-peaks-teadma-t%c3%b6%c3%b6stusspionaa%c5%beist.html. 20. jaanuar 2021 kuni tänaseni: https://web.archive.org/web/20210410221810/https://kapo.ee/et/content/majandusjulgeolek.html.
[88] Sama leht 2011. aastal: https://web.archive.org/web/20110909120145/http://www.kapo.ee/est/toovaldkonnad/majandusjulgeolek ja https://web.archive.org/web/20110909092048/http://www.kapo.ee/est/hea-teada/toostusspionaaz.
[89] Tänan Lauri Almanni, kes juhtis minu tähelepanu võimalusele, et info puudumine võib tähendada ka seda, et tööstusspionaaž tõusis KAPO prioriteetide nimekirjas kõrgemale mademele.
[90] KAPO aastaraamat 2021–2022, lk 40.
[91] KAPO aastaraamat 2024–2025, lk 34.
[92] Samas.
[93] Samas.

millised ettevõtted on sobilikud sellistes projektides osalema“[94]. KAPO väitel on paljudes Euroopa riikides tööstusjulgeolek „tagatud juba aastakümneid“[95]. Omalt poolt lisaksin, et ka Ameerika Ühendriikides kehtib juba aastakümneid tööstusjulgeolekuprogramm, mille üheks missiooniks on kindlustada, et erasektoris kaitstaks salastatud teavet sama tõhusalt kui riigisektoris.[96]

Ümberkorraldus kaitseministeeriumi juhtimises, millega luuakse eraldi kaitsetööstuse ja innovatsiooni asekantsleri ametikoht, annab märku, et tööstusspionaaž tõuseb ka kaitseministeeriumi prioriteetide nimekirjas.[97] Kantsler Kaimo Kuuski sõnul luuakse kantsleri alluvusse eraldi julgeoleku ja sisekontrolli osakond.[98] K. Kuusk leiab, et praegusel hetkel on kaitseministeeriumis sisekontroll „praktiliselt üldse puudu“ ja julgeolek on „alamehitatud“.[99] Riigi suurenenud huvi tõkestada tööstusspionaaži nähtub ka Vabariigi Valitsuse 2023–2027 tegevusprogrammi ülesandest 1.2.5 („Tugevdame luure ja vastuluure võimekusi ning vajadusel ajakohastame julgeolekuasutuste seaduse“). [100] Muuhulgas soovitakse ülesande raames muuta RSVS-i eesmärgiga „tugevdada tööstusjulgeolekut [...]“[101].

Välisluureamet ütleb 2024. aasta julgeolekuhinnangus: „Ettevõtted peavad üha enam kaitsma salastatud teavet vaenulike riikide tööstusluure eest ning riik kaitsma riigisaladust, mis usaldatakse välisettevõtetele.“[102] Samas annab KAPO hinnang 2021. aasta aastaraamatus alust kahelda ettevõtete võimekuses kaitsta end tööstusspionaaži eest. KAPO kirjutab: „Viimaste

[94] Samas.
[95] Samas.
[96] Vt lähemalt: 32 CFR part 117 ehk *National Industrial Security Program Operating Manual*. USA tööstusjulgeolekuprogrammi kõige olulisem lüli on DCSA (*Defense Counterintelligence Security Agency*), mis vastutab kaitseministeeriumiga koostööd tegevate ettevõtete tööstusjulgeoleku eest, ning mille praegune juht David Cattler töötas NATO peakorteris koos Välisluureameti peadirektori Kaupo Rosinaga. Seega, Eesti tööstusjulgeoleku raamistiku tarvis eeskujude ja parimate praktikate leidmisel ei tohiks tekkida takistusi. Vt: Defense Counterintelligence and Security Agency Strategic Plan 2025-2030. Introduction. Our Mission Areas. Industrial Security. – https://www.dcsa.mil/Portals/128/Documents/about/err/DCSA%202025-2030%20Strategic%20Plan.pdf (14.04.2025); LinkedIn. Kaupo Rosin. Recommendations. Given. – https://www.linkedin.com/in/kauporosin/ (14.04.2025).
[97] Kaitseministeerium. Kaitseministeerium saab kaitsetööstuse asekantsleri. (03.02.2025). – https://kaitseministeerium.ee/et/uudised/kaitseministeerium-saab-kaitsetoostuse-asekantsleri (04.02.2025)
[98] Samas.
[99] Hindre, M. Kuusk kaitseministeeriumist: sisekontrolli pole ja julgeolek on alamehitatud. ERR 04.02.2025. – https://www.err.ee/1609595108/kuusk-kaitseministeeriumist-sisekontrolli-pole-ja-julgeolek-on-alamehitatud (04.03.2025).
[100] Vabariigi Valitsuse 18. mai 2023. a korraldus nr 131 „Vabariigi Valitsuse tegevusprogrammi 2023–2027“ „kinnitamine“ muutmine. – RT III, 06.03.2024, 6.
[101] Samas.
[102] Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2024. – https://valisluureamet.ee/doc/raport/2024-et.pdf (28.10.2024), lk 87.

aastate kontrollide põhjal tuleb nentida, et julgeolekualaseid ohte ei teadvustata piisavalt, samuti on riigisaladuseks tunnistatud teabe kaitsmiseks ning füüsilise turvalisuse tagamiseks eraldatud ressursid ebapiisavad. Tihti näeme, et kehtivaid õigusakte ei järgita vajaliku hoolsusega. [...] Sageli tegutsetakse riigisaladuse kaitse korraldamisel n-ö mugavustsoonis. [...] Riigisaladuse kaitset korraldavad isikud täidavad seda ülesannet sageli põhitöö või muude tööülesannete kõrvalt, mistõttu ei pühendata sellele valdkonnale pahatihti piisavalt tööjõudu, -aega ega tehnilist ressurssi.“[103]

Tõsi on ka see, et mistahes kaitsemeetmed on kognitiivne ja materiaalne kuluartikkel ning kiirele kasvule orienteeritud kõrgtehnoloogiasektoris ei pruugi tootearenduse ja müügitöö kõrvalt kaitsemeetmete rakendamiseks alati ressurssi jätkuda.[104] K. Koidumäe ütleb, et külastades kaitsetööstuse iduühinguid ta ikka küsib: „Kas te õhtul ukse lukku panete?“[105] Samas tõdeb EKTL-i tegevjuht, et ajaga on olukord paranenud. Põhjuseks 2022. aastal alanud täiemahuline sõda Ukrainas, aga ka koolitused, mida korraldavad julgeolekuasutused.[106]

Kaitsetööstuse ettevõtjad kinnitavad, et tööstusspionaaž on julgeolekuoht.[107] „Meie vaatest ei ole selles küsimustki. Proovimine, sondeerimine käib pidevalt. Olgu see eraettevõtluse mängijate vahel või riikide vahel. Teabe ja tehnoloogia varastamine toimub kogu aeg,“ ütleb E. Kannike.[108] V. Naruskberg leiab, et ohu suurus sõltub toote uudsusest ja klientide iseloomust.[109] Kui pakutakse väga unikaalset toodet kaitseväele, on tööstusspionaaži oht keskmisest suurem.[110] Kõrgendatud ohust saab rääkida ka küber- või kosmosevaldkonnas, samuti toodete puhul, mida kasutatakse vee all.[111] V. Naruskbergi väitel huvitavad tööstusspioone tooted, mis

[103] KAPO aastaraamat 2021–2022, lk 25.
[104] USA, Suurbritannia, Kanada, Austraalia ja Uus-Meremaa ehk *Five Eyes* riikide julgeolekuastused on enda iduühingutele koostanud juhiste kogumiku nimega *Secure Innovation*, mis selgitab tehnoloogiaettevõtjatele ja investoritele, kuidas kaitsta end võõrriikide eriteenistuste eest. Vt lähemalt: National Protective Security Authority. – https://www.npsa.gov.uk/secure-innovation (15.11.2024); MI5. Security Service. Five Eyes launch drive to secure innovation. (17.10.2024). – https://www.mi5.gov.uk/news/five-eyes-launch-drive-to-secure-innovation (15.11.2024).
[105] Priit Pruksi intervjuu Kalev Koidumäega.
[106] Samas; Koolitustest: Kaitsepolitseiamet tegi 2024. aastal umbes 60 koolitust, kus osales kokku ligikaudu 1800 inimest. Vt lähemalt: KAPO aastaraamat 2024–2025, lk 34.
[107] Priit Pruksi intervjuud Lauri Almanni (Cybexer Technologies OÜ, 27.01.2025), Erik Kannike (Sensus Septima OÜ, 31.01.2025, 10.04.2025), Silver Lätti (Milrem AS, 28.01.2025), Oliver Väärtnõu (Cybernetica AS, 09.04.2025), Ingvar Pärnamäe (Defensphere OÜ, 15.04.2025), Viido Naruskbergi ja julgeolekueksperdiga (Defsecintel OÜ, 10.04.2025).
[108] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[109] Priit Pruksi intervjuu Viido Naruskbergi ja julgeolekueksperdiga.
[110] Samas.
[111] Samas.

annavad eelise turul ja lahinguväljal.[112] Võrdlusena, klassikalistes valdkondades nagu lõhkeaine tootmine on oht pigem väike.[113]

Tööstusspionaaži ohtu suurendab Eesti asukoht. Näiteks piirasid Ameerika Ühendriigid tehisintellekti arendamiseks oluliste kiipide eksporti osadesse Euroopa Liidu ja NATO liikmesriikidesse, sh Eestisse.[114] „Kui lased asju sisse osta Eestil, Ungaril ja Kreekal, siis võib-olla nad suunatakse vaikselt Hiina poole minema," spekuleerib Tallinna Tehnikaülikooli professor Tanel Tammet otsuse tagamaade kohta.[115] Samuti suurendab spionaažiohtu Eesti majanduse väiksusest tulenev vajadus keskenduda unikaalsete toodete arendamisele. Endise kaitseministeeriumi kaitseinvesteeringute asekantsleri Ingvar Pärnamäe sõnul ei ole Eesti kaitsetööstusel mõtet hakata tootma asju, mida toodetakse kuskil mujal paremini ja odavamini.[116] Eesti kaitsetööstus on täna tugev nišivaldkondades, mis olid katmata ja kus Eestil olid konkurentsieelised.[117] „Küberkaitse valdkond ei tekkinud ju õhust, vaid [...] 2007. aasta pronksiöö tulemusest. Ehk et, kus oli mingi reaalne kogemus, mida me saime maailma mastaabis rahaks teha," ütleb I. Pärnamäe.[118] RK otsuse 1-21-1421 kohaselt andis Hiina sõjaväeluure selge juhise oma agendile koguda teavet Eesti kübervaldkonna kohta.[119]

Endine kaitseministeeriumi kaitseinvesteeringute asekantsler I. Pärnamäe hindab Eesti võimekust tulla toime tööstusspionaažiga kehvaks.[120] Probleem on tema sõnul sügavam, kui KAPO hiljutises aastaraamatus serveeritud riskihaldusmudeli puudumine, ebaselgus õiguskorras või mõni muu tehniline nüanss.[121] KAPO sõnul[122] esitavad julgeolekualased arendusprojektid ametnikele väljakutse, aga I. Pärnamäe leiab[123], et probleem on hoopis

[112] Samas.
[113] Samas.
[114] Department of Commerce. Bureau of Industry and Security. Framework for Artifical Intelligence Diffusion. A Rule by the Industry and Security Bureau on 01/15/2025. Vt ka meediakajastust: ERR. Tsahkna kritiseeris Bideni valitsuse otsust piirata kiibieksporti Eestisse. (16.01.2025). – https://www.err.ee/1609577518/tsahkna-kritiseeris-bideni-valitsuse-otsust-piirata-kiibieksporti-eestisse (05.03.2025).
[115] ERR. Tammet: USA kiibipiirang Eestit ei mõjuta. 20.01.2025. – https://www.err.ee/1609581007/tammet-usa-kiibipiirang-eestit-ei-mojuta (18.04.2025).
[116] Kagge, R., Pärnamäe, I., Koidumäe, K. Väikeriigi suur võimalus. Eesti kaitsetööstuse juhid: on väga problemaatiline ja isegi ohtlik jääda lootma välisettevõtetele. Delfi (03.04.2025).
– https://forte.delfi.ee/artikkel/120368082/vaikeriigi-suur-voimalus-eesti-kaitsetoostuse-juhid-on-vaga-problemaatiline-ja-isegi-ohtlik-jaada-lootma-valisettevotetele (13.04.2025).
[117] Samas.
[118] Samas.
[119] RKKKo 1-21-1421, p 17 9).
[120] Priit Pruksi intervjuu Ingvar Pärnamäega.
[121] Samas; KAPO aastaraamat 2024–2025, lk 34.
[122] KAPO aastaraamat 2024–2025, lk 34.
[123] Priit Pruksi intervjuu Ingvar Pärnamäega.

ametnikes endis. „Tunnetus poliitikute poolt on teravam, et [kaitse]tööstuses võib-olla peitub midagi ja võib-olla seal on mingisuguseid asju, mida Eestil võiks olla vaja. Ametnike tasemel või ka kaitseväelaste või ka politseinike või piirivalvurite tasemel ma näen seda palju, palju vähem. See on imelik," ütleb I. Pärnamäe. „Tõsiseltvõetavat partnerlust [kaitsetööstuse ja riigi vahel] ei ole tekkinud."[124] Olgu öeldud, et I. Pärnamäe hinnang on vastuolus valitseva narratiiviga, mille kohaselt ametnikud eesotsas kaitseministeeriumi endise kantsleriga tahavad edendada riigikaitset, aga kaitseminister ei võta vedu.[125] I. Pärnamäe leiab, et tööstusspionaaži ohuga tegelemiseks tuleb ennekõike ära otsustada, kas kaitsetööstus on üldse strateegilise tähtsusega valdkond või lihtsalt osa tavamajandusest.[126] Kui kaitsetööstuse ettevõte on „nagu kiosk või Selveri pood", ei ole ka tarvidust seda kaitsta.[127]

Illustreerimaks tehnoloogilise eelise ja tööstusspionaaži tähtsust riigi julgeolekule ja geopoliitikale laiemalt tooksin kaks näidet Ukrainast. Esiteks, 2024. aasta aprilli seisuga hävitasid ukrainlased kaks kolmandikku Venemaa miljoneid dollareid maksvatest tankidest FPV (*first-person view*) droonidega tükihinnaga 400 dollarit (USD).[128] Teiseks, Venemaa pommitab Ukrainat ja hirmutab Ukraina liitlasi Orešniku ehk ülehelikiirusel liikuva ballistilise raketiga.[129]

„[M]e katsetame Orešniku raketisüsteemi vastusena NATO Venemaa-vastastele agressiivsetele tegevustele. [...] Me peame õigustatuks kasutada oma relvi sõjaliste objektide vastu, sellistes riikides, mis lubavad kasutada oma relvi meie objektide vastu", ütleb Putin ametlikus läkituses pärast Dnipro pommitamist Orešnikutega.[130] Kui uskuda president Trumpi ja tema endist julgeolekunõunikku John Boltonit, varastasid Venemaa tööstusluurajad rakettide

[124] Samas.
[125] Epner, E., Moora, E. „Ta on meie aja kangelane." Rahva ees säravale Pevkurile heidetakse ette suure plaani puudumist. – Eesti Ekspress 03.02.2025; Hõbemägi, P. Kusti Salm põhjendab kantsleri ametist lahkumist: „Kui me 1,6 miljardi eest laskemoona ei osta, siis oleme samas olukorras nagu 1939. aastal." – Postimees 12.06.2025.
[126] Priit Pruksi intervjuu Ingvar Pärnamäega.
[127] Samas.
[128] Detsch, J. Ukraine's Cheap Drones Are Decimating Russia's Tanks. Report. Foreign Policy 09.04.2024. – https://foreignpolicy.com/2024/04/09/drones-russia-tanks-ukraine-war-fpv-artillery/.
[129] Associated Press. Russia has used its hypersonic Oreshnik missile for the first time. What are its capabilities? (09.12.2024). – https://apnews.com/article/russia-oreshnik-hypersonic-missile-putin-ukraine-war-345588a399158b9eb0b56990b8149bd9 (04.02.2025); Antonov, D., Osborn, A. Russia says hypersonic missile strike on Ukraine was a warning to 'reckless' West. Reuters 22.11.2025. – https://www.reuters.com/world/europe/kremlin-says-hypersonic-missile-strike-ukraine-was-warning-west-2024-11-22/ (04.02.2025).
[130] Statement by President of the Russian Federation, 21.11.2024. – http://en.kremlin.ru/events/president/news/75614 (05.02.2025).

valmistamiseks vajaliku intellektuaalse vara ameeriklastelt.[131] Tänu tööstusspionaažile on Venemaal tuumarelvade kõrval veel üks vahend, millega külvata hirmu.

Kuid kaitsetööstust ei ohusta ainult vastaste eriteenistused. Tööstusspionaažiga tegelevad kõik riigid, sh liitlased. C. Lotrionte hinnangul on „hulgaliselt tõendeid", et lisaks Hiinale ja Venemaale üritavad ka Lõuna-Korea, Jaapan, Prantsusmaa, Iisrael ja Saksamaa hankida Ameerika Ühendriikidest ärisaladusi.[132] Endine Prantsusmaa välisluure (pr *direction générale de la sécurité extérieure*, DGSE) juht Pierre Marion ütleb: „[O]n rumal eksitus arvata, et oleme liitlased. Kui tegemist on äriga, oleme sõjas."[133] WikiLeaksi kaudu 2011. aastal lekitatud USA diplomaatilises läkituses ütleb Saksamaa satelliidiettevõtte juht B. Smutny: „Prantsusmaa on tehnoloogia varastamises kurjuse impeerium ja Saksamaa teab seda."[134] Ühe endise luureametniku sõnul on prantslastel ärisaladuste hankimise tudeerimiseks isegi eraldi kool.[135] M. Reid peab 2016. aasta seisuga kõige suurematekstööstusspionaažiga tegelevateks riikideks lisaks Hiinale, Venemaale ja Prantsusmaale veel Indiat ja Iisraeli.[136]

„Pole olemast sellist asja nagu sõbralikud luureteenistused. On ainult sõbralike riikide luureteenistused," kõlab tuntud ütlus, mida omistatakse Henry Kissingerile.[137] Endine KAPO peadirektor Arnold Sinisalu on selle mõttega osaliselt päri, kuid lisab, et vastuluures ning seda eriti partneritega Läänemere regioonis on sõprus võimalik küll.[138] Üheks oluliseks sõpruse allikaks peab Sinisalu terrorismivastast võitlust, kus Euroopa Liidu liikmesriigid, Norra, Šveits ja Suurbritannia teevad omavahel tihedat koostööd, ning tänu millele on ära hoitud palju

[131] Radio Free Europa/Radio Liberty. Bolton: Russian Accident Shows Kremlin's Nuclear Ambitions. (15.08.2019). – https://www.rferl.org/a/bolton-russian-accident-shows-kremlin-nuclear-ambitions/30111305.html (04.02.2025); Fox News. Trump reveals 'one very big power' the US has over China. – https://www.youtube.com/watch?v=RN0nR8Rx0KI (04.02.2025). („*Because during Obama's administration [...] Russia stole the design, they got it from us. Some bad person gave them the design.*")
[132] Lotrionte, C., lk 468 jj. Vt lähemalt: Fialka, J. J. War by Other Means: Economic Espionage in America (1997); Schweitzer, P. Friendly spies: How America's Allies are Using Economic Espionage to Steal Our Secrets. Atlantic Monthly Press 1993.
[133] Nasheri, H. Economic Espionage and Industrial Spying. Cambridge University Press 2005, lk 13. (viidatud: Reid, M. A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat? – University of Miami Law Review 2016/70, No 3, lk 798.)
[134] France 24. France is top industrial espionage offender. (04.01.2011). – https://www.france24.com/en/20110104-france-industrial-espionage-economy-germany-russia-china-business (02.04.2025).
[135] Priit Pruksi intervjuu endise luureametnikuga.
[136] Reid, M., lk 783–802.
[137] Lowenthal, M. Intelligence. From Secrets to Policy (8th Edition). CQ Press 2020, Chapter Seven: Counterintelligence.
[138] Priit Pruksi intervjuu A. Sinisaluga, 07.08.2024.

terroriakte.[139] A. Sinisalu sõnul on olukord sootuks teine majanduses ja poliitikas, kus liitlaste huvid võivad lahkneda.[140] Ka Eestis on tulnud ette konflikte liitlasriikide eriteenistustega. A. Sinisalu meenutab: „Detaili minemata ma võin öelda, et selle aja jooksul, mis ma olen kaitsepolitseis töötanud, on mul teada juhtumeid küll, kus on nii-öelda jalgpalli keeles kollast kaarti näidatud. Võib-olla isegi ka punast kaarti näidatud. Aga lihtsalt liitlaste vahel ei tehta võib-olla sellist suurt lärmi. Öeldakse, et see mees lahkub. Käitus valesti. Ja loetakse see teema lahendatuks. [Koos]töö peab edasi jätkuma.“ [141] Hüpoteetilise stsenaariumi kohta, kus liitlasriigi eriteenistus värbab kellegi üle andma Eesti riigisaladust, ütleb Sinisalu: „[See isik] tuleb sama moodi kinni panna... Kui on võimalik kinni panna.“[142]

Olukorras, kus Eesti kaitsetööstus kasvab, ning aina enam tehakse koostööd riikidega, kellel on rahvusvaheliselt tegutsevad kaitsetööstused ja tööstusspionaaži kogemustega eriteenistused, ei ole välistatud, et ebaterve huvi meie kaitsetööstuse vastu võib tekkida ka liitlastel. Ettevaatlikkusele liitlastega läbikäimisel manitseb ka üks kaitsetööstuse ekspert, kes väidab, et selles valdkonnas tegutsedes on üpris keeruline vältida kokkupuuteid endiste CIA (*Central Intelligence Agency*) ametnikega.[143] Rääkides USA julgeolekuametnikest on selge, et nende abi ja kogemus on Euroopa kaitsetööstusele kasulik ja vajalik, kuid Euroopa strateegilise autonoomia tõsiseltvõetavuseks on mõistlik säilitada teatav distants.

EKTL-i juhatuse liige K. Koidumäe ütleb: „[Me] ei räägi siin ainult vaenulikest riikidest, vaid ka teiste riikide relvatööstustest, kes samuti arendavad mingeid programme ja relvasüsteeme ja koguvad samuti infot, et saada aru, mis toimub partnerite juures. [...] Euroopas käib tööstusspionaaž suur[te] *prime*’ide[144] vahel veel aktiivsemalt kui me siin mõtleme, et palju hiinlased ja venelased siin ringi luusivad.“[145] Ehkki K. Koidumäe kasutab siin tööstusspionaaži mõistet viitamaks ärispionaažile ehk olukorrale, kus spionaažiga soodustatakse äriühingut, ei

[139] Priit Pruksi intervjuu A. Sinisaluga, 26.09.2024.
[140] Priit Pruksi intervjuu A. Sinisaluga, 07.08.2024. Vt poliitilis-sõjalise ja majandusspionaaži eristamise kohta: Lotrionte, C., lk 459 jj.
[141] Priit Pruksi intervjuu A. Sinisaluga, 07.08.2024.
[142] Samas.
[143] Priit Pruksi intervjuu kaitsetööstuse eksperdiga.
[144] Ameerika Ühendriikide õiguskorras eristatakse *prime contractor*’it ehk peatöövõtjat ja *subcontractor*’it ehk alltöövõtjat. *Prime contractor* on ettevõtja, kes sõlmib Ameerika Ühendriikide valitsusega hankelepingu. *Subcontractor* on ettevõtja, kes sõlmib *prime contractor*’iga allhankelepingu. Ehk siis, kui räägitakse *defense prime*’idest, mõeldakse selle all kaitsetööstuse äriühinguid, kes on sõlminud riigiga hankelepingud. *Defense prime*’ideks on Ameerika Ühendriikides suurkorporatsioonid nagu Lockheed Martin, Raytheon või General Dynamics. Vt lähemalt: 38 CFR § 3.502-1; Neenan, A. G. Defense Primer: Department of Defense Contractors. Congressional Research Service, 06.06.2024. – https://www.congress.gov/crs-product/IF10600 (09.04.2025).
[145] Priit Pruksi intervjuu K. Koidumäega, 01.04.2025.

pruugi tööstus- ja ärispionaaž kaitsetööstuses olla esmapilgul – ega ka pikemal pilgul – üksteisest eristatavad. Seda põhjusel, et kaitsetööstuses on riik ja erasektor omavahel tihedalt seotud. Ja seda mitte ainult vaenulikes riikides nagu Hiina või Venemaa, vaid ka liitlasriikides nagu Prantsusmaa. M. Reid leiab, et Prantsusmaal on „[t]ööstus ja riik omavahel keeruliselt läbipõimunud“ [146] . Väitele lisab kaalu endise DGSE peadirektori Claude Silberzahni ülestunnistus, et Prantsusmaa on aastakümneid spioneerinud kodumaiste riigiettevõtete huvides.[147] Tööstusspionaaži ohtu Euroopas suurendab Euroopa kaitsetööstuse killustatus. K. Koidumäe toob näite, et võrreldes USA sõjaväega, kus on kasutusel üks tank[148], konkureerivad Euroopas sakslaste, prantslaste ja inglaste tankid. [149] Killustatus tekitab konkurentsi ja konkurents omakorda vajaduse koguda konkurentide kohta teavet.

Kolmkümmend aastat tagasi nimetas USA luurejuht Robert Gates luurekogukonna kasutamist kodumaiste ettevõtete konkurentsieelise säilitamiseks „moraalseks ja õiguslikuks sooks“[150]. Kas ja kui palju abistavad meie liitlasriikide eriteenistused kodumaiseid kaitsetööstusettevõtteid on huvitav küsimus – kasvõi juba Euroopa Liidu riigiabi reeglite aspektist – kuid kindlasti mitte miski, millele suudame vastata selle töö raames. Käesolev magistritöö võib aga anda mõtteid hetkel veel hüpoteetilise stsenaariumi kohta, kui liitlasriigi kaitsetööstusega seotud isik tabatakse Eesti kaitsetööstuse äriühingust ärisaladuse hankimiselt. Kas sel juhul tegutseb täideviija välisriigi eriteenistuse või välisriigi äriühingu huvides? Või kas sel juhul ohustatakse konkreetse äriühingu majandustegevust või Eesti Vabariigi julgeolekut?

[146] Reid, M., lk 797.
[147] Rustmann Jr., F.W. CIA, Inc.: Economic Espionage and the Craft of Business Intelligence. Potomac Books 2002.
[148] M-1 Abrams. Vt lähemalt: Feickert, A. The Army’s M-1E3 Abrams Tanks Modernization Program. Congressional Research Service, 21.01.2025. – https://www.congress.gov/crs-product/IF12495 (09.04.2025).
[149] Priit Pruksi intervjuu Kalev Koidumäega.
[150] („*moral and legal swamp*“) Vt: Warner, W. T. Economic Espionage: A Bad Idea. – National Law Journal, 12 April 1993. (viidatud: Lotrionte, C., lk 469)

## 2. Kaitsetööstuse mõiste

Mõistetel on õigusteaduses oluline tähendus. Õigupoolest võib õigusteaduslik uurimistöö piirdudagi mingi mõiste piiritlemisega. Olgu selleks „Eesti kultuur ja rahvus“ [151], „rahvusvaheline leping“ [152], „riigireetmine“[153] või „terrorism“ [154]. Enne kaitsetööstuse kaitsele asumist oleks õige sisustada ka kaitsetööstuse mõiste. Miks?

Sest kui kuulata ettevõtjaid jääb mulje, et tegemist on võrdlemisi kasutu ettevõtmisega. „Kaitsetööstusettevõtete sees ei räägi mitte keegi sellest, mis on kaitsetööstus. Selle mõiste on leiutanud riik,“ ütleb Asutajate Seltsi juhtfiguur ja ettevõtja Allan Martinson. [155] Ühelt poolt on tähelepanekul tõsi taga. Ettevõtjate töö on pakkuda tooteid ja teenuseid, mitte tegeleda mõisteliste aruteludega. Teiselt poolt ei saa sugugi rahul olla arusaamaga, et riik tegeleb mõisteliste aruteludega omal algatusel ja oma suva järgi. Demokraatlikus riigis sünnivad mõisted rahvasaadikute arutelu tulemusena, kusjuures selles arutelus osalevad ka ettevõtjad, nt Eesti Kaitse- ja Kosmosetööstuse Liidu kaudu. Tõsi, teatud valdkondades nagu julgeolek on täitevvõimu mõjuvõim mõistete sisule võrdlemisi suur.

Arutelu mõistete ja reeglite vajalikkusest eksistentsiaalse ohu olukorras on kahtlemata üleval. Ühel pool rindejoont seisab juriidiline idealism, teisel pool ettevõtjate pragmatism. Eesti ühiskonnas iseloomustab seda vastuolu õigusharidusega kaitseministri Hanno Pevkuri ja ettevõtja loomuga endise kantsleri Kusti Salmi vahel. Pevkuri tegevust ja tegevusetust lahkavad ajakirjanikud Eero Epner ja Erik Moora kirjutavad: „Lääne demokraatialt oodatakse kiirust, otsustavust, nurkadest üle sõitmist, reeglite painutamist. Samal ajal ollakse reeglite painutamise suhtes ülitundlikud. Kas demokraatlikus lääne ühiskonnas on üldse võimalik reageerida sõjale nii kiiresti, kui paljude arvates oleks vaja?“[156]

[151] Anton, S. Eesti kultuuri ja rahvuse mõiste põhiseaduse preambulis. – Riigiõiguse aastaraamat 2020, lk 62–67.
[152] Kirjanik Jaan Krossi kaitsmata jäänud kandidaaditöö: Kross, J. Rahvusvahelise lepingu mõistest.
– Riigiõiguse aastaraamat 2020, lk 157–162.
[153] Purre, M. Riigireetmine ja riigireetur. – Juridica 2020/2, lk 79–89.
[154] Värk, R. Julgeolekunõukogu tõlgendused terrorismi olemusele. – Juridica 2010/2, lk 130–144.
[155] Martinson, A., Tammai, K., Mikheim, V.
[156] Epner, E., Moora, E. „Ta on meie aja kangelane.“ Rahva ees säravale Pevkurile heidetakse ette suure plaani puudumist. – Eesti Ekspress 03.02.2025.

„Eesti on tegutsenud Ukraina abistamisel nagu röövlijõuk“, ütleb üks Epneri ja Moora artikli anonüümne allikas. [157] Kas kaitseministeerium saab jätkata samas vaimus? Või võiks põhiseadus osutuda takistuseks?

Kaitsetööstuse piiritlemist võiksid nõuda mitmed põhiseaduslikku järku põhimõtted nagu demokraatia [158], õigusriik [159] ja vaba turumajandus [160]. Seda põhjusel, et kaitsetööstuses põimuvad omavahel era- ja avalik huvi, mis tekitab küsimusi avalike vahendite kasutamise läbipaistvusest, toetuste väärkasutamisest ja riigi sekkumisest majandustegevusse. Hübriidrünnakute tõttu aina suurenev soov paigutada tsiviilobjekte riigi kaitsva vihmavarju alla toob paratamatult päevakorda tuntud maksiimi: „See, kes kaitseb kõike, ei kaitse mitte midagi“.[161] Määramatu sisuga kaitsetööstuse kaitsmine võib viia selleni, et ei kaitstagi mitte midagi. Ja agara kaitsetöö käigus kurnatakse ära väikeriigi niigi piiratud ressursid.

Magistritöö fookust arvestades ei ole võimalik nendel teemadel pikemalt peatuda, kuid päevasündmuste valguses on oluline need vähemalt ära markeerida. Seda enam, et kaitseministeeriumi kantsler Kaimo Kuusk tunnistab, et kaitseministeerium ei ole olnud kohati riigikontrollile väga hea partner. [162] Veel lisab kantsler, et ministeeriumis on hangete auditeerimine „selgelt ebapiisav“, kuivõrd auditeerimisega tegeleb ainult üks inimene. [163] Anonüümsete allikate sõnul on ilmnenud mõnede moonahangete puhul kahtlused, mis ei ole „üksnes hüpoteetilised“ [164]. Kantsler Kuusk kommenteerib kahtlusi järgmiselt: „On küsimärke, kuhu ma tahaksin kindlasti veel sisse vaadata, aga seda ma siin praegu raadioeetris lahkama ei hakkaks.“ [165] Vastuargumendina hankereeglite ja auditite karmistamisele jääb kõlama I.

[157] Samas.
[158] PS § 1 I lause; Eesti Vabariigi põhiseadus (PS). – RT I, 15.05.2015, 2.
[159] PS § 10.
[160] PS § 31; RKÜKo 3-4-1-2-13, p 105: „Põhiseadusega tagatud ettevõtlusvabadusel on mitu tahku. [...]Teisalt peab riik tagama õigusliku keskkonna vaba turu toimimiseks [...]“; RKÜKo 3-4-1-2-13, p 112: „Ettevõtlusvabadus kaitseb ettevõtja võimalust toimida turu tingimustes riigi põhjendamatu sekkumiseta.“
[161] Ei suutnud tuvastada tsitaadi täpset päritolu. Riigikaitseobjektide kohta vt lähemalt: ERR. Riigikontroll: vaid üks elektritaristu objekt on selgelt kaitstud. (15.01.2025). – https://www.err.ee/1609576618/riigikontroll-vaid-uks-elektritaristu-objekt-on-selgelt-kaitstud (29.01.2025); ERR. Läänemets: riigikaitseobjektide nimekiri täieneb. (15.01.2025). – https://www.err.ee/1609577170/laanemets-riigikaitseobjektide-nimekiri-taieneb (29.01.2025); Vabariigi Valitsuse 23. septembri 2016. a määrus nr 106 „Riigikaitseobjekti kaitse kord“. – RT I, 12.03.2019, 33.
[162] Hindre, M. Kuusk kaitseministeeriumist: sisekontrolli pole ja julgeolek on alamehitatud.
[163] Samas.
[164] Epner, E., Moora, E.
[165] Hindre, M. Kuusk kaitseministeeriumist: sisekontrolli pole ja julgeolek on alamehitatud; Korruptsiooniohust kaitsetööstuses tuli juttu ka KAPO 2024–2025 aastaraamatu esitlusel, kui Äripäeva ajakirjanik küsis uute võimalike korruptsiooniriskide kohta. „Kindlasti me vaatame mingil määral kaitsevaldkonda, kuna sinna on suunatud väga suured rahad viimastel aastatel ja need investeeringud kaitsevaldkonda kasvavad,“ ütleb KAPO

Pärnamäe väljendatud usaldamatus riigi ja kaitsetööstuse vahel.[166] Reeglite ja auditite ennatlik ja ülemäärane karmistamine võib lämmatada selle vähesegi usalduse, mis on tekkinud, ning veelgi raskendada kodumaise kaitsetööstuse olukorda.

Kaitsetööstuse piiritlemisel on ka karistusõiguslik õigustus. J. Sootaki järgi on õigusriikliku karistusõiguse ülesandeks kaitsta „inimeste sotsiaalse kooselu aluseid“ ehk õigushüvesid.[167] Järelikult eeldab kaitsetööstuse karistusõiguslik kaitse kaitsetööstuse kui õigushüve määratlemist või siis kaitsetööstuse sidumist mõne teise juba ühiskondlikult tunnustatud õigushüvega, nt julgeolekuga.[168]

Veel rõhutab J. Sootak vajadust eristada õigushüve ja ründeobjekti.[169] Näiteks riigireetmise korral kahjustatakse Eesti Vabariigi julgeolekut kui õigushüve, kuid ründeobjektiks on riigisaladus (KarS § 232). Juhul, kui seadusandja soovib kehtestada koosseisu, mis kaitseb Eesti Vabariigi julgeolekut, aga sätestab ründeobjektina kaitsetööstuse, tuleks järgida määratletusnõuet, mis nõuab, et kaitsetööstus kui objektiivse koosseisu tunnus oleks normi adressaadile ja seaduse rakendajale mõistetav vähemalt sel määral, et selle sisu oleks „tõlgendamisega avatav“.[170] Teisiti öeldes, kui tööstusspioonide tõhusamaks karistamiseks ja heidutamiseks peaks olema tarvis täiendada karistusseadustikku kaitsetööstuse mõistega oleks tarvis teada, kas see mõiste on ka tõlgendamisega avatav.

## 2.1 Kaitseministeeriumi kaitsetööstuse mõiste

Kaitseministeeriumi 2021. aasta kaitsetööstuspoliitika kohaselt hõlmab kaitsetööstus „Eestis registreeritud juriidilisi isikuid, mis tegelevad kaitse- ja julgeolekuotstarbelise teadus- ja arendustegevusega, tootmisega või seotud teenuste osutamisega“[171]. Seotud teenuste näideteks tuuakse kaitse- ja julgeolekuotstarbelise varustuse hooldust ja remonti.[172]

peadirektor Margo Palloson. Vt lähemalt: Kaitsepolitseiameti aastaraamatu esitlus 2025. (alates 34:24.) – https://www.youtube.com/watch?v=dNq3KR8XyCU (21.04.2025).

[166] Priit Pruksi intervjuu Ingvar Pärnamäega.

[167] Sootak, J. Karistusõigus. Üldosa. Tallinn: Juura 2018, lk 34.

[168] Julgeoleku ja kaitsetööstuse omavahelist seost käsitlen pikemalt alapeatükis 4.3.

[169] Sootak, J. Karistusõigus. Üldosa, lk 34.

[170] Samas, lk 43–44.

[171] Kaitseministeerium. Eesti kaitsetööstuspoliitika „Koostöös loodud kaitsevõime“, 2021, lk 1.

[172] Samas.

Kaitseministeeriumi kaitsetööstuse mõiste määratlus koosneb kolmest komponendist: isikud, tegevused ja esemed. Isikute alla kuuluvad Eestis registreeritud juriidilised isikud, tegevused hõlmavad kaitse- ja julgeolekuotstarbelist teadus- ja arendustegevust ja tootmist ning esemete alla liigituvad kaitse- ja julgeolekuotstarbelised tooted ja teenused.

Selline määratlus ei erine kuigi palju „kaitsetööstusbaasi“[173] (*Defense Industrial Base,* DIB) mõiste määratlusest USA õiguskorras. Kongressi teabeteenistuse [174] järgi sisenes „kaitsetööstusbaasi“ mõiste seadusandja leksikoni Korea sõja ajal.[175] Teabeteenistuse järgi on DIB „võrgustik organisatsioone, asutusi, ja ressursse, mis varustavad Ameerika Ühendriikide valitsust – eelkõige kaitseministeeriumi – kaitseotstarbeliste materjalide, toodete, ja teenustega“ [176] . DIB hõlmab nii „kommertsettevõtteid, mis tegutsevad tulu eesmärgil, mittetulunduslikke teaduskeskuseid ja ülikoolide laboratooriumeid, ning valitsuse omanduses olevaid tööstusasutusi“[177]. DIB varustab valitsust „kõigega alates suurtest, tehnoloogiliselt keerukatest relvasüsteemidest ja kõrgspetsialiseerunud operatiivsest toetusest kuni üldiste kommertstoodete ja argiteenusteni“[178]. Kuigi DIB-i peamiseks kliendiks on kaitseministeerium, varustab DIB ka teisi valitsusasutusi, nt CIA-d.[179] *U.S. Code* ehk föderaalkoodeks[180] kasutab ka mõistet „rahvuslik tehnoloogiline tööstusbaas“ (*National Technological Industrial Base*, NTIB) [181], mis sisenes õiguskäibesse 1993. aastal.[182]

---

[173] 10 U.S.C. Subtitle A (General Military Law), Part V (Acquisition), Subpart I (Defense Industrial Base).
Vt lähemalt: European Parliament. Directorate-General for External Policies. The development of a European Defence Technological and Industrial Base (EDTIB). 2013 juuni. – https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/433838/EXPO-SEDE_ET%282013%29433838_EN.pdf (16.01.2025).
[174] Congressional Research Service. – https://crsreports.congress.gov/ (15.01.2025).
[175] Nicastro, L.A. The U.S. Defense Industrial Base: Background and Issues for Congress, lk 1. Nimelt käis Trumani ja Eisenhower valitsuse ametnike vahel käis kemplus, kui lai või kitsas peaks olema kõnealune tööstusbaas.
[176] Samas.
[177] Samas.
[178] Samas.
[179] Samas.
[180] Föderaalkoodeksisse on koondatud Ameerika Ühendriikide föderaalseadused (*statutes*), mis on jagatud 53-ks pealkirjastatud struktuuriüksuseks nimega *Title*. Nt *Economic Espionage Act of 1996* asub 18. *Title*'is §-des 1831–1839. Huvitaval kombel ei pruugi kõik *Title*'id olla kongressi poolt vastu võetud (*enacted*) föderaalkoodeksis kirjeldatud sõnastuses ehk siis osa kehtivast kõigusest. Näiteks *Title* 18 on sõna-sõnalt osa kehtivast õigusest, aga *Title* 22 ei ole. Seetõttu viitan magistritöös 18. puhul otse föderaalkoodeksile, aga 22. puhul kehtivale föderaalseadusele endale (nt *Arms Export Control Act of 1976*). Vt lähemalt: 1 U.S.C. § 204(a); GovInfo. United States Code. – https://www.govinfo.gov/app/collection/uscode (26.04.2025); Wice, S. When to Refer to the U.S. Code Versus the Underlying Statute. Notice & Comment. Yale Journal on Regulation (July 25, 2018). – https://www.yalejreg.com/nc/when-to-refer-to-the-u-s-code-versus-the-underlying-statute/ (26.04.2025).
[181] 10 U.S.C. § 4801.
[182] Nicastro, L. A. Defense Primer: The National Technology and Industrial Base. Congressional Research Service. Uuendatud 30.03.2023. – https://crsreports.congress.gov/product/pdf/IF/IF11311/12 (15.01.2025).

Euroopa Liidu õiguskorras kasutatakse analoogilise mõistena EDTIB-i (*European Defence Technological and Industrial Base*). EDTIB-i mainitakse esmakordselt 2007. aasta Euroopa Liidu kaitseministrite strateegiadokumendis, mis seab tulevikuvisiooniks „tõeliselt euroopaliku DTIB-i“[183]. Viimast määratleb dokument entiteedina, mis: 1) „varustab enamuse varustusest ja süsteemidest, mida meie Relvajõud vajavad“ [184]; 2) „kindlustab, et neil [Relvajõududel] on maailma kõige parem tehnoloogia“[185]; 3) „garanteerib, et saame tegutseda kohase sõltumatusega“[186]. EDTIB figureerib Euroopa Kaitsefondi määruse (2021/697[187]), ühishangete määruse (2023/2418[188]) ja laskemoonamääruse (2023/1525[189]) põhjendustes ning 2024. aasta kaitsetööstuse strateegia esimestel ridadel, kuid mõiste määratlust ei leia ühestki mainitud dokumendist. EDTIB mõiste määratluse leiab Euroopa Parlamendi 2013. aasta uuringust.[190] Ilma detailidesse süüvimata võib öelda, et tegemist on võrdlemisi ebamäärase määratlusega. Põhjuseks poliitilised erimeelsused, mis seisnevad EDTIB-i „E“ ehk *European* määratlemises. Veel 2009. aastal leidis Euroopa Komisjoni tellimusel koostatud TNO raport, et „tegelikkuses ei ole sellist asja nagu ’Euroopa kaitsetööstus’“[191] ning Euroopa DTIB on „alltööstuste konglomeraat (*conglomerate of subindustries*)“ [192]. Esimene Euroopa kaitsetööstuse strateegia[193] on esimene suurem samm killustatuse vähendamiseks.

Aga tuleme tagasi Eesti kaitseministeeriumi kaitsetööstuse käsitluse juurde. Sõnaühendi „kaitse- ja julgeolekuotstarbelise“ juures viitab kaitseministeerium strateegilise kauba seadusele [194] öeldes, et kaitsetööstuse mõiste määratluses mainitud juriidilised isikud on

[183] European Defence Agency. A strategy for the European Defence Technological and Industrial Base. (14.05.2007) – https://eda.europa.eu/docs/documents/strategy_for_the_european_defence_technological_and_industrial_base.pdf (16.01.2025).
[184] Samas.
[185] Samas.
[186] Samas.
[187] Euroopa Parlamendi ja Nõukogu Määrus (EL) 2021/697, 29. aprill 2021, millega luuakse Euroopa Kaitsefond ja tunnistatakse kehtetuks määrus (EL) 2018/1092, ELT L 170/149, 12.5.2021.
[188] Euroopa Parlamendi ja Nõukogu Määrus (EL) 2023/2418, 18. oktoober 2023, millega luuakse instrument Euroopa kaitsetööstuse tugevdamiseks ühishangete kaudu (EDIRPA). – ELT L-seeria, 26.10.2023.
[189] Euroopa Parlamendi ja Nõukogu määrus (EL) 2023/1525, 20. juuli 2023, mis käsitleb laskemoona tootmise toetamist. – ELT L 185/7, 24.7.2023.
[190] European Parliament. Directorate-General for External Policies. The development of a European Defence Technological and Industrial Base (EDTIB). 2013 juuni. – https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/433838/EXPO-SEDE_ET%282013%29433838_EN.pdf (16.01.2025).
[191] Bekkers, F. jt . Development of a European Defence Technological and Industrial Base. TNO report (2009), 1.1.
[192] Samas.
[193] Euroopa Komisjon. Liidu välisasjade ja julgeolekupoliitika kõrge esindaja. Uus Euroopa kaitsetööstuse strateegia: EL-i valmisoleku saavutamine reageerimisvõimelise ja kerkse Euroopa kaitsetööstuse abil. (5.3.2024)
[194] Strateegilise kauba seadus. – RT I, 12.12.2024, 12.

„[s]trateegilise ja kahese kasutusega kauba tootjad ja sellega seotud teenuste osutajad StrKS tähenduses“ [195]. Veel täpsustab kaitseministeerium, et kaitsetööstus hõlmab ka „kriitilise tähtsusega kauba või teenuse pakkumist kriisi- ja sõjaajal“[196].

Puutuvalt tingimusse, et Eesti kaitsetööstus koosneb ainult Eestis registreeritud juriidilistest isikutest, tuleks täpsustada, et lisaks Eesti äriregistrisse kantud aktsiaseltsile või osaühingule on „[s]sõjarelva, relvasüsteemi, sõjarelva laskemoona või lahingumoona käitlev ettevõtja“ ka „Euroopa Liidu liikmesriigis, Euroopa Majanduspiirkonna lepinguriigis või Šveitsi Konföderatsioonis asutatud sellesarnane juriidiline isik“ (Relvaseaduse [197] § $83^{21}$ lg 1). Ettevõtja ja tema juhatuse asukoht peab aga olema Eestis (RelvS § $83^{22}$ lg 1). Samuti tuleks mainida, et relvaseaduse muutmisega võimaldatakse „anda tegevusluba ka Eesti ja Euroopa Liiduga sõbralikes suhetes olevate kolmandate riikide ettevõtjatele, mille omanikud, osanikud või aktsionärid ei ole NATO või Euroopa Liidu liikmesriikide kodanikud“ [198]. Ehk siis detailidesse laskumata võib väita, et Eesti kaitsetööstuse isikukoosseis muutub edaspidi aina rahvusvahelisemaks.

Siinkohal võiks tõmmata paralleeli NTIB mõistega Ameerika Ühendriikide õiguskorras. Föderaalkoodeksi § 4801 kohaselt on NTIB: „Isikud ja organisatsioonid, mis tegelevad teaduse, arenduse, tootmise, integratsiooni, teenuste osutamise või infotehnoloogiliste tegevustega Ameerika Ühendriikides, Suurbritannia ja Põhja-Iirimaa Ühendkuningriigis, Austraalias, Uus Meremaal või Kanadas.“ [199] 1993. aasta NDAA (*National Defense Authorization Act*) [200]

[195] Kaitseministeerium. Eesti kaitsetööstuspoliitika, lk 1 (joonealused märkused).
[196] Samas.
[197] Relvaseadus (RelvS). – RT I, 12.12.2024, 3.
[198] 468 SE. Relvaseaduse muutmise ja sellega seonduvalt teist seaduste muutmise seaduse eelnõu seletuskiri. Vastu võetud 20.11.2024, lk 3. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/6af5a052-2757-4a32-8048-7cc285580339/relvaseaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/ (09.04.2025).
[199] 10 U.S.C. § 4801.
[200] Kontekstiks: Ühendriikide kongress võtab iga aasta vastu kaks riigikaitselist õigusakti: NDAA ja eraldamiseelnõu (*appropriations bill*). Esimene neist kuulub esindajatekoja ja senati relvajõudude komitee pädevusse ning annab volituse eraldada raha kaitseministeeriumile, energiaministeeriumi tuumarelvade programmile ja muudele riigikaitsega seotud tegevustele. Ühtlasi kehtestab NDAA „kaitsepoliitika ja piirangud (*restrictions*) ning käsitleb kaitseministeeriumiga seotud organisatsioonilisi-administratiivseid küsimusi“. Vt lähemalt: Heitshusen, V., McGarry, B. W. Congressional Research Service. Defense Primer: The NDAA Process. Uuendatud 06.01.2025. – https://crsreports.congress.gov/product/pdf/IF/IF10515 (15.01.2025).

Siiski ei toimu NDAA alusel raha eraldamine, vaid selleks võtab kongress vastu eraldi eraldamiseelnõu. Kuigi NDAA alusel raha ei eraldada, annab see siiski hea ülevaate kongressi kaitsepoliitilistest prioriteetidest ja kaitsekulutuste orienteeruvast suurusjärgust vastaval eelarveaastal. Vt lähemalt: Saturno, J. V. Authorizations and the Appropriations Process. Congressional Research Service. Uuendatud 16.05.2023. – https://crsreports.congress.gov/product/pdf/R/R46497 (15.01.2025).

vastuvõtmisega, mis sisaldas esmakordselt NTIB mõistet, soovis kongress tagada, et külma sõja lõpuga kaasnenud kaitsekulutuste vähendamise tuhinas oleks riik endiselt võimeline vastu seisma julgeoleku- ja majandusohtudele.[201] Sisuliselt kirjutati NTIB mõistega seadusesse juba toimiv Ameerika Ühendriikide ja Kanada vaheline tööstusalane koostöö. Aja jooksul on koostöö laienenud lisaks Kanadale ka teistesse „anglosfääri" riikidesse, mis kuuluvad alates 1956. aastast nn UKUSA lepingusse. [202] Kõnealuse kokkuleppe alusel toimub viie riigi vaheline luurealane koostöö.[203]

Seega, liitlaste kaasamine enda kaitsetööstusesse on igati loogiline samm ja tõenäoliselt sellel kursil edaspidi Euroopa Liidus ka jätkatakse. Ja, kes teab, äkki tekib üks hetk ka paljuräägitud EDTIB.[204] Seevastu Ameerika Ühendriikide praeguse valitsuse poliitikat arvestades ei ole välistatud, et NTIB-riikide kaitsetööstuste integreeritus ja koostöö edaspidi hoopis väheneb.[205]

Eelnevast nähtub, et kaitsetööstuse mõiste määratlemisel langeb põhirõhk tegevustele ja esemetele. Sooviga arutelu veelgi kitsendada küsin, kuidas määratleb praegune õiguskord mõisteid „kaitseotstarbeline" või „julgeolekuotstarbeline". Siin tulevad abiks strateegilise kauba seadus, riigihangete seadus[206] ning riigisaladuse ja salastatud välisteabe seadus. Põgusalt käsitleme ka riigikaitseliste sundkoormiste koondkava.

Mõistagi võiks käsitleda ka relva- ja lõhkeaineseadust, kuid magistritöö mahupiirang ja hiljutine täiendus RSVS-i „sõjalise otstarbega asja" mõiste näol võimaldavad jätta meil need seadused tähelepanuta. Pealegi, eesmärk ei ole anda üksikasjalikku ülevaadet igast kaitsetööstusettevõtja jaoks olulisest õigusaktist, vaid luua üldpilt, millised esemed kuuluvad

[201] Nicastro, L. A. Defense Primer: The National Technology and Industrial Base. Congressional Research Service. Uuendatud 30.03.2023.
[202] GCHQ. A Brief History of the UKUSA agreement. – https://www.gchq.gov.uk/information/brief-history-of-ukusa (15.01.2025).
[203] Samas. Tegemist on nn „*Five Eyes*" riikidega.
[204] Meenutuseks: EDTIB ehk *European Defence Technological and Industrial Base*.
[205] Kanada peaminister Mark Carney ütleb seda sõnaselgelt. Vt lähemalt: The Times and Sunday Times. „Canada's old relationship with the US is over," says Carney. (27.03.2025). – https://www.youtube.com/watch?v=dgjybooP-pA (04.03.2025). Enamgi veel, D. V. Gioe leiab, et USA praeguse valitsuse *policy* võib nõrgestada tavatingimustel poliitiliselt neutraalset luurekoostööd: Gioe, D.V. How America's Allies Boost U.S. Intelligence. And Why Trump Threatens That Cooperation. Foreign Affairs 13.02.2025. – https://www.foreignaffairs.com/united-states/how-americas-allies-boost-us-intelligence (05.03.2025). Võrdlusena, Välisluureameti *policy* luureinfo jagamisel liitlastega on „*business as usual*": Mackinnon, A. jt. How US allies may try to safeguard their intel ops from Trump. Politico 21.02.2025. – https://www.politico.com/news/2025/02/21/us-allies-intel-sharing-trump-00205204 (05.03.2025).
[206] Riigihangete seadus. – RT I, 07.06.2024, 11.

kaitsetööstuse mõiste alla ning uurida, kas kaitsetööstuse mõiste kasutamine karistusseadustikus oleks üldse mõeldav.

## 2.2 Strateegilise kauba seadus

Strateegiline kaup koosneb viiest kategooriast: 1) sõjaline kaup; 2) kaitseotstarbeline toode; 3) inimõiguste rikkumiseks kasutatav kaup; 4) kahesuguse kasutusega kaup; 5) kaup, mida ei ole kantud strateegiliste kaupade nimekirja, aga mille suhtes on strateegilise kauba komisjon asunud seisukohale, et „kaubal on strateegilise kauba tunnused kas tema omaduste, lõppkasutuse või lõppkasutaja tõttu või avaliku julgeoleku või inimõigustega seotud kaalutlustel“ (StrKS § 2 lg 11).[207]

Sõjalist kaupa on kolme liiki. Esiteks võib selleks olla „relv, aine, materjal, vahend, seade, süsteem, nende osad, nendega seotud varustus ja spetsiaalsed komponendid, tarkvara ja tehnoloogia, mis on projekteeritud, valmistatud, määratud või kohandatud sõjalisel otstarbel kasutamiseks“[208]. Teiseks võivad selleks olla kõik eelmainitud esemed, mis küll ei ole projekteeritud, valmistatud, määratud või kohandatud sõjalisel otstarbel kasutamiseks, kuid „mida kasutatakse sõjalisel otstarbel“[209]. Kolmandaks võivad selleks olla kõik eelmainitud esemed, mis on loetletud sõjaliste kaupade nimekirjas.[210]

Sõjaliste kaupade nimekiri sisaldub strateegiliste kaupade nimekirjas, mille kehtestab Vabariigi Valitsus määrusega.[211] Määruse Lisas 1 sisalduv sõjaliste kaupade nimekiri ei erine esmapilgul[212] sugugi sõjaliste kaupade ühisest Euroopa Liidu nimekirjast, mille on vastu võtnud Euroopa nõukogu.[213] Arvestades, et nõukogu seisukoht esindab liikmesriikide valitsuste seisukohta, on tegemist täitevvõimu diskretsiooni alusel koostatud nimekirjaga.[214] See sõjatehnoloogia ja -varustuse ekspordikontrolli tugevdamisel eesmärgil koostatud nimekiri koosneb 22-st erineva mahuga kategooriast, mida tähistatakse lühendiga „ML“.[215] Näiteks,

[207] StrKS § 2 lg-d 1, 10 ja 11; RKKKo 3-1-1-23-17, p 15.
[208] StrKS § 2 lg 2.
[209] Samas.
[210] Samas.
[211] StrKS § 2 lg 10; Vabariigi Valitsuse 22. detsembri 2011. a määrus nr 171 „Strateegiliste kaupade nimekiri“. – RT I, 04.06.2024, 2.
[212] Ei saa väita, et nimekirjad on identsed, kuna selleks tuleks kontrollida kahe nimekirja kattuvust. See ei ole praeguse fookuse juures vajalik.
[213] Sõjaliste kaupade ühine Euroopa Liidu nimekiri, mille nõukogu võttis vastu 19. veebruaril 2024. – C/2024/1945, 1.3.2024.
[214] Euroopa Liidu leping (ELL). – C 202/1, 7.6.2016; ELL, art 16(2).
[215] Sõjaliste kaupade ühine Euroopa Liidu nimekiri. – C/2024/1945.

kategooria ML1 on võrdlemisi konkreetne: „sileraudsed tulirelvad kaliibriga alla 20 mm ja teised käsirelvad ning automaattulirelvad kaliibriga 12,7 mm [...]“[216]. Seevastu kategooriad ML21 ja ML22 (vastavalt „Tarkvara“ ja „Tehnoloogia“) on võrdlemisi avarad.[217] Sealjuures peetakse tehnoloogiaks ka esemeid, mis on vajalikud „sõjaliste kaupade ühises EL nimekirja loetletud kaupade tootmisseadmete projekteerimiseks, kokkupanekuks, käsitsemiseks, hooldamiseks ning remontimiseks [...]“; mis aga omakorda avardab juba olemuslikult avarat määratlust. [218]

Kaitseotstarbeline toode on StrKS mõttes „Euroopa Liidu siseselt edasitoimetatav kaup, mille veo suhtes rakendatakse lihtsustatud korda kooskõlas Euroopa Parlamendi ja nõukogu direktiiviga 2009/43/EÜ [219] kaitseotstarbeliste toodete ühendusesisese veo tingimuste lihtsustamise kohta [...] ning mis on loetletud kaitseotstarbeliste toodete nimekirjas“ [220]. Kaitseotstarbeliste toodete nimekirja kehtestab Vabariigi Valitsuse määrusega (StrKS § 2 lg 10). Esmapilgul on valitsuse määruse Lisas 2 sisalduv kaitseotstarbeliste kaupade nimekiri võrdlemisi sarnane[221] direktiivi 2009/43/EÜ lisas sisalduva nimekirjaga.

Inimõiguste rikkumiseks kasutatav kaup on „kaup, millel puudub muu praktiline eesmärk kui kasutamine surmanuhtluse täideviimiseks, piinamiseks või muul julmal, ebainimlikul või alandaval moel kohtlemiseks või karistamiseks nõukogu määruse (EÜ) nr 1236/2005 [...] artiklite 3 ja 4 tähenduses“[222]. Kõnealune määrus on praeguseks kehtetu ja seda asendab määrus 2019/125[223], mille art-d 3 ja 4 viitavad määruse II lisas leiduvatele kaupadele ja nende kaupadega seotud tehnilisele abile. II lisa nimekiri on ootuspäraselt lühike: hukkamiseks mõeldud seadmed ning seadmed, mida ei tohi kasutada inimeste ohjeldamiseks või massirahutuste ohjeldamiseks või enesekaitseks.[224]

[216] Samas.
[217] Samas.
[218] Samas.
[219] Euroopa Parlamendi ja Nõukogu direktiiv 2009/43/EÜ, 6. mai 2009, kaitseotstarbeliste toodete ühendusesisese veo tingimuste lihtsustamise kohta. – ELT L 14/1, 10.6.2009.
[220] StrKS § 2 lg 5.
[221] Taaskord: ei saa väita, et nimekirjad on identsed, kuna selleks tuleks kontrollida kahe nimekirja kattuvust. See ei ole praeguse fookuse juures vajalik.
[222] StrKS § 2 lg 6.
[223] Euroopa Parlamendi ja Nõukogu määrus (EL) 2019/25, 16. jaanuar 2019, mis käsitleb kauplemist teatavate kaupadega, mida on võimalik kasutada surmanuhtluse täideviimiseks, piinamiseks või muuks julmaks, ebainimlikuks või alandavaks kohtlemiseks või karistamiseks. – ELT L 30/1 31.1.2019.
[224] Samas.

Kahesuguse kasutusega kaup on „kaup, sealhulgas tarkvara ja tehnoloogia, mida saab kasutada nii tsiviil- kui ka sõjalisel otstarbel, nii rahuotstarbelisel eesmärgil kui ka abivahendina tuumarelvade või muude tuumalõhkeseadmete tootmisel nõukogu määruse (EÜ) nr 428/2009 [...] tähenduses“[225]. Määruse 428/2009[226] art 3 viitab I lisale, mis sisaldab 27 lehekülge üldmärkusi ja mõistete definitsioone ning 290 lehekülge katkematut esemete loetelu koos märkuste ja tehniliste märkustega.

Lisaks eeltoodud kategooriatele on võimalik, et strateegilise kauba komisjon omistab strateegilise kauba tähistuse kaubale, mis ei ole kantud strateegiliste kaupade nimekirja.[227] Strateegilise kauba komisjoni kuuluvad Välisministeeriumi, Kaitseministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi, Maksu- ja Tolliameti, Kaitsepolitseiamet ning Politsei- ja Piirivalveameti esindajad (StrKS § 70 lg 1).

Sarnane süsteem, millega piiratakse kaitseotstarbeliste esemete ja teenuste vedu, toimib ka Ameerika Ühendriikides ning selle haldamine kuulub presidendi pädevusse.[228] Kaitseotstarbelised esemed ja teenused moodustavad nimekirja, mida kutsutakse *United States Munitions List* (USML).[229] Täitevkorralduse 13637 järgi delegeerib president talle antud õiguse piirata USML-i kuuluvate esemete väljavedu ja ajutist sissevedu välisministrile (*Secretary of State*).[230] Välisministeerium rakendab föderaalkoodeksis sätestatu elluviimiseks regulatsiooni, mida tuntakse ITAR (*International Traffic in Arms Regulations*) nime all.[231] ITAR-iga paralleelselt eksisteerib ka teine ekspordikontrolli raamistik ehk EAR (*Export Administration Regulations*)[232], mille alusel kaubandusministeerium (*Department of Commerce*) haldab nimekirja nimega CCL (*Commerce Control List*), kuhu kuuluvad „kahesuguse kasutusega esemed [...] ja mõned vähem tundlikud sõjalised esemed“[233].

[225] StrKS § 2 lg 8.
[226] Nõukogu määrus (EÜ) nr 428/2009, 5. mai 2009, millega kehtestatakse ühenduse kord kahesuguse kasutusega kaupade ekspordi, edasitoimetamise, vahendamise ja transiidi kontrollimiseks. – ELT L 134, 29.5.2009.
[227] StrKS § 2 lg 1; RKKKo 3-1-1-23-17, p 15.2.
[228] Arms Export Control Act (AECA) of 1976, Public Law 90–629, § 38(a)(1) I lause. [22 U.S.C. § 2778]
[229] Samas, § 38(a)(1) II lause.
[230] Executive Order 13637 – Administration of Reformed Export Controls (08.03.2013). Section 1.(n)(i).
[231] 22 CFR 120-130.
[232] 15 CFR 730-780.
[233] The White House. Fact Sheet: Implementation of Export Control Reform. (08.03.2013). – https://obamawhitehouse.archives.gov/the-press-office/2013/03/08/fact-sheet-implementation-export-control-reform (16.01.2025).

Ameerika Ühendriikide strateegilise kauba veokontrolli reeglid on olulised ka Eesti kaitsetööstusele. Näiteks piiras Bideni valitsus CCL-i kuuluvate tehisintellekti kiipide eksporti osadesse Euroopa Liidu ja NATO liikmesriikidesse, sh Eestisse.[234] Ühtlasi on Ühendriikide kaitseministeerium ehk Pentagon maailma suurim kaitseotstarbeliste toodete ja teenuste arendaja ning hankija. 2023. aastal moodustasid Pentagoni kulutused 37% maailma 15-ne kõrgeima kaitsekulutustega riigi kaitsekulutuste kogusummast – järgnesid Hiina (12%) ja Venemaa (4,5%).[235] 2025. eelarveaastal on kongressilt oodata 143,77 miljardit dollarit kaitsealasteks teadus- ja arendustegevusteks ning 167,85 miljardit dollarit riigihangeteks.[236]

Pentagoni tegevus mõjutab oluliselt kaitsetööstusi üle kogu maailma, sh Euroopa Liidu kaitsetööstust. EL-i kaitsetööstuse strateegia kohaselt oli „Venemaa agressioonisõja alguse ja 2023. aasta juuni vahelisel ajal [...] EL-i liikmesriikide poolt väljastpoolt EL-i tehtud kaitseotstarbeliste ostude osakaal 78%, kusjuures ainuüksi USA osakaal oli 63%“[237]. Euroopa Komisjoni taasrelvastumise plaani valguses võib olukord muutuda.[238]

## 2.3 Riigihangete seadus

Eesti riigihankeõigus on suures osas Euroopa Liidu õigus, mistõttu on selle õigusvaldkonna jaoks olulised Euroopa Liidu direktiivid, sh kaitse- ja julgeolekuvaldkonna riigihankelepingute direktiiv 2009/81/EÜ[239]. Kõnealuse direktiivi art 1 kohaselt on kaitseotstarbeline varustus: „[V]arustus, mis on spetsiaalselt projekteeritud või kohandatud sõjaliseks otstarbeks ning mõeldud kasutamiseks relvana, laskemoonana või sõjavarustusena“[240]. Asjakohane on ka direktiivi „tundliku“ varustuse/ehitustööde/teenuste määratlus: „[J]ulgeoleku eesmärgiga

[234] Department of Commerce. Bureau of Industry and Security. Framework for Artifical Intelligence Diffusion. A Rule by the Industry and Security Bureau on 01/15/2025. Vt ka meediakajastust: ERR. Tsahkna kritiseeris Bideni valitsuse otsust piirata kiibieksporti Eestisse. (16.01.2025).
[235] Trends in World Military Expediture, 2023. SIPRI Fact Sheet, 2024 aprill. – https://www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf (14.01.2025).
[236] FY2025 NDAA: Summary of Funding Authorizations. Congressional Research Service, 07.01.2025. – https://crsreports.congress.gov/product/pdf/IN/IN12404 (14.01.2025).
[237] Euroopa Komisjon. Liidu välisasjade ja julgeolekupoliitika kõrge esindaja. Uus kaitsetööstuse strateegia: EL-i valmisoleku saavutamine reageerimisvõimelise ja kerkse Euroopa kaitsetööstuse abil. (5.3.2024), lk 3. Vt lähemalt: Maulny, J.-P. The impact of the war in Ukraine on the European defence market. IRIS, 2023 september. – https://www.iris-france.org/wp-content/uploads/2023/09/19_ProgEuropeIndusDef_JPMaulny.pdf (14.01.2025)]
[238] European Commission. Press statement by President von der Leyen on the defence package. (04.03.2025) – https://ec.europa.eu/commission/presscorner/detail/sv/statement_25_673 (05.04.2025).
[239] Euroopa Parlamendi ja Nõukogu direktiiv 2009/81/EÜ, 13. juuli 2009, millega kooskõlastatakse teatavate kaitse- ja julgeolekuvaldkonnas ostjate poolt sõlmitavate ehitustööde ning asjade ja teenuste riigihankelepingute sõlmimise kord ja muudetakse direktiive 2004/17/EÜ ja 2004/18/EÜ. – ELT L 216/76, 20.08.2009.
[240] Samas, art 1.

varustus, ehitustööd ja teenused, millega kaasneb, mis eeldavad ja/või sisaldavad salastatud teavet“[241].

Direktiivi 2009/81/EÜ põhjenduste punkti 10 kohaselt tuleks „kaitseotstarbelise varustuse all mõista eelkõige tooteliike, mis on esitatud nõukogu 15. aprillil 1958. aasta otsusega 255/58 vastu võetud relvade, laskemoona ja sõjavarustuse loetelus, ning liikmesriigid võivad käesoleva direktiivi ülevõtmisel piirduda üksnes selle loeteluga“[242]. Samas ütleb direktiivi sama punkt, et otsuse 255/58[243] loetelu on „üldine ja seda tuleb tõlgendada laialt, arvestades tehnoloogia, riigihankepoliitika ja sõjaliste nõuete arengut, mis toob kaasa uut liiki varustuse väljatöötamise, näiteks liidu ühise sõjaliste kaupade nimekirja põhjal“[244].

B. Heuninckx leiab, et direktiivi 2009/81/EÜ „kaitseotstarbelise varustuse“ mõiste jääb „mõneti segaseks“[245], kuivõrd viitab nii 1958. aastal koostatud nimekirjale kui ka ühisele sõjaliste kaupade nimekirjale. T. Väljaots ja C. Ginter leiavad samal tsitaadile tuginedes, et ühine sõjaliste kaupade nimekiri on uuendatud ja detailsem versioon 1958. aasta nimekirjast.[246] Siinkirjutaja hinnangul B. Heuninckxi seda ei väida, vaid ta juhib hoopis tähelepanu, et mõiste tõlgendamisel eksisteerib kaks eraldi allikat: 1958. aasta nimekiri ja ühine sõjaliste kaupade nimekiri. Viimast uuendatakse pidevalt.

Riigihangete seaduse § 169 lg 1 p 1 sätestab kaks kumulatiivset eeldust, mille täitmisel kohalduvad „kaitseotstarbelisele asjale“ kaitse- ja julgeolekuvaldkonna riigihangete erireeglid. Seda juhul, kui kaitseotstarbeline asi on: 1) „projekteeritud või kohandatud sõjaliseks otstarbeks“[247]; 2) „hõlmab laskemoona, lõhkeainet, relvastust, inseneri-, side- ja seirevarustust, riide- ja erivarustust, maismaa-, mere- ja õhusõidukeid, nendega seotud remondi- ja hooldusvahendeid ja muid sõjalistel eesmärkidel kasutatavaid materjale, sealhulgas selle mis tahes osa, koostisosa ja alamkoost või üks neist“[248]. Eelnevast nähtub, et riigihangete seaduse

[241] Samas.
[242] Samas, põhjendus 10.
[243] Council of The European Union. Interinstitutional File: 2007/0280 (COD). (26.11.2009). – https://data.consilium.europa.eu/doc/document/ST-14538-2008-REV-4/en/pdf (14.04.2025).
[244] Samas.
[245] Heuninckx, B. EU Public Procurement Law: An Introduction. (ed. Arrowsmith, S.) University of Nottingham 2010, lk 287.
[246] Väljaots, T., Ginter, C. RHS komm § 169, p 4. – Riigihangete seadus. Komm vlj. Tallinn: Juura 2019.
[247] RHS § 169 lg 1 p 1.
[248] Samas.

silmis iseloomustavad kaitseotstarbelist asja kaks tunnust: sõjaline otstarve ja kuulumine teatud esemete gruppi (nt relvastus).

T. Väljaots ja C. Ginter eristavad objektiivset ja subjektiivset sihtotstarvet leides, et asja kaitseotstarbeliseks kvalifitseerimisel tuleb lähtuda objektiivsest sihtotstarbest ehk siis sellest, mis eesmärgiks konkreetne ese on projekteeritud või kohandatud, ning mitte subjektiivsest otstarbest ehk siis sellest, mis eesmärgiks eset kasutada soovitakse.[249] Näiteks, „tsiviiltüüpi buss, mis on sõjaväele kasutamiseks sõjaväemustriliseks värvitud“ [250] ei erine objektiivse sihtotstarbe poolest tsiviilotstarbelistest esemetest, kuigi subjektiivne sihtotstarve võib olla sõjaline kasutus. Objektiivse ja subjektiivse sihtotstarbe eristamine on oluline juhis, mille abil piirata kaitseotstarbeliste toodete ringi.

RHS § 169 lg 1 p 2 kasutab mõistet „julgeolekuotstarbeline asi“, kuigi kaitse- ja julgeolekuvaldkonna riigihankelepingute direktiivis kasutatakse mõistet „tundlik varustus“. Direktiivi 2009/81/EÜ järgi on „tundlik varustus“ „julgeoleku eesmärgiga varustus, ehitustööd või teenused, millega kaasneb salastatud teave, mis eeldavad ja/või sisaldavad seda“ [251]. Järelikult iseloomustavad julgeolekuotstarbelist asja kaks tunnust: julgeolekualane otstarve ja seotus salastatud teabega.

113 SE I seletuskirja kohaselt peetakse julgeolekualase otstarbe all silmas „nii sõjalist kui ka mittesõjalist julgeolekut, s.t. varustuse, ehitustööde ja teenuste hankimine peab toimuma julgeolekuvaldkonnas kasutamiseks“[252]. Sealjuures, erinevalt kaitseotstarbelisest varustusest „ei pea varustus olema spetsiaalselt projekteeritud või kohandatud julgeoleku tarbeks“[253]. Sätet rakendatakse „riigihangete suhtes, millel on kaitsealaste riigihangetega sarnased tunnused ja mis on niisama tundlikud, näiteks valdkondades, kus kaitsevägi ja mittesõjalised jõud teevad koostööd samade ülesannete täitmiseks ja/või kus riigihanke eesmärk on kaitsta riigi julgeolekut oma territooriumil või kaugemal mittesõjalistest ja/või valitsusvälistest jõududest lähtuva tõsise ohu eest“[254]. Direktiivi 2009/81/EÜ põhjenduse 11 järgi võib see hõlmata näiteks

[249] Väljaots, T., Ginter, C. RHS komm § 169, p 7. Vt ka: EKo C-337/05, Euroopa Ühenduste Komisjon *versus* Itaalia Vabariik, p 58.
[250] Samas.
[251] Euroopa Parlamendi ja Nõukogu direktiiv 2009/81/EÜ, art 1 p 7.
[252] 113 SE I. Riigihangete seaduse muutmise seaduse eelnõu seletuskiri. Vastu võetud 25.01.2012, lk 6. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/5498ac05-bc6e-7882-13a3-328366ee31f2/riigihangete-seaduse-muutmise-seadus/ (09.04.2025).
[253] Samas.
[254] Samas.

piirikaitset, politseitööd ja kriisimissioone; 113 SE I seletuskirja järgi ka „elutähtsa infrastruktuuri ettevõtjate hankelepingute sõlmimist võrgustikega seotud valdkondades“[255]. Viide mittesõjalistest jõududest lähtuvale ohule annab mõista, et julgeolekualane otstarve võiks olla eelkõige vahenditel, mis aitavad tõrjuda „hübriidrünnakuid“[256]. Näiteks vahendid, mis aitavad ennetada ja takistada rünnakuid merealustele sidekaablitele.

Direktiivi 2009/81/EÜ kohaselt on salastatud teave „igasugune teave või materjal [...], millele on määratud salastatuse tase või kaitsetase ning mis riigi julgeoleku huvides ning vastavalt asjaomases liikmesriigis kehtivatele õigus- või haldusnormidele vajab kaitsmist [...]“[257]. 113 SE I seletuskirja järgi on Eesti õiguskorras direktiivi 2009/81/EÜ mõttes salastatud teabeks riigisaladus ja salastatud välisteave.[258]

RHS § 169 lg 1 p 3 laiendab kaitse- ja julgeolekuvaldkonna erireegleid ka kaitse- ja julgeolekuotstarbeliste asjadega otseselt seotud ja nende elutsükli etappide jaoks vajalike asjade ostmisele ning teenuste või ehitustööde tellimisele. Direktiivi 2009/81/EÜ põhjenduse 12 kohaselt on sellisteks etappideks teadus- ja arendustegevus, tööstuslik arendamine, tootmine, parandamine, uuendamine jne.[259] 113 SE I seletuskirja kohaselt tähendab sõnaühend „otseselt seotud“, et asjad, teenused või ehitustööd peavad olema nii tihedalt seotud tundliku varustusega, et eraldivõetuna ei oleks neil mingit tähendust.[260]

## 2.4 Riigikaitseliste sundkoormiste koondkava

Kaitseministeeriumi kaitsetööstuse mõiste hõlmab muuhulgas kriitilise tähtsusega kaupu või teenused, nt „meditsiiniteenused, sideteenused, maismaa-, mere- ja raudteetransport, kütus ja laskemoon“[261]. Ühtlasi viitab kaitseministeerium Vabariigi Valitsuse 05.03.2021 korraldusele „Tegevusalade riigikaitseliste sundkoormiste koondkava kinnitamine“. [262]

[255] Samas.
[256] Sazonov, V. jt Sisejulgeoleku hübriidohtude tutvustamine. Sisekaitseakadeemia 2020.
[257] Euroopa Parlamendi ja Nõukogu direktiiv 2009/81/EÜ, art 1 p 8.
[258] 113 SE I. Riigihangete seaduse muutmise seaduse eelnõu seletuskiri, lk 6.
[259] Euroopa Parlamendi ja Nõukogu direktiiv 2009/81/EÜ, põhjendus 12.
[260] 113 SE I. Riigihangete seaduse muutmise seaduse eelnõu seletuskiri, lk 6–7.
[261] Kaitseministeerium. Eesti kaitsetööstuspoliitika, lk 1.
[262] Samas, joonealused märkused; Vabariigi Valitsuse 5. märtsi 2021. a korraldus nr 104 „Tegevusalade riigikaitseliste sundkoormiste koondkava kinnitamine“. – RT III 09.03.2021, 3.

Kõnealune korraldus enam ei kehti, kuivõrd korraldus võeti vastu nüüdseks kehtetuks tunnistatud riigikaitseliste sundkoormiste seaduse[263] alusel. Sundkoormiste kohta käivad asjakohased normid sätestab nüüd riigikaitseseadus[264], mis lisaks muudele uuendustele on loobunud „sundkoormiste" mõiste kasutamisest. Selle asemel kasutab seadus mõistet „riigikaitselised kohustused"[265], mis on sisuliselt omandipõhiõigust riivavad kohustused.[266]

Uue regulatsiooni järgi ei reguleerita riigikaitseliste sundkoormiste koondkava enam seaduse tasandil.[267] Koondkava on nüüdsest „haldusesisene planeerimisdokument, mille koostamist toetab tsiviiltoetuse register"[268]. Koondkava eesmärk on „kinnitada varade/teenuste nomenklatuur ja kogused, mis on lubatud riigikaitselise sundkoormisena Kaitseväe poolt kasutusele võtta alates kõrgendatud kaitsevalmiduse kehtestamisest"[269]. Siinkirjutajal puudub juurdepääs kehtivale koondkavale, mistõttu tuleb aluseks võtta Vabariigi Valitsuse korraldusega 2021. aasta 5. märtsil kehtestatud koondkava.

Sellest koondkavast leiame 9-leheküljelise loetelu tegevusaladest ja võimalikest koormatavatest tegevustest. Osade tegevusalade puhul on seos kaitsetööstusega ilmselge, nt „relva- ja laskemoonatootmine"[270]. Teiste puhul on seos otsese sõjategevusega kaugem, nt „saunad"[271] või „fekaalivedu"[272]. Samas tasub meenutada kindral Omar Bradleyle omistatud lauset: „Amatöörid räägivad strateegiast. Professionaalid räägivad logistikast"[273]. I. Pärnamäe kinnitab, et sundkoormiste koondkavas figureerivad valdavalt logistikaga tegelevad äriühingud.[274]

[263] Riigikaitseliste sundkoormiste seadus. – RT I, 10.03.2022, 13.
[264] Riigikaitseseadus (RiKS). – RT I, 14.03.2023, 31.
[265] RiKS, 5. peatükk, 3. jagu. Asja sundkasutus ja asja sundvõõrandamine.
[266] 417 SE. Riigikaitseseaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri. Vastu võetud 16.02.2022, lk 29. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/44178720-02b2-4d30-8707-d7dcf606dcee/riigikaitseseaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/ (09.04.2025); Vabariigi Valitsuse 5. märtsi 2021. a korraldus nr 104 „Tegevusalade riigikaitseliste sundkoormiste koondkava kinnitamine".
[267] 417 SE seletuskiri, lk 2.
[268] Samas, lk 30.
[269] Samas.
[270] Vabariigi Valitsuse 5. märtsi 2021. a korraldus nr 104 „Tegevusalade riigikaitseliste sundkoormiste koondkava kinnitamine" Lisa. Tegevusalade riigikaitseliste sundkoormiste koondkava, nr 7.
[271] Samas, nr 51.
[272] Samas, nr 12.
[273] Boot, M. Our enemies aren't drinking lattes. Los Angeles Times 07.07.2006. – https://www.latimes.com/archives/la-xpm-2006-jul-05-oe-boot5-story.html (24.01.2025).
[274] Priit Pruksi intervjuu Ingvar Pärnamäega.

Fekaalivedu on kahtlemata osa sõjapidamise logistikast, mistõttu ei ole selle väljaarvamine kriitiliste teenuste nimekirjast õigustatud. Eraldi küsimus on, kas fekaalivedu peaks kuuluma kaitsetööstuse mõiste esemesse, kui räägime kaitsetööstuse karistusõiguslikust kaitsmisest tööstusspionaaži eest. Mõistuspärane oleks seda eitada.

## 2.5 Riigisaladuse ja salastatud välisteabe seadus

RSVS §-i 7 pealkirjaga „riigikaitse riigisaladus" täiendati punktiga $6^1$ järgmises sõnastuses: „sõjalise otstarbega asja omadusi, projekteerimist, valmistamist ja kohandamist käsitlev teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut."[275]. Täiendus tehti, kuna eelnevalt nägi RSVS ette ainult ühe kaitsetööstuse jaoks sobiliku salastamisaluse. Nimelt võimaldab RSVS § 7 p 6 salastada salajasel või madalamal tasemel „riigikaitselisi leiutisi ja uuringuid ning nende tulemusi käsitlevat teavet"[276], kuid 468 SE seletuskirja järgi on see alus „seotud kitsalt tehnikavaldkonna innovatsiooni ja intellektuaalomandi kaitsega ning ei oleks sageli kaitsetööstusele kohaldatav"[277].

RSVS § 11 lg 1 kohaselt sätestatakse RSVS § 7 punktides 1-8 nimetatud riigisaladuseks oleva teabe alaliigid Vabariigi Valitsuse määrusega. 468 SE seletuskirja kohaselt täiendatakse kõnealuse Vabariigi Valitsuse määruse[278] §-i 5 lg-ga $6^1$ järgmises sõnastuses: „Sõjalise otstarbega asja projekteerimist, valmistamist ja kohandamist käsitleva teabe osas on riigisaladuseks teave, mis käsitleb riigi tellimusel sõjarelva, selle olulise osa, sõjalise otstarbega laskemoona, lahingumoona, lahingutehnika ning kaitseotstarbelise erivarustuse omadusi, projekteerimist, valmistamist, parandamist ja ümbertegemist, kui sellise teabe avalikuks tulek kahjustaks Eesti Vabariigi või muu EL või NATO liikmesriigi julgeolekut."[279]

468 SE seletuskirja järgi on „sõjalise otstarbega asi": „[Ü]ldmõiste, millega on soovitud hõlmata võimalikult laia ringi asju, mida kaitsetööstus toodab, piiritledes neid samas sõjalise otstarbega."[280] Konkreetsemalt mainitakse sõjarelva, selle olulist osa, sõjalise otstarbega laskemoona, lahingumoona, lahingutehnikat ning kaitseotstarbelist erivarustust.[281]

[275] RSVS § 7 p $6^1$.
[276] RSVS § 7 p 6.
[277] 468 SE seletuskiri, lk 18.
[278] Vabariigi Valitsuse 20. detsembri 2007. a määrus nr 262 „Riigisaladuse ja salastatud välisteabe kaitse kord". – RT I, 29.12.2024, 16.
[279] 468 SE seletuskiri, lk 18–19.
[280] Samas.
[281] Samas.

## 2.6 Eesti kaitsetööstus

2021. aasta kaitseministeeriumi kaitsetööstuspoliitika kohaselt on kohaliku kaitsetööstuse tugevusteks: „küberkaitse, autonoomsed süsteemid, sensorid, side- ja seiretehnoloogiad, elektroonika, isikuvarustus, sõidukite remont ja hooldus“[282]. Veel rõhutatakse, et eriti tugevad on rahvusvahelisel turul „mehitamata süsteemide, küberkaitse ja seiretehnoloogiate“ [283] pakkujad.

Kaitseministeeriumi väitel on EKTL riigi jaoks oluline partner.[284] EKTL juhatuse liige Kalev Koidumäe kirjeldab Eesti kaitsetööstuse arengus nelja verstaposti. Esiteks: 2000. aastate keskpaik, kui kaitsevägi osales NATO operatsioonis Afganistanis ja Ameerika Ühendriikide juhitud operatsioonis Iraagi Vabadus, kus kaotati sõdureid plahvatustes, mille põhjustasid raadio teel juhitavad improviseeritud lõhkekehad. Vastumeetmena arendasid Tallinna Tehnikaülikool ja osaühing Rantelon välja elektroonilise segamisseadme nimega IRIS, mis on endiselt kasutusel nii Eesti kui Ukraina kaitseväes.[285] Teiseks: 2007. aasta aprillirahutused, mille käigus rünnati Eesti Vabariiki küberruumis, ning mille tulemusena elavnes küberkaitse valdkond. Kolmandaks: 2014. aasta september, kui Eesti-Venemaa piirilt rööviti kaitsepolitseinik Eston Kohver. Kohveri röövimise tõttu asus riik rajama kõrgtehnoloogilist idapiiri, mille raames arendas osaühing ELI välja droonipesa, Defendec vaatlussüsteemid ning Defsecintel kogus esimesi mõtteid piirivalvetehnoloogiate kohta. Neljandaks: 2014. aasta, kui algas sõda Ida-Ukrainas, mida asus jälgima OSCE missioon, mida toetasid Eesti ettevõtte Threod mehitamata õhusõidukid. Täiemahulise sõja alguses 2022. aastal sisenes Ukrainasse Defsecintel, mis töötas välja füüsilise platvormi (suur treiler), millele teised kaitsetööstuse ettevõtjad said paigaldada oma tooteid ning neid Ukrainas testida.[286]

K. Koidumäe väitel kuulub 2025. aasta aprilli seisuga EKTL-i 173 äriühingut, millest veidi rohkema kui kakskümne portfellis on 100% kaitse- ja julgeoleku valdkonna tooteid või teenuseid.[287] Äriühingutest suurimad on: 1) AS Milrem, kus töötab 308 töötajat, ning mille

[282] Kaitseministeerium. Eesti kaitsetööstuspoliitika, lk 2.
[283] Samas.
[284] Kaitseministeerium. Kaitsetööstuspoliitika. – https://www.kaitseministeerium.ee/et/eesmargid-tegevused/kaitsetoostuspoliitika (05.03.2025).
[285] Defence Estonia. EKTL member Rantelon is a creator, developer and manufacturer of innovative electronic systems. (24.11.2023). – https://defence.ee/news/ektl-member-rantelon-is-a-creator-developer-and-manufacturer-of-innovative-electronic-systems/ (03.04.2025).
[286] Priit Pruksi intervjuu K. Koidumäega.
[287] Samas.

2023. aasta müügitulu ulatus 19 miljoni euroni[288]; 2) AS Threod Systems 160 töötajaga. Müügitulu teeniti 2023. aastal 20 miljonit eurot[289]; 3) Defsecintel Solutions OÜ 93 töötajaga. 2023. aastal teeniti müügitulu 30 miljonit eurot[290]. Kõigi kolme äriühingu tooteid tellis Eesti riik osana 100 miljoni euro suurusest abipaketist Ukrainale.[291] Liitu kuulub veel hulk ettevõtteid, kus kaitse- ja julgeolekuvaldkonna toodete ja teenuste osakaal tooteportfellist on kasvanud viimase 3–4 aastaga 5%-lt üle 50%.[292] Liidu liikmeskond kasvab kiiresti: 2024. aastal ühines liiduga umbes 30 äriühingut, 2025. aastal on ainuüksi esimese kvartaliga liitunud juba umbkaudu 20 äriühingut.[293]

EKTL-i 2023. aasta majandusaasta aruande kohaselt on nende liikmete peamisteks tegevusvaldkondadeks: „imitaatorid ja väljaõppesüsteemid; kaitseotstarbelised infotehnoloogia-, elektroonika-, juhtimis- ja sidesüsteemid; küberkaitse lahendused; laevaehitus, remont ja hooldus; lasersüsteemid; meditsiinivarustus; militaarsõidukite elutsüklihooldus; piirikaitsesüsteemid; pioneeri- ja insenerilahendused; relvad, lõhkeaine ja laskemoon, relvade tarvikud; robootika (mehitamata õhusõidukid, mehitamata maismaasõidukid), kosmosevaldkond“.[294]

EKTL nõukogu liikme ja osaühingu Defsecintel juhatuse liikme Jaanus Tamme sõnul on paljud lahendused „kahese kasutusega, rakendatavad nii kaitsevaldkonnas kui ka tsiviilkasutuses, näiteks piirikaitses ja kriitilise taristu turvamises“[295]. J. Tamm toob veel esile mitmeid varajases faasis äriühinguid ehk iduühinguid nagu Wayren, SensusQ, Vegvisir, Lendurai ja Frankenburg.[296] K. Koidumäe sõnul kuulub EKTL-i iduühinguid umbkaudu kolmekümne kanti.[297]

[288] AS Milrem 2023. aasta majandusaasta aruanne.
[289] AS Threod Systems 2023. aasta majandusaasta aruanne.
[290] Defsecintel Solutions OÜ 2023. aasta majandusaasta aruanne.
[291] Lauri, V. Riik tellib Eesti kaitsetööstuselt 100 miljoni eest toodangut Ukrainale. ERR 24.03.2025. – https://www.err.ee/1609642670/riik-tellib-eesti-kaitsetoostuselt-100-miljoni-eest-toodangut-ukrainale (06.04.2025).
[292] Priit Pruksi intervjuu K. Koidumäega.
[293] Samas.
[294] Eesti Kaitse- ja Kosmosetööstuse Liit. Majandusaasta aruanne 2023, lk 1.
[295] Tamm, J. Jaanus Tamm: Eesti kaitsetööstus on valmis järgmiseks arengufaasiks. ERR 25.02.2025. – https://www.err.ee/1609614869/jaanus-tamm-eesti-kaitsetoostus-on-valmis-jargmiseks-arengufaasiks (05.03.2025).
[296] Samas.
[297] Priit Pruksi intervjuu K. Koidumäega, 01.04.2025.

## 2.7 Vahekokkuvõte

Kaitsetööstuse mõiste avamisel võtsin lähtekohaks kaitseministeeriumi määratluse[298], mis koosneb kolmest komponendist: isikud, tegevused ja esemed. Õiguslikult kõige keerulisemaks osutus kaitse- ja julgeolekuotstarbelise eseme määratlemine, mille raames tuli käsitleda „strateegilise kauba“, „kaitse- ja julgeolekuotstarbelise asja“, „riigikaitselise sundkoormise“ ning „sõjalise otstarbega asja“ mõisteid. Selleks tuli tutvuda strateegilise kauba seaduse, riigihangete seaduse, riigikaitseseaduse, riigikaitseliste sundkoormiste seaduse ning riigisaladuse ja salastatud välisteabe seadusega. Mainitud seadustega on seotud ka terve rida EL-i õigusakte: sõjaliste kaupade ühine Euroopa Liidu nimekiri, direktiiv 2009/43/EÜ kaitseotstarbeliste toodete ühendusesisese veo tingimuste lihtsustamise kohta, määrus 2019/125 inimõiguste rikkumiseks kasutatavate kaupadega kauplemise kohta, Nõukogu 15. aprilli 1958. aasta otsus 255/58 ning riigihankelepingute direktiiv 2009/81/EÜ.

StrKS § 2 lg 1 kohaselt on strateegiline kaup sõjaline kaup, kaitseotstarbeline toode, inimõiguste rikkumiseks kasutatav kaup ning kahesuguse kasutusega kaup. StrKS § 2 lg 11 järgi käsitletakse strateegilise kaubana ka kaupa, mille suhtes on strateegilise kauba komisjon asunud seisukohale, et kaubal on strateegilise kauba tunnused „kas tema omaduste, lõppkasutuse või lõppkasutaja tõttu või avaliku julgeoleku või inimõigustega seotud kaalutlustel“. Teisisõnu, strateegilise kauba komisjoni kriteeriumid strateegilise kauba määratlemisel koosnevad neljast kategooriast: 1) eseme omadused; 2) eseme lõppkasutus; 3) lõppkasutaja isik; 4) eseme puutumus avaliku julgeoleku või inimõigustega.

Sõjalise kauba määratlemisel on kolm alternatiivi: 1) eseme omadused ehk kui ese on „projekteeritud, valmistatud, määratud või kohandatud sõjalisel otstarbel kasutamiseks“[299]; 2) eseme lõppkasutus ehk kui eset kasutatakse sõjalisel otstarbel[300]; 3) täitevvõimu otsus ehk kui ese kuulub Vabariigi Valitsuse määrusega vastuvõetud sõjaliste kaupade nimekirja või Euroopa Liidu nõukogu vastuvõetud sõjaliste kaupade ühisesse nimekirja[301]. Sõjaliste kaupade nimekiri koosneb 22-st erineva mahuga kategooriast, mis jätab täitevvõimule olulisel määral

[298] Kaitseministeerium. Eesti kaitsetööstuspoliitika „Koostöös loodud kaitsevõime“, 2021, lk 1.
[299] StrKS § 2 lg 2.
[300] Samas.
[301] StrKS § 2 lg 2 ja 10; Vabariigi Valitsuse 22. detsembri 2011. a määrus nr 171 „Strateegiliste kaupade nimekiri“; Sõjaliste kaupade ühine Euroopa Liidu nimekiri.

tõlgendamisruumi.[302] Esmapilgul ei erine Vabariigi Valitsuse ja Euroopa Liidu nõukogu nimekirjad üksteisest kuigi palju.

Kaitseotstarbelise toote määratlemisel tuleb tugineda EL direktiivi 2009/43/EÜ lisas sisalduvale nimekirjale või Vabariigi Valitsuse määruses[303] sisalduvale kaitseotstarbeliste toodete nimekirjale. Esmapilgul ei erine üksteisest ka need kaks nimekirja.

Inimõiguste rikkumiseks kasutatava kauba puhul tuleb lähtuda EL määruse 2019/125 lisas sisalduvast nimekirjast.

Euroopa Liidu õigus omab tähendust ka kahesuguse kauba määratlemisel. Nimelt sisaldab määruse 428/2009 lisa 27 lehekülge üldmärkusi ja mõistete definitsioone ning 290 lehekülge katkematut loetelu kahesuguse kasutusega esemetest koos märkuste ja tehniliste märkustega. Mõistagi on tõlgendamisruum ka siin võrdlemisi avar.

Kaitse- ja julgeolekuotstarbelise asja mõiste tuleneb riigihangete seadusest. RHS § 169 lg 1 p 1 sätestab kaks kumulatiivset eeldust otsustamaks, kas tegemist on kaitseotstarbelise asjaga. Esiteks peab asi olema „projekteeritud või kohandatud sõjaliseks otstarbeks“[304]. Teiseks peab asi kuuluma teatud kategooriasse nagu laskemoon, lõhkeaine, relvastus, inseneri-, side- ja seirevarustus jne.[305] Sealjuures kuuluvad kaitse- ja julgeolekuotstarbelise asja mõistesse ka eelnimetatud asjadega seotud remondi- ja hooldusvahendid ning muud sõjalistel eesmärkidel kasutatavad materjalid, sh nende osad, koostisosad ja alamkoostisosad või üks neist. [306] RHS § 169 lg 1 p-s 1 sätestatud eeldused tulenevad riigihankelepingute direktiivi art 1 p-st 6, mille kohaselt on kaitseotstarbeline varustus „spetsiaalselt projekteeritud või kohandatud sõjaliseks otstarbeks“ ning „mõeldud kasutamiseks relvana, laskemoonana või sõjavarustusena“. Seega, kaitseotstarbelise asja määratlemisel on olulised kaks tingimust: 1) lõppkasutus ehk sõjaline otstarve, 2) asja omadused ehk kuulumine teatud liiki asjade hulka, nt laskemoon, lõhkeaine, sidevarustus.

[302] Vabariigi Valitsuse 22. detsembri 2011. a määrus nr 171 „Strateegiliste kaupade nimekiri“; Sõjaliste kaupade ühine Euroopa Liidu nimekiri.
[303] Vabariigi Valitsuse 22. detsembri 2011. a määrus nr 171 „Strateegiliste kaupade nimekiri“.
[304] RHS § 169 lg 1 p 1.
[305] Samas.
[306] Samas.

Riigihankelepingute direktiivi 2009/81/EÜ põhjenduse 10 kohaselt tuleks kaitseotstarbelise varustuse all mõista eelkõige tooteliike, mis kuuluvad 15. aprilli 1958. aasta otsuse 255/58 nimekirja. Sama põhjenduse kohaselt on otsuse 255/58 näol üldise loeteluga ja seda tuleb „tõlgendada laialt, arvestades tehnoloogia, riigihankepoliitika ja sõjaliste nõuete arengut, mis toob kaasa uut liiki varustuse väljatöötamise [...]“[307]. Ühtlasi viitab põhjendus perioodiliselt uuendatavale sõjaliste kaupade Euroopa Liidu ühisele nimekirjale. Järelikult omab kaitseotstarbelise asja määratlemisel tähendust ka täitevvõimu ehk käesoleval juhul Euroopa Liidu nõukogu kaalutlusõigus.

RHS § 169 lg 1 p 2 kohaselt on julgeolekuotstarbeline asi selline asi, mis eeldab või sisaldab salastatud teavet. Riigihankelepingute direktiivi art 1 p 7 kasutab julgeolekuotstarbelise asja asemel „tundliku varustuse“, „tundlike ehitustööde“ ja „tundlike teenuste“ mõisteid. Tegemist on „julgeoleku eesmärgiga“[308] varustuse, ehitustööde ja teenustega, millega „kaasneb, mis eeldavad ja/või sisaldavad salastatud teavet“[309]. 113 SE I seletuskirja kohaselt seisneb julgeolekualane otstarve nii sõjalises kui ka mittesõjalises julgeolekus.[310] Direktiivi 2009/81/EÜ põhjenduse 11 järgi on üheks tüüpolukorraks nt piirikaitse, kus „sõjavägi ja mittesõjalised jõud teevad koostööd samade ülesannete täitmiseks“. Põhjenduses 11 sisalduv viide mittesõjalistest jõududest lähtuvale ohule annab mõista, et julgeolekualane otstarve võiks olla vahenditel, mis aitavad tõrjuda hübriidrünnakuid. Näiteks vahendid, mis aitavad ennetada ja takistada rünnakuid merealustele sidekaablitele. Järelikult, julgeolekuotstarbelise asja määratlemisel on kaks olulist tingimust: 1) asja lõppkasutus ehk julgeolekualane otstarve; 2) asja omadus ehk seotus salastatud teabega.

RHS § 169 lg 1 p 3 hõlmab kaitse- ja julgeolekuotstarbeliste asjade mõistetega ka sama sätte p-des 1 ja 2 nimetatud asjadega otseselt seotud ja nende elutsükli etappide jaoks vajalikud asjad, teenused ja ehitustööd. 113 SE I seletuskirja järgi tähendab otsene seotus, et asjad, teenused või ehitustööd peavad olema nii tihedalt seotud kaitse- või julgeolekuotstarbelise varustusega, et eraldivõetuna ei oleks neil mingit tähendust.[311]

[307] Euroopa Parlamendi ja Nõukogu direktiiv 2009/81/EÜ, põhjendus 10.
[308] Samas, art 1 p 7.
[309] Samas.
[310] 113 SE I seletuskiri, lk 6
[311] Samas, lk 6–7.

Eelnevast nähtub, et tõlgendamisruum on taaskord võrdlemisi lai. Seetõttu tuleks mainida mõningaid vahendeid, mille abil saab piirata kaitse- ja julgeolekuotstarbeliste asjade hulka. Üheks vahendiks on ülalmainitud „otsese seotuse“ mõiste. Teine on objektiivse ja subjektiivse otstarbe vahetegu. T. Väljaotsa ja C. Ginteri hinnangul tuleb asja kaitseotstarbeliseks kvalifitseerimisel lähtuda objektiivsest sihtotstarbest ehk siis sellest, mis eesmärgiks konkreetne ese on projekteeritud või kohandatud, ning mitte subjektiivsest otstarbest ehk siis sellest, mis eesmärgiks eset kasutada soovitakse.[312]

Riigikaitseliste sundkoormiste koondkava mõiste tuleneb riigikaitseliste sundkoormiste seadusest, mis enam ei kehti. Praeguseks on „riigikaitselise sundkoormise“ mõiste asendunud mõistega „riigikaitseline kohustus“, mida reguleerib riigikaitse seadus. Sisuliselt on tegemist omandiõiguse piiranguga[313] olukorras, kus riik vajab kaitsetegevuseks mingit asja, mis kuulub eraisikule. Varasem koondkava, mis kehtestati Vabariigi Valitsuse 5. märtsi 2021. a korraldusega, koosnes 9-leheküljelisest nimekirjast tegevusaladest, mis kuuluvad valdavalt logistika valdkonda. Kaitsetööstuse piiritlemise seisukohast on oluline rõhutada, et sundkoormiste koondkava on nüüdseks „haldusesisene planeerimisdokument“[314]. Teisisõnu, selle koostab täitevvõim ning see ei ole enam avalik.

Riigisaladuse ja salastatud välisteabe seadusest (RSVS § 7 p $6^1$) leiame „sõjalise otstarbega asja“ mõiste, mis on 468 SE seletuskirja kohaselt „üldmõiste, millega on soovitud hõlmata võimalikult laia ringi asju, mida kaitsetööstus toodab, piiritledes neid samas sõjalise otstarbega“[315]. Seega, määrav tegur on taaskord lõppkasutus ehk sõjaline otstarve. Seletuskirja järgi kuuluvad sõjalise otstarbega asja mõiste alla konkreetsemad kategooriad nagu sõjarelv, sõjalise otstarbega laskemoon, lahingumoon ja lahingutehnika, aga ka ähmasema sisuga kategooria nagu kaitseotstarbeline erivarustus[316].[317]

Õigusaktidest nähtub, et otsustamaks, kas tegu on kaitsetööstuse tootega, on määravad eseme omadused, lõppkasutus, lõppkasutaja ning täitevvõimu kaalutlusõigus. Viimane väljendub

[312] Väljaots, T., Ginter, C. RHS komm § 169, p 7. Vt ka: EKo C-337/05, p 58.
[313] 417 SE seletuskiri, lk 29.
[314] Samas.
[315] 468 SE. Relvaseaduse muutmise ja sellega seonduvalt teist seaduste muutmise seaduse eelnõu seletuskiri, lk 18–19.
[316] Näide kaitseotstarbelisest erivarustusest on OÜ Defensphere arendatav olukorrateadlikkuse süsteem soomukitele ja mehitamata maismaasõidukitele nimega Vegvisir. Vt lähemalt magistritöö alapeatükki „Kaitsetööstuse ärisaladus“.
[317] 468 SE seletuskiri, lk 18–19.

avarate kategooriatega nimekirjades, mis jätavad täitevvõimule laia tõlgendamisruumi. Sealjuures võidakse kaalutlusõiguse teostamisel tugineda mahukatele õiguslikele kategooriatele nagu avalik julgeolek või inimõigused. Täitevõimu eesmärk tundub olevat hõlmata kaitsetööstuse mõistega võimalikult lai ring juba olemasolevaid ja tulevikus loodavaid tooteid, teenuseid ja materjale.

Osundades õigusfilosoof John Austini väitele[318], et õigus on valitseja käsk, mis on tagatud sanktsiooniga – ehk siis õigus on täpselt see, mis valitseja ütleb, et õigus on – võiks mõtiskleda, et ehk on kaitsetööstus samuti see, mida valitseja parasjagu ütleb, et kaitsetööstus on.[319] Ja kui nii, mida ütleb Eesti valitseja hetkel kaitsetööstuse kohta? Kui küsida valitsejalt selle sõna põhiseaduslikus tähenduses – ehk siis rahvalt – võiks läbi rahvasaadikute suu öelda, et mitte just eriti palju. Riigikogu on jätnud kaitsetööstuse piiritlemise täitevvõimule, kelle kõneisiku kaitseministeeriumi määratlus on sisuliselt piiramatu. See, kas täitevvõimu tegevusvabadust nähakse vooruse või pahena, sõltub, kui palju usaldatakse riigivõimu ja kui oluliseks parasjagu peetakse julgeolekut.

Kaitsetööstuse kui õigushüve kaitsmine karistusõiguslikult on küsitav. Kahtlemata on kaitsetööstuse mõiste tõlgendamisega avatav – kuid ehk isegi liialt avatav. Õigusnormi adressaadile ja rakendajale peaks olema selgemini mõistetav, kus jookseb piir kaitsetööstuse ja muu majandustegevuse vahelt. Vastuargumendiks võib tuua asjaolu, et KarS §-d $421^1$ ja $421^2$ sisaldavad „strateegilise kauba“ mõistet ning siiamaani ei ole tõusetunud küsimust vastuolust määratletuspõhimõttega. Seda enam, et strateegilise kauba veoga seotud süütegude arv on alates täiemahulise sõja algusest Ukrainas aina kasvanud.[320]KAPO aastaraamatus 2024–2025 kirjutatakse: „Venemaa Föderatsioon vajab strateegilist kaupa ja püüab seda importida, kasutades keerulisi võrgustikke ja kaubateid.“[321] Olgu öeldud, et KAPO hoiatas juba enne

[318] Vt lähemalt: Austin, J. The Province of Jurisprudence Determined. Cambridge University Press 1995.
[319] Eesti kaitsetööstuses tegutsev endine CIA luureametnik James Acuna ütleb: „[K]üsimuse juures milliseid relvasüsteeme hakatakse tulevikus kasutama. Selle peale keegi vastas: mida iganes poliitikud soovivad. Selles lauses on tõetera, vaadates, kui suur osa USA sisemajanduse kogutoodangust sõltub sõjatööstusest.“ Ehk siis Acuna tähelepaneku põhjal võib öelda, et kaitsetööstuse mõiste sisustavad poliitikud. Seejuures on oluline, keda poliitikud kuulda võtavad, kas rahvast, ametnikke või ettevõtjaid. Vt lähemalt: Martin, M. Luure Keskagentuuri endine ohvitser: paljudele tuleb Venemaalt lähtuvat ohtu meelde tuletada. – Postimees 25.01.2025.
[320] Riigi Teataja järgi on KarS § $421^1$ kohtulahendite arv alates 2015. aastast 13, kusjuures 7 lahendit on tehtud alates täiemahulise sõja algusest. KarS § $421^2$ kohtumenetlusi on kaks, mõlemad 2025. aastal.
[321] KAPO aastaraamat 2024–2025, lk 60 jj.

täiemahulise sõja algust, et Eestit võidakse kasutada massihävitusrelvade levitamise ja strateegilise kauba smugeldamise transiitriigina.[322]

Kaitsetööstuse mõiste konkretiseerimisel võiks abi olla hiljutistest arengutest Taiwani õiguskorras. Kaitsmaks ärisaladust riiklikult olulistes tehnoloogiavaldkondades Hiina eest täiendas Taiwani parlament riigi julgeoleku seaduse (*National Security Act*)[323] tööstusspionaaži koosseisu „riikliku võtmetehnoloogia" (*national core key technology*) mõistega. Tõsi, ka selle mõistega kaasneb täitevvõimu kaalutlusõigus ning oht pikkadeks ja abstraktseteks nimekirjadeks; kuid keskendumine just võtmetehnoloogiatele võiks mõjuda distsiplineerivalt. Sest mitte kõik, mida kaitsetööstus toodab, ei paku huvi võõrriikidele. Sellele viitas ka seadusandja, kui täiendas RSVS-i uue salastamisalusega. Seletuskirja kohaselt on ebatõenäoline vajadus salastada teavet „lihtsate sõjalise otstarbega asjade tootmise kohta (nt riidevarustus, lihtne laskemoon), mille puhul ei ole tootmis- ja tarneahelat puudutavat teavet vaja varjata"[324]. Eelkõige näeb seadusandja RSVS § 7 p $6^1$ kasutusjuhuna vajadust „salastada (kõrg)tehnoloogilisi lahendusi, mille suhtes on vaenulikel välisriikidel suurem huvi ning mille kaitsmine üksnes ärisaladusena ei pruugi anda piisavat kaitset"[325].

Erikaitset vajava kõrgtehnoloogia kategooria sisustamisel võiks abi olla kaitsetööstuse ettevõtjaid koondavatest ühingutest nagu EKTL, mille liikmete sisend ja tegevusvaldkonnad annavad lähtekoha võtmevaldkondade tuvastamiseks. Tuleme selle arutelu juurde tagasi magistritöö kokkuvõttes, kui käsitleme mõningaid ettepanekuid tööstusspioonide tõhusamaks heidutamiseks ja karistamiseks. Esmalt aga küsime: mis on tööstusspionaaž?

[322] KAPO aastaraamat 2021–2022, lk-d 3 ja 37.
[323] National Security Act. Executive Yuan. (08.06.2022); Mao, L., Yu, D.. Tien, D. Taiwan. Trends and Developments. Heavier Punishments for Theft of Taiwanese Core Technologies. (16.01.2025). – https://practiceguides.chambers.com/practice-guides/investing-in-2025/taiwan/trends-and-developments (05.03.2025).
[324] 468 SE. Relvaseaduse muutmise ja sellega seonduvalt teist seaduste muutmise seaduse eelnõu seletuskiri, lk 19.
[325] Samas.

# 3. Tööstusspionaaži karistatavus Eesti õiguskorras

## 3.1 Luuretegevuse mõiste

M. Lowenthal eristab infot ja luureinfot: „Kõik luureinfo on informatsioon; kuid mitte kõik informatsioon ei ole luureinfo“[326]. Eristavaks kriteeriumiks on informatsiooni kasulikkus poliitikakujundajatele[327]. A. Zegarti väitel annab luureinfo poliitikakujundajatele „eelise oma vastaste ees“[328]. Järelikult seisneb luuretegevus poliitikakujundajatele kasuliku informatsiooni kogumises.

Luureinfot ei ihalda mitte ainult riigid, vaid ka äriühingud ja poliitilised ühendused. Äriühingute puhul kasutatakse mõistet äriluure[329] või konkurentsiluure[330]. Elukutselisi konkurentsiluurajaid ühendava organisatsiooni SCIP[331] eetikakoodeksi kohaselt on äri- ja konkurentsiluure sisuliselt sünonüümid.[332] L. Madureira jt. järgi on konkurentsiluure „protsess ja tulevikku vaatavad praktikad, mida kasutatakse konkurentsiolukorra kohta teadmiste kogumiseks ja organisatsiooni toimimise parandamiseks“[333].

[326] Lowenthal, M. Intelligence. From Secrets to Policy (8th Edition). CQ Press 2020, Chapter One: What is Intelligence?
[327] T. H. Ilves väidab, et eesti keeles pole võimalik eristada sõnu *politics* ja *policy*. „Kui inimesed küsivad, miks me peaks neid eristama, siis ma ütlen, et tõlkige järgmine lause eesti keelde: '*Policy was ruined by politics*,' ütleb Ilves.“ [ERR. Ilves: üritan lugemise asemel panna lõpuks kirja seda, mida olen tahtnud öelda. (28.01.2025). – https://kultuur.err.ee/1609588466/ilves-uritan-lugemise-asemel-panna-lopuks-kirja-seda-mida-olen-tahtnud-oelda (09.04.2025)] Siinkirjutaja nõustub, mistõttu tuleb väljendi *policymakers* tõlkimisel piirduda vastega poliitikakujundajad. Siia hulka võivad kuuluda nii poliitikud kui ka ametnikud. Heaks näiteks on riigi julgeolekuteabe hanke ja analüüsi kava (JAS § 9 lg 2), mille koostamine toimub täitevvõimu poliitikute ning Kaitsepolitseiameti, Välisluureameti ja kaitseväeluure ametnike koostöös.
[328] Zegart, A. Spies, Lies, and Algorithms. The History of American Intelligence. Princeton University Press 2022, lk 79.
[329] *Business intelligence*.
[330] *Competitive intelligence*.
[331] SCIP – *Strategic Consortsium of Intelligence Professionals*. (Varem: *Strategic and Competitive Intelligence Professionals*)
[332] SCIP. Code of Ethics (30.04.2014).
– https://web.archive.org/web/20141013115335/https://www.scip.org/CodeOfEthics.php (12.02.2025).
[333] Madureira, L. jt. Competitive intelligence: A unified view and modular definition. – Technological Forecasting and Social Change 2021/173.

Luureinfo kogumisega tegelevad muuhulgas terroriorganisatioon Hamas[334], Ameerika Ühendriikide mootorrattajõugud[335] ja Mehhiko narkokartellid[336]. Kokkuvõtvalt võiks väita, et luureinfo kogumisest on huvitatud kõik isikud või isikute ühendused, kes tegutsevad rahvusvahelises keskkonnas, kus luureinfost sõltub ellujäämine – kas füüsiline või majanduslik.

Tavaarusaam „luurele minekust“[337] ei taba oluliselt laiema luuretegevuse mõiste sisu. Luuramise all selles kitsamas tähenduses mõeldakse sõjaväelist tegevust, mida tuntakse „reke“[338] (*reconnaissance*) nime all. Cambridge'i sõnaraamatu järgi on tegemist „protsessiga, mille käigus hangitakse teavet vaenlase jõudude või positsioonide kohta saates välja väikeseid sõdurite üksusi või kasutades lennuvahendeid[339] jne“[340]. C. L. Foxi väitel viivad Vene sõjaväeluurele alluva Spetsnazi 8–14-mehelised kompaniid ellu „sügavaid rekkeoperatsioone [...] vaenlase tagalas“[341]. Foxi sõnul on nende tegevus võrreldav Ameerika Ühendriikide merejalaväe rekkeüksustega[342]. Eesti kaitseväes tegeleb lahinguväljal teabekogumisega luurepataljon, mille alla kuuluvad inimluuregrupp, tehnilise luure kompanii ja

[334] U.S. Department of State. Foreign Terrorist Organizations. – https://www.state.gov/foreign-terrorist-organizations/ (11.02.2025); European Council on Foreign Relations. Mapping Palestinian Politics. Security Forces. Internal Security Force (ISF) – Hamas. – https://ecfr.eu/special/mapping_palestinian_politics/internal_security_force/ (11.02.2025).

[335] Ameerika mootorrattajõugud kasutavad uute liikmete värbamisel erajuurdlusbüroode abi taustakontrollide läbiviimisel. Kuid mitte ainult. Arvestades, et märkimisväärne hulk mootorrattajõukude liikmeid on endised sõjaväelased ei ole välistatud, et jõukudel on ka endal luure- ja vastuluurevõimekus. Väitele annab kinnitust endine CIA luureametnik Matthew Hedger, kes mitteametliku kattega (*non-official cover*) luurajana liitus varjatult mootorrattajõuguga osana missioonist võimaldada Ameerika Ühendriikide luurekogukonnal finantseerida oma operatsioone. Vt lähemalt: Mobley, B. W., Wege, C. A. Counterintelligence Vetting Techniques Compared across Multiple Domains. – International Journal of Intelligence and Counterintelligence 2021/34 (4), lk 690; Rambo, R., Holder, D. UnIntelligence. The Corporate Counterintelligence Podcast. Episode 13 with Matthew Hedger (21.12.2024). 1:01:00 jj – https://open.spotify.com/show/20KFuFQNMbSW6ubqS3Z88r (11.04.2025); Trusted Strategic Solutions. Expertise. Matthew Hedger. – https://tss.llc/expertise/ (11.04.2025).

[336] Uurivaid ajakirjanikke ühendava võrgustiku Forbidden Stories väitel on kartellid enda käsutusse saanud Mehhiko politsei kasutuses olnud Iisraeli äriühingu NSO Group luuretarkvara Pegasus. Vt lähemalt: Schilis-Gallego, C., Lakhani, N. 'It's a free-for-all': how hi-tech spyware ends up in the hands of Mexico's cartels. The Guardian 07.12.2020. – https://www.theguardian.com/world/2020/dec/07/mexico-cartels-drugs-spying-corruption (11.02.2025).

[337] Sedasorti arusaam luurest kumab läbi E. Kergandbergi Juridica artikli pealkirjast: Luurates „Teeme ära!“ meeskonnaga kevadisel jälitusmaastikul. – Juridica 2020/3, lk 210–221.

[338] Lühendatult inglise keeles: *recon* või *recce*. Vt lähemalt: Eesti Keele Instituut. Reke. – https://sonaveeb.ee/search/unif/dlall/dsall/reke/1/est (11.02.2025).

[339] Näiteks Ameerika Ühendriikide luurekogukonda kuuluv *National Reconnaissance Office* tegeleb satelliitide arendamise ja haldamisega: https://www.nro.gov/ (11.02.2025).

[340] Cambridge Dictionary. Reconnaissance. – https://dictionary.cambridge.org/dictionary/english/reconnaissance (19.04.2025).

[341] Fox, C. L. Hybrid Warfare. The Russian Approach to Strategic Competition and Conventional Military Conflict. Four Minute Men Books 2023, lk 176. Curtis L. Fox on endine USA sõjaväe eriüksuse (*Green Berets*) liige ja praegune USA kaitseministeeriumi ametnik: https://www.hybridwarfare.info/the-author-2 (11.02.2025).

[342] Marines. Third Force Reconnaissance Company. – https://www.marforres.marines.mil/Units/4th-Marine-Division/3rd-Force-Reconnaissance-Company-/ (11.02.2025).

rekkekompanii.[343] Kaitseväe käsitluses on rekkekompaniil kitsam roll „viia läbi luure- ja snaiprialast väljaõpet“[344].

Lisaks rekkele kuulub Spetsnazi ampluaasse ka sabotaaž, väidavad C. L. Fox ja M. Galeotti.[345] „Spetsnazi üksused on eriti sobivad ’poliitilise sõjapidamise’[346] operatsioonideks, peegeldades Moskva erilist huvi ühildada tavapärased sõjalised missioonid varjatud ’aktiivsete meetmetega’,“ ütleb Galeotti. Spetsnazi sabotaažipädevus ja poliitiline sõjapidamine on heaks vahelüliks välistamaks tegevusi, mida tihtipeale liigitatakse luuretegevuse alla. Nimelt tegevusi, millele Ameerika Ühendriikide õiguskorras vastab legaaldefinitsioon „varjatud tegevus“ (*covert action*), ning mille algatamise otsustab president ja viib ellu presidendi poolt määratud valitsusasutus.[347] Selleks valitsusasutuseks võib olla CIA, aga mitte tingimata.[348] Varjatud tegevuste näol on tegemist presidendi „kolmanda valikuga“[349] olukordades, kus diplomaatia ei ole andnud tulemust ja sõja kuulutamine on välistatud.

Väljaspool otsest sõjategevust tegelevad Venemaal mõjutustegevuste, sabotaažiaktide ja atentaatidega FSB (vene k *Федеральная служба безопасности*) ja GU[350] (vene k *Главное управление Генерального штаба Вооружённых сил Российской Федерации*).[351] R.

[343] Eesti Kaitsevägi. Luurepataljon. – https://mil.ee/uksused/maavagi/diviis/luurepataljon/ (11.02.2025).
[344] Samas.
[345] Fox, C. L, lk 175–177; Galeotti, M. Spetsnaz: Operational Intelligence, Political Warfare, and Battlefield Role. Marshall Center Security Insight, no. 46, 2020 veebruar. – https://www.marshallcenter.org/en/publications/security-insights/spetsnaz-operational-intelligence-political-warfare-and-battlefield-role-0 (12.02.2025).
[346] Termin pärineb George Kennanilt: U.S. Department of State. Office of the Historian. 269. Policy Planning Staff Memorandum. (Washington, May 4, 1948). – https://history.state.gov/historicaldocuments/frus1945-50Intel/d269 (12.02.2025). Kaasaegne sünonüüm on hübriidsõda (*hybrid warfare*).
[347] 50 U.S. Code § 3093 – Presidential approval and reporting of covert actions. Sama sätte (e): *„ ’covert action’ means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly“*. Sama sättega on *covert action* mõiste alt välistatud luureinfo kogumine, vastuluure tegevused jms. tavapärased tegevused. A. Sinisalu kasutab enda doktoritöös mõistet varjatud e salaoperatsioonid. Vt lähemalt: Mõjutustegevuse piirid rahvusvahelises õiguses. Doktoritöö. Tartu: Tartu Ülikool 2012, lk 36–37.
[348] 50 U.S. Code § 3093(a)(3).
[349] Johnson, L. K. The Third Option: Covert Action and American Foreign Policy. OUP 2022.
[350] Varem GRU (vene k *Главное разведывательное управление*).
[351] FSB kohta: Shulipa, Y. How Putin Kills Abroad. Vilnius: International Center for Civic Initiatives „Our Home“, 2021. (Viidatud: Riehle, K. P. The Russian FSB. A Concise History of the Federal Security Service. Georgetown University Press 2024, lk 90); Mõned näited GRU kohta: ERR. Siseministri ja ajakirjaniku auto lõhkumises korraldas venemeelne aktivist. (05.12.2024). – https://www.err.ee/1609542391/siseministri-ja-ajakirjaniku-auto-lohkumise-korraldas-venemeelne-aktivist (11.02.2025); Richterova, D. jt, lk 10–21; Dobrokhotov, R., Grozev, C., Weiss, M. Afgantsy Redux: How Russian military intelligence used the Taliban to bleed U.S. forces at the end of America’s longest war. The Insider 08.01.2025. – https://theins.ru/en/politics/277723 (11.02.2025); Bellingcat. How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine. (26.04.2021). – https://www.bellingcat.com/news/uk-

Bergmani ulatuslik käsitlus Iisraeli tapmisoperatsioonidest näitab, et Iisraelis on nimetatud tegevused peamiselt Mossadi korraldada. [352] Erinevalt Iisraeli, Venemaa või Ameerika Ühendriikide eriteenistustest ei ole Hiina eriteenistused jõudnud maailmameediasse atentaatide ja sabotaažiaktide tõttu. Küll aga kirjeldab A. Joske üksikasjalikult Hiina julgeolekuministeeriumi ulatuslikke mõjutusoperatsioone lääne eliidi seas. [353] Ühtlasi on Hiina üks agressiivsemaid välismaal elavate kodanike represseerijaid. „Hiina viib ellu ühte keerulisemat, globaalsemat ja ulatuslikumat piiriülese repressiooni kampaaniat maailmas, " ütleb Freedom House. [354]

Vahemärkusena: kuigi Ameerika Ühendriigid ja Iisrael asuvad Eesti Vabariigiga sarnases väärtusruumis on nimetatud riikidel ka teatav ühisosa Venemaa ja Hiinaga. Nimelt korraldavad kõik mainitud riigid varjatud operatsioone. Samuti ei tunnusta ükski neist Rahvusvahelise Kriminaalkohtu jurisdiktsiooni.[355]

Varjatud operatsioone tuleks eristada luuretegevusest. M. Purre leiab, et luuretegevusega kaasneb „ühe mehe vabadusvõitleja on teise mehe terrorist"-stiilis paradoks: „[O]ma riigis õilis ja väärikas luuraja, võõras riigis spioon ja kurjategija"[356]. Kindlasti on võõrriigis tegutsev luuraja võõrriigi seaduste järgi kurjategija. Kuid siinkohal tasub mõelda, mis sorti kurjategijaga on tegemist. Teisisõnu, milliste kuritegude toimepanemist kodumaa nimel ühelt luurajalt oodatakse. Endine CIA luureametnik J. Atwell, kelle kogemused pärinevad külma sõja päevilt, leiab, et CIA spetsialiseerumine varjatud operatsioonidele pärast 11. septembri terrorirünnakuid muutis CIA kultuuri: luureinfo spetsialistid suruti organisatsioonist välja ning

and-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/ (11.02.2025).

[352] Bergman, R. Rise and Kill First. The Secret History of Israel's Targeted Assassinations. John Murray 2018. Mossad viis ellu ka Hezbollah vastu suunatud nn piiparirünnaku: Stahl, L. Former agents from Israel's Mossad detail how they build an sold explosive pagers to Hezbollah terrorists. CBS News 22.12.2024. – https://www.cbsnews.com/news/israel-former-mossad-agents-detail-explosive-pagers-hezbollah-terrorists-plot-60-minutes-transcript/ (11.02.2025).

[353] Joske, A. Spies and Lies. How China's Greatest Covert Operations Fooled the World. Hardie Grant Books 2022.

[354] Freedom House. Case Studies: China. (2021) – https://freedomhouse.org/sites/default/files/2021-02/FH_TransnationalRepressionReport2021_rev020221_CaseStudy_China.pdf (19.04.2025). FBI nimetab kõnealust nähtust *transnational repression* ning peab seda ohuks Ameerika Ühendriikide suveräänsusele. Vt lähemalt: FBI. Counterintelligence. Transnational Repression. – https://www.fbi.gov/investigate/counterintelligence/transnational-repression (19.04.2025).

[355] International Criminal Court. The States Parties to the Rome Statute. – https://asp.icc-cpi.int/states-parties (09.04.2025).

[356] Purre, M. Riigireetmine ja riigireetur. – Juridica 2020/2, lk 81.

värbama asuti erioperatsioonide taustaga sõjaväelasi.[357] Siit võib järeldada, et luureinfo kogumine nõuab erinevaid oskusi ja isikuomadusi kui varjatud operatsioonide elluviimine. Järeldusele annab kaalu Välisluureameti peadirektori Kaupo Rosina kogemus: „Kunagi kusjuures tegime ka mingisugused isiksuse testid. Siis ma avastasin, et eriop[eratsioonide] tüüp ja inimallika-luure tüüp on kaks erinevat hõimu. Täiesti erinevad inimesed on need.“[358]

CIA agendijuht „valib, hindab, arendab, värbab ja käitleb“[359] võõrriikide kodanikke, kellel on „juurdepääs välisteabele, mis on elutähtis USA välispoliitika ja rahvusliku julgeoleku otsustajatele“[360]. Teisisõnu: agendijuhi eesmärk on veenda võõrriikide kodanikke andma üle väärtuslikku infot, st reetma oma riiki. Kuidas agendijuhid seda täpselt teevad, kuulub julgeolekuasutuse meetodite ja taktika alla, mistõttu ei ole võimalik seda teaduslikult käsitleda.[361] Küll aga on eluliselt usutav, et agendijuhi kunst on erinev neist kunstidest, mida peab valdama inimene, kes saadetakse külvama hirmu, hävitama vara ja võtma elu. Lihtsustatult: kui luurajal on ehk kasu kelmi või varga kutseoskustest, siis sabotaaži ja tapmisoperatsioonide toimepanija peab olema terrorist ja mõrvar. Ei ole mõistlik panna kelme ja mõrvareid ühte potti; hoolimata sellest, et ühisosaks on petmine ja mõrvamine riigi nimel.

Vajadus eristada klassikalist luuretegevust ja erioperatsioone ei ole pelgalt akadeemiline. Julgeoleku tagamisel ei tohiks alahinnata informeeritud avalikkuse osatähtsust. A. Zegart räägib luurealasest „hariduskriisist“ Ameerika Ühendriikides.[362] Lühidalt: arusaamad julgeolekuasutuste tööst tulevad televiisorist ja televiisor valetab. Endise CIA luureametniku J. Sipheri sõnul seisneb Hollywoodi läbikukkumine spionaažižanri muutmises osaks *action*-filmide žanrist.[363] Või nagu ütleb KAPO töökuulutus: „Filmides ja teleseriaalides kujutatud

[357] Grey Dynamics. Senior CIA Ops Officer John Atwell on Culture Change, Working with Five Eyes and Career Advice – Episode 48. 9:10 – The shift towards paramilitarism at CIA after 9/11. – https://podcasts.apple.com/ee/podcast/grey-dynamics/id1637438384?i=1000650118299 (09.04.2025). Atwelli hinnangul kahjustas see CIA luurevõimekust.
[358] Käsper, R. Eriväelase jutud. Intervjuu Kaupo Rosinaga. (14.03.2025). – https://tasku.delfi.ee/podcast/ff0c1df9-082d-414f-b06d-f48decd50f45/ (04.03.2025).
[359] CIA. Careers. Jobs. Case Officer. – https://www.cia.gov/careers/jobs/case-officer/ (11.02.2025). Tegemist on nn agenditsükliga, vt lähemalt: KAPO aastaraamat 2018, lk 21. Kuigi loogilisem oleks kasutada mõistet „agendi elutsükkel“.
[360] Samas.
[361] Välisluureameti töökuulutus luureinfo spetsialistile nõuab kandidaadilt oskuste ja isikuomaduste osas: 1) „teeme ära“ suhtumist; 2) vestlustasemel vene ja inglise keelt; 3) head suhtlusoskust ja meeskonnamängu oskust; 4) huvi maailmas toimuva vastu; 5) kiiret õppimisvõimet, uudishimu ja avatud meelt. [Välisluureamet. Tööle välisluureametisse. Luureinfo spetsialist. – https://valisluureamet.ee/toole.html (12.02.2025).]
[362] Zegart, A. Chapter 2.
[363] Sipher, J. The Car Chase to Nowhere: Hollywood & Spies. Tomorrow's Affairs 05.02.2025. – https://tomorrowsaffairs.com/the-car-chase-to-nowhere-hollywood-spies (06.03.2025).

julgeolekuasutuste või spioonide lummaval elul ei ole reaalsusega kuigi palju ühist“[364]. Kui ekslikel arusaamadel lastakse vabalt levida, jõuavad need üks hetk riigivalitsejateni ning lõpuks ka seadustesse. A. Zegart kirjeldab tabavalt, kuidas teleseriaalis „24“ serveeritud stsenaarium viitsütikuga pommist, mille kahjutuks tegemiseks tuleb inimesi piinata, jõudis ajapikku kõiki kolme riigivõimu harusse: Kongressi, Valgesse Majja ja isegi Ülemkohtusse.[365]

Kui ka Eestis hakkaks levima sellised arusaamad luuretööst, võib üks hetk mõnel erakonnal tekkida mõte kaotada julgeolekuasutuste seaduse § 3 lg 1 p-st 2 keeld, mille kohaselt „teabe kogumise ja töötlemisega ei või ohustada isiku elu ja tervist [...]“.[366] Võrdlusena: Kaitseväe korralduse seaduses [367] sellist piirangut ei ole. [368] Seega: et ühiskondlikud arusaamad julgeolekuasutuste tööst oleksid kammitsetud reaalsusest on oluline eristada luuretegevust, sõjalist tegevust ja halli ala, mis jääb nende vahele.

Veel tuleks peatuda spionaaži ja salakuulamise mõistetel. Eesti Keele Instituudi järgi on spionaaž ja salakuulamine sünonüümid. [369] N. Polmari ja T. Alleni erialaentsüklopeedia kohaselt eristab spionaaži ja luuretegevust asjaolu, et spionaaž on „luuretegevus, mille eesmärk on teabe kogumine salajastel meetoditel“[370]. Sama väidab ka H. Tiido tuginedes J. Rislakki[371] käsitlusele: „Luuramine on laias laastus seaduslik tegevus, spionaaž on aga ebaseaduslik aktiivne tegevus info hankimiseks spioonide, salaagentide või tehniliste vahenditega.“ [372] Ühesõnaga: luuretegevus kui kasuliku teabe kogumine poliitikakujundajatele on üldmõiste, spionaaž kui ebaseaduslik luuretegevus on erimõiste.

[364] KAPO. Tule tööle. – https://kapo.ee/et/kandideeri/ (06.03.2025).
[365] Zegart, A., lk 40–43.
[366] Arnold Sinisalu: „Kartma peaks hakkama, siis kui – on üks poliitik, kes on sellest ka natukene rääkinud – kui tullakse välja algatusega, et võetakse JAS-ist välja teatud piirangud, et teabehange ei tohi kahjustada inimese elu, tervist, vara ja keskkonda.“ Vt: 38. Eesti õigusteadlaste päevade paneel „Jälitus ja teabehange kriminaalmenetluses“ (26.09.2024). – Tartu Ülikooli Televisioon. 38. Eesti õigusteadlaste päevade paneeli „Jälitus ja teabehange kriminaalmenetluses“ videosalvestis (26.09.2024). – https://uttv.ee/naita?id=35990 (21.04.2025).
[367] Kaitseväe korralduse seadus. – RT I, 12.12.2024, 5.
[368] Küll aga on keelatud anda käsku, mille „täitmine on põhjendamatult ohtlik [...] teiste isikute elule, tervisele [...]“ (KKS § 34 lg 1 p 4). Samas tuleb keelatud käsku siiski täita (KKS § 34 lg 2). Tühist käsku, millega kohustatakse toime panema süütegu, täitma ei pea (KKS § 33 lg 1 p 1, lg 3).
[369] Eesti Keele Instituut. Spionaaž. – https://sonaveeb.ee/search/unif/dlall/dsall/spionaa%C5%BE/1/est (11.02.2025).
[370] Polmar, N., Allen, T. B. Spy Book: The Encyclopedia of Espionage. 2. Ed. New York: Random House Reference 2004, lk HVI. (Viidatud: Purre, M. Riigireetmine ja riigireetur, viide 34).
[371] Risklakki, J. Luure ja spionaaž. Doktriinid, operatsioonid, agendid. 2023.
[372] ERR. Harri Tiido: luuramisest ja spioneerimisest. (24.09.2024). – https://www.err.ee/1609468270/harri-tiido-luuramisest-ja-spioneerimisest (11.02.2025).

Ühelt poolt on sellise vaheteo tunnustamine õigusteaduslikus arutelus keeruline, kuivõrd karistusseadustiku järgi on kriminaliseeritud nii salakuulamine ehk spionaaž (KarS § 234) kui ka Eesti Vabariigi vastane luuretegevus (KarS § $234^2$). Teiselt poolt täpsustab KarS § $234^2$, et seadusevastane on just Eesti Vabariigi vastane luuretegevus. Seega: luuretegevus, mis ei ole suunatud Eesti Vabariigi vastu, võiks olla endiselt lubatud – või vähemasti mitte kriminaalne.

Seadusliku luuretegevuse näiteks võib tuua äri- või konkurentsiluure, mis ei riku EL andmekaitsemäärust [373] ega kvalifitseeru eraviisiliseks jälitustegevuseks (KarS § 137), ärisaladuse ebaseaduslikuks saamiseks (KarS § 377), arvutisüsteemile ebaseaduslikult juurdepääsu hankimiseks (KarS § 217) vms. Samuti võiks iseenesest olla seaduspärane info kogumine, mida tehakse enda õiguste või positsiooni kaitsmiseks õigusvaidluses, poliitiliste erakondade konkurentsis või investeeringute tegemisele eelneva auditi ehk *due diligence*'i raames. Tõsi, võib tekkida küsimus, kas KarS § 137 jätab üldse ruumi seaduslikuks luuretegevuseks Eesti Vabariigis. Aga sellele küsimusele vastamine vajaks eraldi uurimust.

Õigusteaduslik arutelu nõuab täpset keelekasutust, mistõttu kasutan edaspidi seadusevastasele luuretegevusele viitamisel spionaaži mõistet. Eelnevast tulenevalt oleks kohane käsitleda lühidalt ka vastuluure mõistet. Sest kui spionaaž on ebaseaduslik, siis miks mitte kasutada mõistet vastuspionaaž või spionaažitõrje (*counter-espionage*)?

Esiteks soovitab EKI riigikaitseterminite andmebaas vältida termini vastuspionaaž kasutamist. Põhjus võib peituda selles, et mõiste ei ole praktikas leidnud kasutust.[374] Sama võib väita suts suupärasema „spionaažitõrje" kohta. Julgeolekuasutuste kodulehtede ja aastaraamatute kõrval annab sellest märku ka õiguskord, mis kasutab läbivalt mõistet vastuluure.[375] JAS § 6 p 2 kohaselt seisneb vastuluure riigi vastu suunatud luuretegevuse ennetamises ja tõkestamises.

[373] Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016. – ELT L 119/1, 4.5.2016.
[374] KAPO ja Välisluureamet, mis täidavad Eesti õiguskorras vastuluure-ülesandeid (JAS § 6 p 2, JAS § 7 p 3,), kasutavad mõistet „vastuluure". Vt lähemalt: https://kapo.ee/et/content/luure-ja-vastuluure/ (11.02.2025) ja Välisluureameti ohuhinnangud „Eesti rahvusvahelises julgeolekukeskkonnas" 2022–24. KKS § 36 p 3 kohaselt täidab vastuluurega sarnaseid ülesandeid ka Kaitseväeluure, kes nimetab seda tegevust „julgeolekuluureks". „Julgeolekuluure mõiste: luureteave spionaaži, sabotaaži, õõnestustegevuse, terrorismi või organiseeritud kuritegevusega tegelevate või tegeleda võivate vaenulike organisatsioonide või isikute identiteedi, võimete ja kavatsuste kohta." Vt lähemalt: Eesti Kaitsevägi. Luurekeskus. Julgeolek. – https://mil.ee/uksused/luurekeskus/julgeolek/ (11.02.2025); Eesti Kaitsevägi. Julgeoleku tagamine luure abil. – Ajakiri Sõdur 2025/1, lk 13–15.
[375] Nt JAS § 6 p 2, RSVS § 52 lg 3 p 2.

## 3.2 Majandus-, tööstus- ja ärispionaaži mõisted

Tööstusspionaaž on spionaaži eriliik, mistõttu kuulub tööstusspionaaži ennetamine ja tõkestamine vastuluurega tegelevate asutuste pädevusse. Eestis tegeleb vastuluurega peamiselt KAPO, kitsamas ulatuses Välisluureamet.[376] Ameerika Ühendriikides tegelevad vastuluurega mitmed erinevad valitsusasutused, mille eraldi üles loetlemine ei ole otstarbekas. [377] Ühendriikide „juhtivaks vastuluureasutuseks“[378] nimetab end FBI. Muuhulgas kuulub FBI ülesannete hulka tööstusspionaaži ennetamine ja tõkestamine.[379]

Kuna sarnaselt KAPO-ga on FBI politseiliste õigustega julgeolekuasutus, mis võimaldab asutusel „liikuda sujuvalt luureinfo kogumiselt tegutsemisele“ [380] , tegeleb FBI ka tööstusspionaaži kohtueelse menetlusega. Seda põhjusel, et tööstusspionaaži näol on tegemist Ameerika Ühendriikide vastu suunatud kuriteoga, mille uurimise on justiitsminister (*Attorney General*) usaldanud FBI-le. [381] Arvestades, et KAPO ja FBI on olemuselt sarnased asutused, mille ülesandeks on ennetada, tõkestada ja uurida tööstusspionaaži, on sobilik otsida esmamuljet nende asutuste leksikonist.

KAPO eristab majandusluuret ja tööstusspionaaži: „Majandusluure tunneb huvi välisriigi majandusressursside, majandustegevuse ja majanduspoliitika vastu tervikuna, hõlmates nii tootmist, tarbimist, finantse, maksundust kui ka teisi rahvusvahelise majanduse aspekte.“[382] Seevastu tööstusspionaaži mõiste on „kitsam ja hõlmab pigem omandiõiguste (informatsioon, tehnoloogia) ebaseaduslikku hankimist. Lihtsalt väljendudes: uue tehnoloogia

[376] JAS § 6 p 2, § 7 p-d 2–4.
[377] Ülevaate annab presidendi täitevkorraldus EO 12333: ODNI. Office of the General Counsel. Intelligence Community Legal Reference Book. Digital Edition, 2024, lk 682–708. (FBI pädevust puudutav asub lk 696–697). – https://www.dni.gov/files/documents/OGC/IC-Legal-Reference-Book-2024.pdf (11.02.2025)
[378] FBI. FAQ. What is the FBI’s foreign counterintelligence responsibility? – https://www.fbi.gov/about/faqs/what-is-the-fbis-foreign-counterintelligence-responsibility (09.04.2025).
[379] FBI. Counterintelligence. – https://www.fbi.gov/investigate/counterintelligence (09.04.2025).
[380] FBI. FAQ. Where is the FBI’s authority written down? – https://www.fbi.gov/about/faqs/where-is-the-fbis-authority-written-down (11.02.2025); Politseiliste õigustega ja ilma politseiliste õigusteta julgeolekuasutuste kohta vt: Heldna, E. Julgeolekuasutuste kogutud informatsiooni kasutamine kriminaalmenetluses ja jagamine uurimisasutustega. – Juridica 2016/10, lk 718–726.
[381] 28 U.S. Code § 533(1) koosmõjus 18 U.S. Code §-iga 1831; U.S. Department of Justice. Criminal Resource Manual. Introduction to the Economic Espionage Act. – https://www.justice.gov/archives/jm/criminal-resource-manual-1122-introduction-economic-espionage-act (20.04.2025). Tsitaat: *„Congress, recognizing the importance of the protection of intellectual property and trade secrets to the economic health and security of the United States, enacted the Economic Espionage Act of 1996, Pub.L. 104-294, 110 Stat. 3489 (October 11, 1996).“* FBI tegevuse õiguslike aluste kohta vt ülal: FBI. FAQ. Where is the FBI’s authority written down?
[382] Kaitsepolitseiamet. Mida peaks teadma tööstusspionaažist? – https://web.archive.org/web/20191103141731/https://www.kapo.ee/et/content/mida-peaks-teadma-t%c3%b6%c3%b6stusspionaa%c5%beist.html (06.04.2025).

väljatöötamiseks ei hakata ressursse kulutama, vaid see varastatakse konkurentide käest. Tööstusspionaaži alla käib ka korporatiiv- ehk äriluure kus üritatakse varastada ideid, ärisaladusi jne.“[383] KAPO kasutab siin küll luure ja spionaaži mõisteid läbisegi, kuid sisuliselt mõeldakse ikkagi spionaaži ehk Eesti Vabariigi vastu suunatud luuretegevust, mille ennetamine ja tõkestamine on KAPO kohustus.[384] Veel lisab KAPO: „Majandusluure ja tööstusspionaaži kaudu püütakse tugevdada riigi majandust.“ [385] Järelikult on KAPO järgi majandus- ja tööstusspionaaži näol tegemist välisriigist lähtuva ohuga.

FBI määratleb majandusspionaaži [386] ehk *economic espionage*’i järgmiselt: „[V]älisvõimu toetatud või koordineeritud luuretegevus, mis on suunatud USA valitsuse või USA ettevõtete, asutuste või isikutele vastu. Selle eesmärk on ebaseaduslikult või varjatult mõjutada tundlikke majanduspoliitilisi otsuseid või hankida ebaseaduslikult tundlikku finants-, kaubandus- või majanduspoliitilist teavet; konfidentsiaalset majandusteavet või olulisi tehnoloogiaid. See vargus, kasutades avalikke ja varjatud meetodeid, võib anda välismaistele organisatsioonidele juurdepääsu olulisele konfidentsiaalsele majanduslikule teabele murdosa eest selle tegelikust uurimis- ja arenduskulust, põhjustades märkimisväärseid majanduslikke kahjusid.“[387]

Ebamäärasus KAPO määratlustes on tingitud asjaolust, et Eesti õiguskorras puuduvad majandus-, tööstus- või ärispionaaži legaaldefinitsioonid. FBI seevastu peab lähtuma Ameerika Ühendriikide föderaalkoodeksist, mis eristab majandusspionaaži (*economic espionage*) ja ärisaladuste vargust (*theft of trade secrets*). Kahte kuritegu eristab toimepanija: Kui välisriik, välisriigi agent või välisriigi kontrolli all olev entiteet omandab USA valitsuse, ettevõtete, asutuste või isikute ärisaladusi, on tegemist majandusspionaažiga (18 U.S. Code § 1831). Kui võõramaine element puudub, on tegemist ärisaladuste vargusega (18 U.S. Code § 1832). Oluline on märgata, et ründeobjektiks on mõlemal juhul ärisaladus, mis on määratletud võimalikult laialt [18 U.S. Code § 1839(3)].

---

[383] Samas.
[384] Seda võib välja lugeda KAPO seisukohast: „Kaitsepolitseiametil on julgeolekuasutusena Eesti majandusjulgeoleku tagamisel täita vastutusrikas roll: riik on teinud meile kohustuseks välisriigist lähtuva majandusluure ja tööstusspionaaži [...] takistamise [...] Majandusluure ja tööstusspionaaži tõkestamisel oleme täheldanud välisriikide eriteenistuste huvi eelkõige energiasektori vastu.“ KAPO. – https://web.archive.org/web/20201021122615/https:/www.kapo.ee/et/content/majandusjulgeolek.html (06.04.2025).
[385] Samas.
[386] Lotrionte, C.
[387] FBI. What is „economic espionage“? – https://www.fbi.gov/about/faqs/what-is-economic-espionage (12.02.2025). Tööstusspionaaži ehk *industrial espionage*’i mõistet FBI ei kasuta. Küll kasutab seda mõistet Defense Production Act of 1950. Vt lähemalt: 50 U.S. Code § 2170(k)(1)(B).

KAPO käsitlusest on võimalik välja lugeda järgmist:

1) Majandusspionaaži eristab tööstusspionaažist ründeobjekt. Majandusspionaaži ründeobjekt on riigi kohta käiv strateegiline informatsioon. Tööstusspionaaži ründeobjekt on aga omandiõigused (informatsioon, tehnoloogia).
2) KAPO püüe eristada tööstus- ja ärispionaaži ründeobjekti alusel on ebaõnnestunud, kuivõrd pole selgelt arusaadav, kuidas erinevad üksteisest „omandiõigused (tehnoloogia, informatsioon)“ ning „ideed, ärisaladused jne“.
3) Majandus- ja tööstusspionaaži eesmärk on tugevdada riiki, mistõttu on mõlemal juhul tegemist välisriigist lähtuva ohuga.

Mõistagi pole mõistlik loetleda kõikide maailma riikide eriteenistuste arusaamasid majandus-, tööstus- ja ärispionaaži mõistetest. Seda enam, et Carl jt on leidnud, et ainult nelja Euroopa Liidu liikmesriigi (Leedu, Holland, Poola ja Ungari) õiguskorras on tööstusspionaaži legaaldefinitsioon ning ainult kolmes riigis (Leedu, Holland ja Ungari) kehtib majandusspionaaži legaaldefinitsioon. [388] Seetõttu pöördume selguse saamiseks teaduskirjanduse poole.

M. Button ja S. Knickmeier on erinevate käsitluste analüüsimisel jõudnud järeldusele, et kõige mõistlikum on eristada majandus- ja tööstusspionaaži toimepanija – või täpsemalt soodustatava isiku – alusel. Nad kirjutavad: „Majandus- ja tööstusspionaaž viitavad ärisaladuste ja konfidentsiaalse teabe sihitamisele [389] või omandamisele kodumaistelt äriühingutelt või riigiasutustelt, et teadlikult soodustada esimesel juhul välisriiki ja teisel juhul eraõiguslikku entiteeti.“[390]

M. Buttoni ja S. Knickmeieri majandusspionaaži definitsioon vastab majandusspionaaži legaaldefinitsioonile Ameerika Ühendriikide föderaalkoodeksis (18 U.S. Code § 1831). Ärisaladuste varguse (18 U.S. Code § 1832) legaaldefinitsioon ühtib M. Buttoni ja S.

[388] Carl, S., Kilchling, M., Knickmeier, S., and Wallwaey, E.
[389] *Targeting*.
[390] Button, M., Knickmeier, S. Economic and Industrial Espionage: Characteristics, Techniques and Response. – The Handbook of Security (ed. M. Gill) Springer 2022, lk 263.

Knickmeieri tööstusspionaaži definitsiooniga. Ühtlasi nähtub kõnealusest käsitlusest, et ärispionaaži mõiste järgi pole tarvidust. Sisuliselt on äri- ja tööstusspionaaž sünonüümid.[391]

M. Buttoni ja S. Knickmeieri järgi on Saksamaal majandusspionaaž karistatav StGB § 99 alusel. [392] Nimelt karistatakse StGB § 99 lg 1 alusel isikut, kes: 1) „osaleb välisriigi luureteenistuse huvides Saksamaa Liitvabariigi vastases luuretegevuses, mis on suunatud faktide, objektide või teadmiste edastamisele või varustamisele“ [393]; või 2) „avaldab välisriigi luureteenistusele või selle vahendajale oma valmisolekut sellises tegevuses osaleda“[394]. Sama sätte teine lõige sätestab kvalifitseeritud koosseisu, mille üheks eelduseks on, et edastatavad esemed on salastatud ametiasutuse poolt või selle ülesandel. StGB § 99 eeskujul kehtestati Eesti õiguskorras KarS § $234^2$ pealkirjaga „Eesti Vabariigi vastu suunatud luuretegevus ja selle toetamine“.[395] Arvestades StGB § 99 ja KarS § $234^2$ kaitsealade sarnasust oleks loogiline nimetada KarS §-i $234^2$ majandusspionaaži kriminaliseerivaks sätteks.

M. Buttoni ja S. Knickmeieri järgi on Saksamaal tööstusspionaaž karistatav GeschGehG § 23 alusel.[396] Tegemist on keerulise struktuuriga viitelise koosseisuga, mis loodi selleks, et võtta õiguskorda üle Euroopa Liidu direktiiv 2016/943[397].[398] Direktiivi art-s 1 sätestatakse normid kaitsmaks ärisaladusi ebaseadusliku omandamise, kasutamise ja avalikustamise eest. Eesti õiguskorras tõi direktiivi vastuvõtmine kaasa KarS §-i 377 täiendamise.[399] Arvestades KarS § 377 kaitseala kattuvust GeschGehG §-iga 23, mida Button ja Knickmeier peavad tööstusspionaaži koosseisuks, oleks loogiline nimetada KarS § 377 samuti tööstusspionaaži koosseisuks Eesti õiguskorras.

---

[391] C. Lotrionte eristab *state-sponsored industrial espionage* ja *industrial espionage*. Esimene on sünonüümne majandusspionaažiga (*economic espionage*) ja teine on sünonüümne ärispionaažiga (*corporate espionage*). Vt Lotrionate, C., lk 452 (joonealune märkus nr 25).
[392] Button, M., Knickmeier, S., lk 269.
[393] StGB § 99 lg 1.
[394] Samas.
[395] 642 SE. Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (terrorismivastase võitluse direktiivi ülevõtmine) eelnõu seletuskiri, lk 6.
[396] Button, M., Knickmeier, S., lk 269.
[397] Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2016/943, 8. juuni 2016, milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset. – ETL L 157/1, 15.06.2016.
[398] WIPO. Overview of national and regional trade secret systems. Germany. – https://www.wipo.int/documents/d/trade-secrets/docs-overview-country-sheets-germany-final.pdf (20.04.2025).
[399] 678 SE. Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seaduse eelnõu seletuskiri. Vastu võetud 21.11.2018. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/9b6f21b8-db1c-436d-a045-326913d80d22/ebaausa-konkurentsi-takistamise-ja-arisaladuse-kaitse-seadus/ (09.04.2025).

KarS § 234[2] nimetamist majandusspionaaži koosseisuks ja KarS § 377 nimetamist tööstusspionaaži koosseisuks takistab Eesti ametkondade seas juba omaks võetud käsitlus, mille kohaselt on tööstusspionaaž võõrriigist lähtuv riigivastane tegevus. KAPO käsitlusest oleme juba rääkinud, kuid samal arusaamal on ka Välisluureamet. 2025. ja 2024. aasta aastaraamatutes räägib Välisluureamet tööstusjulgeolekust, mille määratleb kitsalt kui „salastatud teabe kaitse erasektoris“[400]. Välisluureamet kirjutab: „Ettevõtted peavad üha enam kaitsma salastatud teavet vaenulike riikide tööstusluure eest“[401]. Veel räägib Välisluureamet „tööstusluureohust“, millele on amet enda sõnul aastaraamatutes „läbivalt tähelepanu juhtinud“.[402] Tööstusjulgeoleku mõiste on käibel riigisaladuse ja salastatud välisteabe seaduse muutmise seaduse eelnõus, mille eesmärk on võimaldada juriidilistel isikutel töödelda paindlikumalt salastatud teavet.[403] Tööstusspionaaži mõistet kasutab ka kaitseministeerium 2021. aasta kaitsetööstuspoliitikas.[404]

Kui pidada KarS § 377 tööstusspionaaži koosseisuks ei oleks tööstusspionaaži ennetamine, tõkestamine ja uurimine enam KAPO pädevuses. Seda põhjusel, et JAS § 6 p 2 kohaselt ennetab ja tõkestab KAPO riigi vastu suunatud luuretegevust. Politsei- ja Piirivalveameti (PPA) ja KAPO vahelise uurimisalluvuse määruse alusel on KarS § 377 uurimine PPA alluvuses.[405]

Rahvusvahelises erialakirjanduses omaks võetud käsitluse ülevõtmine võib olla teaduslikus mõttes eelistatud, kuid arvestada tuleb ka kodumaiste tavadega. Juba sissejuurdunud keelekasutuse muutmine võib raskendada suhtlust, mistõttu oleks parem uurida, kas on võimalik võtta aluseks KAPO käsitlus, kuid muuta see õiguslikult arusaadavamaks.

---

[400] Eesti rahvusvahelises julgeolekukeskkonnas 2025, lk 91; Eesti rahvusvahelises julgeolekukeskkonnas 2024, lk 87.
[401] Eesti rahvusvahelises julgeolekukeskkonnas 2024, lk 87.
[402] Samas; Tööstusspionaaži või -luuret mainitakse põgusalt järgmistes aastaraamatutes: 2018. aastal peatükis „Küberohud“ („Hiina tööstusspionaaž“) [Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2018.] 2019. aastal peatükis „Hiina kasvav mõju“ („Hiina küberoperatsioonid toetavad kommunistliku võimupartei ja sõjaväe tegevust ning teevad tööstusspionaaži Hiina tehnoloogiaettevõtete kasuks“) [Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2019.]; 2024. aastal peatükis „Tööstusjulgeolek: salastatud teabe kaitse erasektoris“ („Ettevõtted peavad üha enam kaitsma salastatud teavet vaenulike riikide tööstusluure eest ning riik kaitsma riigisaladust, mis usaldatakse välisettevõtele.“) [Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2024.]
[403] Riigisaladuse ja salastatud välisteabe seaduse, riigihangete seaduse ning riigilõivuseaduse muutmise seaduse (tööstusjulgeolek) eelnõu seletuskiri. Eelnõude infosüsteem (18.09.2024). – https://eelnoud.valitsus.ee/main/mount/docList/7771037e-ded1-492e-928e-01a464e17d27#yDoVThpg (09.04.2025).
[404] Kaitseministeeriumi kaitsetööstuspoliitika, lk 1.
[405] Politsei- ja Piirivalveameti ja Kaitsepolitseiameti vaheline uurimisalluvus. §1 p 1. – RT I, 07.05.2019, 4.

Järgnevalt eeldame, et majandus- ja tööstusspionaaži toimepanijaks on välisriik või selle huvides tegutsev isik.

Ärispionaaži puhul ei tegutseta välisriigi huvides, vaid eesmärk on omandada ebaseaduslikult eelis teiste äriühingute ees. Sisuliselt on tegemist ebaausa konkurentsiga ehk siis olukorraga, kus teiste äriühingute vastu suunatud äri- või konkurentsiluure ületab ebaeetilisuse lävendi ja muutub ebaseaduslikuks. Seega oleks õigem kutsuda KarS §-i 377 ärispionaaži koosseisuks. Meeldejääv näide[406] ärispionaažist pärineb lasteraamatust „Charlie ja šokolaadivabrik", milles šokolaaditootja Willie Wonka on sunnitud sulgema oma vabriku spioonide tõttu, kes üritavad tema retsepte varastada. [407] Kuid šokolaadiäris ei käi karm konkurents ainult muinasjutumaailmas. E. Javersi väitel palkas šokolaaditootja Nestlé töövõtja, kes palkas endistest riigiametnikest alltöövõtjad, kes käisid läbi Marsi peakorteri prügikastid ning panid roiskunud toidu vahelt leitud vettinud paberitükkidest kokku äriühingu-siseseks kasutuseks mõeldud dokumendid.[408]

### 3.3 Majandus- ja tööstusspionaaži ründeobjektid

Eristamaks majandus- ja tööstusspionaaži tuleks uurida lähemalt ründeobjekte. KAPO järgi seisneb majandusspionaaž riigi kohta käiva strateegilise teabe ebaseaduslikus hankimises võõrriigi poolt. Selline teave võib Eesti õiguskorras olla, kas riigisaladus (RSVS § 3 p 1), asutusesiseseks kasutamiseks mõeldud teave (AvTS § 34 jj) või muu avalikult kättesaadav teave. Kui ründeobjektiks on riigisaladus, on tegu karistatav KarS § 232 (riigireetmine) või § 234 (salakuulamine) alusel. [409] Asutusesiseseks kasutamiseks mõeldud teabe kogumise või edastamise puhul tuleb kohaldamisele, kas KarS § 243 (asutusesisese teabe edastamine) või

[406] Kaasaegne näide ärispionaažist globaalses tehnoloogiasektoris: Winkler, R., Brown, E. Accused Tech Spy Says Rival CEO Recruited Him With Offer to Be Like James Bond. The Wall Street Journal 02.04.2025. – https://www.wsj.com/tech/accused-tech-spy-says-rival-ceo-recruited-him-with-offer-to-be-like-james-bond-793483e1 (03.04.2025).

[407] Dahl, R. Charlie ja šokolaadivabrik. Tallinn: Draakon ja Kuu, 2017.

[408] Javers, E. Spies and Co. The New York Times 24.10.2012. – https://www.nytimes.com/2012/10/25/opinion/corporate-espionage-american-style.html (13.02.2025). Vt lähemalt: Javers, E. Broker. Trader. Lawyer. Spy. The Secret World of Corporate Espionage. New York: Harper 2010. (Eelkõige: Chapter Six: The Chocolate War).

[409] Riigisaladuse ja salastatud välisteabe puhul võib teoreetiliselt kõne alla tulla ka KarS § $234^2$, kui salastatud teavet töötleb välisriigi luure- või julgeolekuteenistuse teenistuja või selle huvides või ülesandel tegutsev isik ning see tegevus on Eesti Vabariigi julgeoleku vastane. Teisisõnu, teabe mõistega KarS § $234^2$ lg 1 tähenduses on hõlmatud ka salastatud teave. Vt: 642 SE seletuskiri, lk 6. Siiski tuleks arvestada, et KarS § $234^2$ on subsidiaarne KarS § 232 ja 234 suhtes ning kõnealused kooseisud juba katavad olukordi, kui välismaalane või EV kodanik töötleb salastatud teavet välisriigi huvides. Kirjandusest ei ole võimalik leida ühtegi hüpoteetilist olukorda, kuna saaks kohaldada KarS §-i $234^2$ seoses salastatud teabega. Isiklikult ei oska ka ühtegi sellist situatsiooni välja mõelda.

KarS § $234^2$ (Eesti Vabariigi vastu suunatud luuretegevus ja selle toetamine). Muu avalikult kättesaadava teabe hankimine välisriigi luure- või julgeolekuteenistuse teenistuja poolt, huvides või ülesandel on karistatav KarS § $234^2$ järgi. Arutleda saaks ka selle üle, kas asutusesiseseks kasutamiseks mõeldud teabe või muu avalikult kättesaadava teabe hankimine võiks olla Eesti Vabariigi iseseisvuse ja sõltumatuse või territoriaalse terviklikkuse vastu suunatud vägivallata tegevus. Kui jah, võiks kohaldamisele tulla, kas KarS § 232 või § 233 – olenevalt sellest, kas tegemist on kodaniku või välismaalasega. Järelikult on Eesti õiguskorras olenevalt ründeobjektist potentsiaalseid majandusspionaaži koosseise viis: KarS § 232, § 233, § 234, § $234^2$ ja § 243.

Päevakajaline näide majandusspionaažist: Ameerika Ühendriikides esitati süüdistus Föderaalreservi vanemnõunikule, keda kahtlustatakse Hiina kasuks spioneerimises.[410] „Rogers reetis Föderaalreservile töötades oma kodumaad andes Hiina riigi luureametnikele Ameerika Ühendriikide piiratud juurdepääsuga (*restricted*) finants- ja majandusteavet," ütleb FBI vastuluureosakonna asedirektor K. Vorndran. [411] Justiitsministeeriumi väitel võimaldab kogutud teave Hiinal mõjutada USA turgu – just nagu siseinfoga kauplemine (*insider trading*) – kuivõrd Hiina omab suures hulgas Ameerika Ühendriikide välisvõlga. 2024. aasta seisuga ulatus Ameerika Ühendriikide võlg Hiina ees 816 miljardi dollarini.[412]

KAPO järgi on tööstusspionaaži ründeobjekt omandiõigused (informatsioon, tehnoloogia). Vältimaks ülemäärast arutelu, mis kaasneb abstraktsete mõistete nagu omand, informatsioon ja tehnoloogia lahkamisega, oleks tööstusspionaaži puhul praktilisem rääkida kolmest ründeobjektist: salastatud teave ehk riigisaladus ja salastatud välisteave, ärisaladus ning isikuandmed. Ärisaladuse juurde tuleme hiljem tagasi, aga järgnevalt mõned tähelepanekud salastatud teabe ja isikuandmete kohta.

Riigisaladus kaitsetööstuses võib seisneda kahes kategoorias. Esiteks, riigikaitsealased leiutised ja uuringud ning nende tulemusi käsitlev teave (RSVS § 7 p 6). Teiseks, sõjalise otstarbega asja omadusi, projekteerimist, valmistamist ja kohandamist käsitlev teave (RSVS

[410] U.S. Department of Justice. Former Senior Adviser for the Federal Reserve Indicted on Charges of Economic Espionage. (31.01.2025). – https://www.justice.gov/opa/pr/former-senior-adviser-federal-reserve-indicted-charges-economic-espionage (13.02.2025).
[411] Samas.
[412] Samas.

§ 7 p 6[1]).[413] Riigisaladuse kõrval on kaitsetööstuse äriühingu jaoks aina olulisem salastatud välisteave, ütleb Milremi süsteemide arhitekt S. Lätt.[414] Seda põhjusel, et Eesti kaitsetööstus on ekspordile suunatud tööstusharu ning osalemine välisriikide hangetel eeldab paratamatult kokkupuudet salastatud välisteabega.[415] Välisluureameti sõnul võib salastatud välisteabeks olla ka salastatud tehnoloogia, mida sisaldab relva- või IT-süsteem, mille kaitsevägi või Eesti riigiasutus on hankinud välisriigi kaitsetööstuse ettevõttelt.[416]

Isikuandmete lisandumine tööstusspionaaži ründeobjektide hulka tuleneb M. Buttoni ja S. Knickmeieri tähelepanekust, et tööstusspioonidele pakuvad huvi ka töötajate isikuandmed, nt isiklikud finantsandmed.[417]

Püüe eristada majandus- ja tööstusspionaaži ründeobjekti alusel on keeruline ja Eesti õiguskorras tarbetu. Riigivastaste kuritegude arutelus ei ole oluline, kas kogutav teave on oma olemuselt strateegiline, mis viitaks majandusspionaažile, või puudutab kitsamalt mingit sorti erahuvi (nt riigikaitseline leiutis, ärisaladus), mis viitaks tööstusspionaažile. Oluline on küsida, kas ründeobjektiks on salastatud teave või mitte. Kui tegemist on salastatud teabega, vastutab isik KarS § 232 või 234 alusel. Kui tegemist ei ole salastatud teabega, on kõige tõenäolisem KarS §-i 234[2] kohaldamine.[418] Veel tuleks mainida, et kuigi tööstusspionaaži ründeobjektiks on majandusliku iseloomu või kaubandusliku väärtusega riigisaladus, ei erista karistusseadustik riigisaladust sisu alusel.[419] Karistusõiguslik vastutus järgneb mistahes liiki riigisaladuse ebaseadusliku töötlemise tõttu.

M. Button ja S. Knickmeier eristavad majandus- ja tööstusspionaaži soodustatud isiku alusel. Kui soodustatakse välisriiki, on tegemist majandusspionaažiga. Kui soodustatakse muud isikut (nt konkureerivat äriühingut), on tegemist tööstusspionaažiga. Nagu eelnevalt mainitud ei sobi kõnealune vahetegu eestikeelsetesse aruteludesse, kuna kodumaised julgeolekuasutused juba seostavad tööstusspionaaži välisriigi eriteenistuste tegevusega. Samuti on tööstusspionaaži

[413] Vt lähemalt: 468 SE. Relvaseaduse muutmise ja sellega seonduvalt teist seaduste muutmise seaduse eelnõu seletuskiri, lk 18–19.
[414] Priit Pruksi intervjuu S. Lättiga, 28.01.2025.
[415] Samas.
[416] Eesti rahvusvahelises julgeolekukeskkonnas 2024, lk 87.
[417] Button, M., Knickmeier, S., lk 263.
[418] See ei välista, et tööstusspionaaži toimepanemise raames ei võidaks realiseerida ka teisi karistusseadustiku koosseise. Pikem arutelu sellel teemal allpool punktis 2.5.
[419] Riigisaladuse erinevad liigid on leitavad RSVS §-des 6–10.

mõiste kaudselt heaks kiitnud seadusandja kasutades eelnõus mõistet „tööstusjulgeolek“[420]. Järelikult sobiks eestikeelsesse arutelusse paremini eristus tööstus- ja ärispionaaži vahel. Esimest pannakse toime võõrriigi osalusel, teist mitte.

### 3.4 Tööstusspionaaži meetodid

Enne kui kirjeldame lõplikult tööstusspionaaži tunnuseid oleks sobilik käsitleda mõningaid tüüpjuhtumeid. Kahjuks või õnneks ei leia Eesti kohtupraktikast ühtegi tööstusspionaaži juhtumit. Küll aga ei tähenda see, et tööstusspionaaž Eestit ei ohustaks.

K. Koidumäe andmetel on Eesti kaitsetööstuse ettevõtete toodete vastu tuntud huvi olukordades, kui need on, kas tollilaos kinni või neid esitletakse rahvusvahelistel näitustel.[421] SensusQ esindaja E. Kannike rõhutab samuti tööstusspionaaži ohtu rahvusvahelistel näitustel.[422] Seda eriti Abu Dhabis asetleidval näitusel IDEX, kus osalevad ka Venemaa ja Hiina ettevõtted. [423] E. Kannike hinnangul ümbritses hiljutisel IDEX-il Eesti ettevõtjate väljapanekuid kahtlaselt palju Hiina ettevõtteid.[424] Rääkides Venemaa ettevõtetest torkavad nende esindajate juures silma militaarsoengutega mehed ja modellivälimusega naised.[425] Seejuures veedavad naissoost müügiesindajad pärast näitust aega hotellide *lobby*'des ja baarides, kus nende tähelepanu köidavad just abielusõrmusega meesterahvad.[426] Venemaa eriteenistuste kalduvus kasutada seksuaalsuhteid inimeste sundimisel koostööle on üldteada ning leidnud kasutamist ka Eesti Vabariigi vastu.[427]

Lisaks inimlikele nõrkustele tuleb kaitsetööstuse ettevõtjail arvestada ka tehniliste haavatavustega. E. Kannike sõnul ei reisita välislähetustele isiklike või tööalaste

[420] Riigisaladuse ja salastatud välisteabe seaduse, riigihangete seaduse ning riigilõivuseaduse muutmise seaduse (tööstusjulgeolek) eelnõu seletuskiri.
[421] Priit Pruksi intervjuu K. Koidumäega.
[422] Priit Pruksi intervjuu E. Kannikega 31.01.2025.
[423] Samas.
[424] Samas.
[425] Samas.
[426] Samas.
[427] Harju Maakohus 1-19-991. Meediakajastus: Weiss, M. The Hero Who Betrayed His Country. The Atlantic 26.06.2019. – https://www.theatlantic.com/international/archive/2019/06/estonia-russia-deniss-metsavas-spy/592417/ (02.04.2025). Mainitud kaasusest tulenevalt täiendati riigisaladusele juurdepääsuloa andmisest ja selle kehtivuse pikendamisest keeldumise aluseid järgmise punktiga: „Juurdepääsuluba andmast või selle kehtivust pikendamast võib keelduda füüsilisele isikule, kelle käitumisega võib kaasneda oht väljapressimise või muu surveavalduse objektiks“ (RSVS § 32 lg 2 p 19).

elektroonikavahenditega.[428] Igapäevast ohtu kujutavad veel õngitsuskirjad[429] (*phishing*), millest professionaalsemad kasutavad ära „nullpäeva“[430] (*zero-day*) haavatavusi, ning sotsiaalmeedia. Näiteks suhtlusplatvormist LinkedIn on saanud Hiina meelisvahend info kogumiseks ja värbamiseks, kusjuures oma vastaste suunas suudetakse paisata lausa tööstuslikes kogustes võltskontosid ja agente.[431]

L. Almann toob esile hiljutise skandaali seoses Silicon Valley riskiinvestoriga Hone Capital, mis on FBI uurimise all selgitamaks välja, kas ettevõtet rahastas Hiina valitsus ning kas ettevõte jagas oma portfelliettevõtteid puudutavat teavet Hiina riigiga.[432] L. Almanni väitel on Eesti ettevõtted hiinlastele huvitavad ning taolisi investeeringuteks maskeerunud tööstusspionaaži operatsioone on nähtud ka Eestis, nt Hiinast ja Iraanist.[433] I. Pärnamäe hinnangul kujutavad investorid „mastaapset“ tööstusspionaažiohtu, sest investoritele antakse *due diligence*'i ehk investeeringule eelneva auditi raames väga palju teavet tehnoloogia, inimeste ja edasiste arenguplaanide kohta.[434] „See on jõhker. Sinuga tehakse täis röntgen. Ja mis selle infoga pärast saab? Me ei kontrolli seda mitte kuidagi,“ ütleb I. Pärnamäe.[435] Sealjuures ei pruugi investor ise olla üldse pahauskne, vaid investorist ja tema arvutisüsteemist võib saada tööstusspioonide sihtmärk.[436] I. Pärnamäe sõnul aitaks olukorda parandada see, kui riik teeks ise otseinvesteeringuid tundlikes valdkondades tegutsevatesse äriühingutesse.[437] Vastasel juhul võib tekkida olukord, kus ettevõtja on äriühingu pankroti vältimiseks sunnitud otsima investoreid kohtadest, kus on oht sattuda tööstusspionaaži ohvriks.[438]

---

[428] Priit Pruksi intervjuu E. Kannikega 31.01.2025.
[429] TikTok-ist saadavad isikuandmed võimaldavad Hiinal disainida veenva õngitsuskirja: Eesti rahvusvahelises julgeolekukeskkonnas 2024, lk 77.
[430] Vt lähemalt: Perlroth, N. This is How They Tell Me the World Ends: The Cyberweapons Arms Race. Bloomsbury 2021.
[431] Wong, E. How China Uses LinkedIn to Recruit Spies Abroad. The New York Times 27.08.2019. – https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html (02.04.2025); Sabbagh, D. 20,000 Britons approached by Chinese agents on LinkedIn, says MI5 head. The Guardian 17.08.2023. – https://www.theguardian.com/uk-news/2023/oct/17/up-to-20000-britons-approached-by-chinese-agents-on-linkedin-says-mi5-head (02.04.2025). Vt lähemalt USA valitsuse juhist enda ametnikele: National Counterintelligence and Security Center. Online Targeting of Current & Former U.S. Government Employees. – https://www.dni.gov/files/NCSC/documents/products/2025-04-08-NCSC-FBI-DCSA-OnlineTargetingUSGEmployees.pdf (17.04.2025).
[432] Priit Pruksi intervjuu Lauri Almanniga. Vt lähemalt: Loizos, C. Hone Capital, a Silicon Valley firm, is being probed by the FBI. Tech Crunch 24.09.2024. – https://www.ft.com/content/d94a5467-ebf9-4992-af13-3e71061707a4 (09.04.2025).
[433] Priit Pruksi intervjuu Lauri Almanniga.
[434] Priit Pruksi intervjuu Ingvar Pärnamäega.
[435] Samas.
[436] Samas.
[437] Samas.
[438] Samas.

E. Kannike lisab: „Ka meil [on] olnud kokkupuuteid investorite või fondidega, kes tahavad [...] väga süvitsi *due diligence*'i teha. Ja kui sa tausta natuke kraabid, siis ilmneb, et [see investor] ei ole võib-olla kõige legitiimsem. Või siis [...] nad ei kavatsegi sinusse investeerida ja nad tahavad võimalikult palju sisemisi protseduure ja tehnilist teavet teada ja siis haihtuvad ära. Ja siis tuleb välja, et nende *portfolio*'s[439] on keegi nende enda riigi ettevõte, kes tegeleb sama asjaga."[440] S. Lätt kinnitab, et selliseid katseid on tehtud, aga tema kogemuses on need olnud amatöörlikud ja lihtsasti läbinähtavad.[441]

Kas ohuks võivad olla ka praktikandid? E. Kannike ütleb, et tema ei ole kuulnud, et Eesti geopoliitilised vastased oleks läkitanud meie äriühingutesse praktikante.[442] Küll võivad spioon-praktikante saata konkureerivad äriühingud.[443]

O. Väärtnõu nõustub eeltoodud nimekirjaga ja lisab, et küberturvalisuse ettevõttena paneb neid rohkem muretsema sisekahjur (*insider threat*) kui küberrünnak. Seda eriti, kui vastane suudab pikaajalisele koostööle sundida juhtorgani liikme. Ettevõttena, kelle tooteks on usaldus, tähendaks kompromiteerimine äritegevuse lõppu. Erilise riskina näeb O. Väärtnõu välislähetusi. Olukord on seda ohtlikum, kui äriühing tegutseb rahvusvaheliselt ning märkimisväärne hulk töötajatest viibib regulaarselt väljaspool riigipiire.[444]

Tulles tagasi tööstusspionaaži kohtupraktika juurde leiab hulgaliselt lahendeid Hiina tegevuse kohta Ameerika Ühendriikides. Arvestades, et ka Eesti julgeolekuasutused peavad Hiinat julgeolekuohuks, võiks nende kaasuste analüüs olla õpetlik ka meile.

Kaasus 1. Hiina kodanik Mo Hailong elas Ameerika Ühendriikides, kuid töötas Hiinas asuva suurettevõtte DBN rahvusvahelise äri direktori ametikohal. DBN tütarettevõte Kings Nower Seed tegeles maisi aretamisega. Mo ja tema kaasosalised varastasid Ameerika Ühendriikide põllumajandusettevõtetele Monsanto ja DuPont Pioneer kuuluvatelt maisipõldudelt seemneid

[439] Investeerimisportfell ehk hulk äriühinguid, kuhu investor on investeerinud.
[440] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[441] Priit Pruksi intervjuu Silver Lättiga.
[442] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[443] Samas.
[444] Priit Pruksi intervjuu Oliver Väärtnõuga.

ning transportisid need DBN-ile Hiinas. Mo mõisteti süüdi vandenõus[445] panna toime majandusspionaaži kuritegu ning teda karistati 36-kuulise vabadusekaotusega.[446]

Kaasus 2. Hiina kodanik Xiang Haitao töötas ajavahemikus 2008–2017 põllumajandusettevõttes Monsanto ja selle tütarettevõttes The Climate Corporation. Mainitud ettevõtted arendasid välja digitaalse platvormi[447], mis võimaldas põllumeestel koguda, talletada ja visualiseerida olulist põllumajanduslikku teavet tõstmaks produktiivsust. Platvormi oluliseks osaks oli algoritm nimega *Nutrient Optimizer*. Töötades Climate Corporationis käis Xiang Hiinas ning reklaamis Hiina valitsusele enda kogemusi. Päev pärast töösuhte lõppemist Monsanto ja The Climate Corporationiga üritas Xiang reisida Hiinasse alustamaks tööd Hiina Teaduste Akadeemia Pinnaseteaduste Instituudis. Lennujaamas peeti Xiang kinni ning tollitöötajad konfiskeerisid tema valdusest teabekandja, millelt avastati hiljem algoritmi *Nutrient Optimizer* koopiad. Tollitöötajad lasid Xiangil riigist lahkuda, kuid ta peeti kinni 2019. aasta novembris, kui ta üritas uuesti siseneda Ameerika Ühendriikidesse. Xiang tunnistas end süüdi vandenõus panna toime majandusspionaaži kuritegu. Talle mõisteti 29 kuud vabadusekaotust koos kolme aasta pikkuse käitumiskontrolliga ning 150 000 dollari suurune rahaline karistus.[448]

Kaasus 3. Hiina päritolu Ameerika Ühendriikide kodanik Zheng Xiaoqing töötas ajavahemikus 2008–2018 turbiinitihenditehnoloogia spetsialistina energeetikaettevõttes GE Power. 2017. aasta novembris avastas FBI ühe teise uurimise käigus, et Zheng pidas ettekande Nanjingi Aero- ja Astronautika Ülikoolis, mille käigus võidi avalikustada GE ärisaladust. FBI andis sellest teada GE-le, kelle küberturvalisuse direktor avastas, et rohkem kui 400 faili Zhengi tööarvutis olid krüpteeritud kasutades krüpteerimistarkvara AxCrypt. GE paigaldas Zhengi

[445] Märkus „vandenõu“ mõiste kohta. Ajavahemikus 15.11.2009 kuni 14.01.2019 kehtis karistusseadustikus KarS § $235^1$ (Eesti Vabariigi vastane vandenõu). Karistusseadustiku muutmisel, millega loodi KarS § $234^2$ koosseis, muudeti ka KarS § $235^1$ sisu ja pealkirja. Uueks pealkirjaks sai „Eesti Vabariigi vastase suhte loomine“, kuid sätte karistusõiguslik olemus jäi samaks. Sisuliselt on tegemist KarS §-des 231, 232, 233, 234 ja $234^2$ ja 235 ettevalmistamist kriminaliseeriva koosseisuga. Vt: 642 SE seletuskiri, lk 6.

[446] *United States* vs. *Mo Hailong*, No. 4:13-CR-147 (S.D. Iowa October 10, 2016); U. S. Department of Justice. Chinese National Sentences to Prison for Conspiracy to Steal Trade Secrets. (05.10.2016). – https://www.justice.gov/archives/opa/pr/chinese-national-sentenced-prison-conspiracy-steal-trade-secrets (02.03.2025).

[447] Eestis on sarnaseks ettevõtteks eAgronom. Vt lähemalt: https://www.eagronom.com/ (02.03.2025).

[448] *United States* vs. *Haitao Xiang*, 67 F.4th 895. (8th Cir. 2023); U.S. Department of Justice. Chinese National Sentenced for Economic Espionage Conspiracy. (07.04.2022). – https://www.justice.gov/archives/opa/pr/chinese-national-sentenced-economic-espionage-conspiracy (02.03.2025); National Counterintelligence and Security Center. Secure Innovation. Scenarios and Mitigations, lk 2. – https://www.dni.gov/files/NCSC/documents/SecureInnovation/10252024_Final_Scenarios.pdf (09.04.2025).

arvutisse jälgimistarkvara, mille abil tuvastati, et Zheng krüpteeris 40 faili, mis puudutasid GE turbiine, ning peitis need päikesetõusu kujutava pildi sisse kasutades tehnikat, mis kannab nime *steganography*[449]. Zheng saatis seejärel pildi e-kirjaga isiklikule e-kirja aadressile pealkirjaga „ilus vaade". Mees mõisteti süüdi vandenõus panna toime majandusspionaaži kuritegu. Zhengi karistati 24 kuu vabadusekaotusega, 7500 USD suuruse rahalise karistuse ning kohustusega alluda ühe aasta pikkusele karistusejärgsele käitumiskontrollile.[450]

Kaasus 4. Hiina kodanik Su Bin elas Kanadas ja tegutses lennundus- ja aeronautikaäris väikeettevõttes Lode-Tech. 2008. aasta oktoobrist kuni 2014. aasta märtsini osales Su vandenõus hankida ebaseaduslikult juurdepääs Boeingu arvutivõrkudele eesmärgiga omandada tundlikku sõjalist teavet – sh teavet C-17 strateegilise transpordilennuki ja teatud hävituslennukite kohta – ning eksportida seda teavet ebaseaduslikult Hiinasse. Su andis Hiina rahvaarmee ohvitseridest kaastäideviijatele juhiseid, milliseid isikuid, ettevõtteid ja tehnoloogiaid sihitada. Üks kaastäideviija hankis seejärel juurdepääsu arvutisüsteemidele ning saatis Sule ülevaate failidest. Su andis seepeale juhised, milliseid faile varastada. Kui kaastäideviija oli andmed varastanud ning kasutanud meetodeid oma tegevuse jälgede peitmiseks, tõlkis Su andmete sisu inglise keelest hiina keelde. Veel saatsid Su ja tema kaastäideviijad Hiina rahvaarmeele e-kirju, mis sisaldasid raporteid häkkimise käigus omandatud teabe kohta, sh selle väärtuse kohta. Su Bin peeti Kanadas kinni ning mees nõustus enda toimetamisega Ameerika Ühendriikidesse. Kokkuleppemenetluse käigus tunnistas Su end süüdi vandenõus panna toime arvutikuritegusid ja ekspordikontrolli nõuete rikkumisi. Kohus mõistis talle 46 kuud vabadusekaotust.[451]

Kaasus 5. 2020. aasta 21. juulil esitas föderaalprokuratuur süüdistuse kahele Hiina kodanikule. Süüdistuse kohaselt panid kõnealused isikud rohkem kui kümne aasta vältel toime

[449] Anderson, R. J., Petitcolas, F. A. P. On the Limits of Steganography. – IEEE Journal of Selected Areas in Communications 1998/16 (4), lk 474–481.
[450] *United States* vs. *Xiaoqing Zheng*, 114 F.4th 280 (2nd Cir. 2024); U.S. Department of Justice. Former GE Power Engineer Sentenced for Conspiracy to Commit Economic Espionage. (03.01.2023). – https://www.justice.gov/archives/opa/pr/former-ge-power-engineer-sentenced-conspiracy-commit-economic-espionage (02.03.2025).
[451] *United States vs. Su Bin*, No. 8:14-cr-00131-CAS (S.D.Cal. July 13, 2016); U.S. Department of Justice. Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information. (23.03.2016). – https://www.justice.gov/archives/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive (02.03.2025); U.S. Department of Justice. Chinese National Who Conspired to Hack into U.S. Defense Contractor's Systems Sentenced to 46 Months in Federal Prison. (13.07.2016). – https://www.justice.gov/archives/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months (02.03.2025).

arvutikuritegusid, mille sihtmärgiks olid kõrgtehnoloogiatööstusega riigid, sealhulgas Ameerika Ühendriigid, Austraalia, Belgia, Saksamaa, Jaapan, Leedu, Holland, Hispaania, Lõuna-Korea, Rootsi ja Suurbritannia. Rünnakute alla sattusid ettevõtted mitmetest tööstusharudest, sh „kõrgtehnoloogiline tootmine, meditsiiniseadmete valmistamine, tsiviil- ja tööstusinseneriteadus, äri-, haridus- ja mängutarkvara, päikeseenergia, ravimi- ja kaitsetööstus“ [452] . Süüdistatavad kasutasid arvutisüsteemidesse tungimiseks teadaolevaid haavatavusi tarkvaras. Mõnel juhul olid need äsja avalikustatud, mistõttu ei olnud paljud kasutajad veel paigaldanud täiendusi. Oma tegevuse varjamiseks kasutasid süüdistatavad konspiratsioonivõtteid. Süüdistuse kohaselt varastasid süüdistatavad ärisaladusi, mis hõlmasid „tehnoloogiadisaine, tootmisprotsesse, testimismehhanisme ja -tulemusi, lähtekoodi ning farmatseutiliste keemiliste ühendite struktuure“ [453] . Süüdistatavad tegutsesid kohati isikliku kasu eesmärgil ning kohati Hiina julgeolekuteenistuse huvides. Süüdistatavatele heidetakse ette vandenõud panna toime arvutikelmust, ärisaladuste vargust, võrgukelmust (*wire fraud*), arvutisüsteemile ebaseaduslikult juurdepääsu hankimist ja teise isiku identiteedi ebaseaduslikku kasutamist. Süüdistatavad on endiselt FBI poolt tagaotsitavad. [454]

Kaasus 6. 2017. aasta märtsis paluti USA lennundusettevõtte GE Aviation töötajal pidada ettekanne Hiina ülikoolis. Kaks kuud hiljem reisis töötaja Hiinasse, kus talle tutvustati Xu Yanjuni, kes osutus Hiina julgeolekuministeeriumi luureametnikuks. Xu ja teised isikud tasusid töötaja reisikulud ning maksid talle stipendiumi. Selliseid tööreise pakuti ka teistele GE Aviationi töötajatele. Samal ajal kui Hiina julgeolekuministeeriumi ametnikud kostitasid oma külalisi õhtusöögiga sisenesid Xu ja tema kolleegid nende hotellitubadesse, kus murdsid sisse arvutitesse ja kopeerisid selle sisu. Hiina julgeolekuametnike eesmärk oli varastada GE Aviationi unikaalne lennukimootori ventilaatormooduli tehnoloogia, mida ükski teine ettevõte maailmas polnud suutnud järgi teha. Tööstusspioonide tegevuse nurjas FBI ja GE Aviationi koostöö, mille raames FBI asus töötaja nime alt ise Xuga suhtlusesse. Suhtluse käigus saadeti Xule kahelehekülgeline dokument märkega, mis hoiatas konfidentsiaalse teabe avaldamise eest. 2019. aasta veebruaris arutas Xu töötajaga kohtumist Euroopas ning palus saata koopia oma tööarvuti failikataloogist. 1. aprillil 2018 reisis Xu Belgiasse, kaasas sularaha ja fotod töötajast.

[452] U.S. Department of Justice. Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research. (21.07.2020). – https://www.justice.gov/archives/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion (02.03.2025).
[453] Samas.
[454] Samas; *United States v. Li Xiaoyu, Dong Jiazhi*, No. 4:20-CR-6019-SMJ (E.D. Wash. July 7, 2020).

Belgias Xu arreteeriti ning anti välja Ameerika Ühendriikidele. Tegemist on esimese Hiina luureametnikuga, kes on Ameerika Ühendriikidele välja antud.[455]

Kaasus 7. Eelmises kaasuses mainitud luureametnik Xu Yanjun värbas agente ka Prantsuse lennukimootorite tootja Hiina tehases. Xu ja tema agendid võtsid sihikule Prantsuse ettevõtte töötaja, kes külastas sageli tehast. 2013. aastal andis Xu ühele oma agendile ülesandeks paigaldada töötaja tööarvutisse pahavara eesmärgiga tungida ettevõtte arvutivõrku.[456]

Xu mõisteti muuhulgas süüdi katses ja vandenõus panna toime majandusspionaaži kuritegu. Kohus karistas teda 20-aastase vabadusekaotusega.[457]

Tegemist ei ole täieliku[458] ülevaatega Hiina tööstusspionaažist Ameerika Ühendriikides, kuid kaasuste pinnalt on võimalik teha esmaseid järeldusi järgmistes küsimustes: Milline on tööstusspionaaži toimepanijate taust? Milliseid esemeid nad soovivad hankida? Kuidas nad neid hangivad? Milliste koosseisude alusel nad vastutavad?

Toimepanijate taust. Kõigil toimepanijatel on mingi seos Hiinaga – kas kodakondsus või päritolu. Kuid see ei tähenda, et agendiks ei võida värvata kedagi, kellel puuduvad igasugused perekondlikud sidemed Hiinaga. Kodakondsus või päritolu lihtsustab eriteenistustel esimese sammu tegemist, kuid haavatavad on kõik, kes töötavad Hiina ettevõtetes (Kaasus 1) või Hiinas tegutsevates lääne ettevõtetes (Kaasus 7), teevad teadustööd Hiina teadusasutustes (Kaasus 2), viibivad Hiinas tööalasel välislähetusel (Kaasus 6) või peavad seal ettekandeid (Kaasus 3[459]).

---

[455] *United States* vs. *Yanjun Xu*, 110 F.4th 841 (6th Cir. 2024); U.S. Department of Justice. Chinese government intelligence officer sentenced to 20 years in prison for espionage crimes, attempting to steal secrets from Cincinnati company. (16.11.2022). – https://www.justice.gov/usao-sdoh/pr/chinese-government-intelligence-officer-sentenced-20-years-prison-espionage-crimes (02.03.2025).

[456] Samas.

[457] Samas.

[458] Ülevaade avalikult kättesaadavatest Hiina spionaažijuhtumitest ajavahemikul 2000 kuni märts 2023: Center for Strategic & International Studies. Survey of Chinese Espionage in the United States Since 2000. March 2023. – https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000 (02.03.2025).

[459] Kolmandas kaasuses figureeriva Zhengi kohta väidab FBI, et tegemist oli nn Tuhande Talendi Programmi osalisega. FBI ja Kanada välisluure CSIS sõnul meelitatakse talendiprogrammide kaudu väljaspool Hiinat elavaid teadlasi tegutsema Hiina riigi ja armee huvides. Vt lähemalt: FBI. Counterintelligence Strategic Partnership Intelligence Note. 2015 september. – https://info.publicintelligence.net/FBI-ChineseTalentPrograms.pdf; CSIS. Thousand Talents Plan. (07.08.2020). – https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20201201/020/index-en.aspx (02.03.2025); Zweig, D., Kang, S. America Challenges China's National Talent Programs. Center for Strategic & International Studies. 2020. – https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/20505_zweig_AmericaChallenges_v6_FINAL.pdf (02.03.2025).

Lisaks ootuspärastele elukutsetele nagu luureametnik ja häkker leidub toimepanijate seas ka ärijuht, insener ja ettevõtja. Elukutsete lai ring annab mõista, et Hiina kasutab tööstusspionaažiks väga erineva taustaga isikuid.

Ründeobjekt. Tööstusharude puhul on selge fookus kõrgtehnoloogial ehk valdkondadel, kus hüvede loomine nõuab suuri investeeringuid. Käesoleva töö vaatepunktist on oluline täheldada, et tööstusspioonidele ei paku huvi mitte ainult salastatud teave, vaid ka ärisaladus. Viitega Kaasusele 4 tsiteerin Ameerika õhuvägede eriuurimiste osakonda, mis tegi juhtumi uurimisel koostööd FBI-ga: „Kuigi suur osa varastatud teabest ei olnud salastatud, tundlik ega ekspordikontrolli all, võimaldas see Hiinal tervikuna paljusid lennukikomponente pöördprojekteerida[460], säästes seeläbi palju aega ja raha tehnoloogia tootmise uurimis-, arendus- ja testimisfaasides.“[461]

Lühidalt: suur hulk salastamata teavet võib koosmõjus olla äärmiselt kasulik.[462] Seda eriti nüüd, kui suure hulga teabe analüüsimiseks ja sünteesimiseks on võimalik kasutada nn tehisintellekti.

Seos Hiina riigiga. Formaalselt liigituvad kaasustes figureerivad Hiina entiteedid äriühinguks (Kaasus 1), teadusasutuseks (Kaasus 2), armeeks (Kaasus 4) ja eriteenistuseks (Kaasus 6), kuid lõplikuks kasusaajaks on ikkagi Hiina riik. Teisisõnu: lääne ühiskondadele omane vahetegu era- ja avaliku huvi vahel Hiinas ei kehti. Samas võib eristada neid juhtumeid, kus side Hiina sõjaväe (Kaasus 4) või eriteenistustega (Kaasus 6, 7) on vahetu, ning neid, kus Hiina riigi osaluse peitmiseks kasutatakse vahendajaid, nt äriühinguid (Kaasus 1) ja teadusasutusi (Kaasus 2 ja 3). Kaasuse 5 puhul esineb eriteenistuse osalus, kuid selle peitmiseks kasutas eriteenistus häkkeritest käsilasi, kes tegutsesid kohati eriteenistuse huvides ja kohati isiklikes huvides. Vahendajate lai ring ning riigi ja toimepanijate isiklike finantshuvide läbipõimumine näitavad,

[460] *Reverse engineer*.
[461] Kidwell, D. Cyber espionage for the Chinese government. U. S. Air Force Office of Special Investigations 17.09.2020. – https://www.osi.af.mil/News/Features/Display/Article/2350807/cyber-espionage-for-the-chinese-government/ (02.03.2025).
[462] Siinkohal tasuks rõhutada üht luurekogukonnas tuntud asjaolu: „Tüüpilise luureraporti puhul põhineb ainult umbes 20% luureinfost salastatud teabel [...]. Ülejäänu korjatakse kokku ja sünteesitakse avalikest allikatest, või avalikult kättesaadavast teabest nagu välisriikide valitsuste raportid ja ajaleheartiklid.“ (Zegart, A., lk 19–20.) Salastatud *vs.* salastamata allikate proportsioon luureraportis sõltub sellest, kas sihtmärk on *soft* (nt Saksamaa) või *hard* (nt Põhja-Korea). Vt lähemalt: „Memorandum Respecting Section 202 (Central Intelligence Agency) of the Bill to Provide for a National Defense Establishment, Submitted by Allen W. Dulles, April 25, 1947,“ reprinted in National Defense Establishment (Unification of the Armed Services), 80th Cong., 1st sess., U.S. Senate Armed Services Committee Hearings Part 3, 525; Friedman, R. S. Open source intelligence: A review essay. – Parameters 1998/28, No 2, lk 159. (Viidatud: Zegart, A. Chapter 2, viide nr 21).

et Hiina suudab tegutseda loominguliselt ning kasutab erinevaid stiimuleid motiveerimaks isikuid tegutsema riigi huvides. Seega, Hiina on küll autokraatlik riik, aga see ei tähenda, et inimesi kontrollitakse ainult vägivallaga. Muidugi, kui muud vahendid ei tööta, on alati võimalik kasutada vägivalda.

Välisvaenlased ja sisekahjurid. Neljandaks võib kaasuseid liigitada kaheks selle alusel, kas tööstusspionaaži sihtmärki rünnatakse väljastpoolt või kasutatakse rünnaku käigus ka sisekahjurit[463] (*insider threat*).

Rünnak väljast: Kaasuses 1 oli ründajaks konkureeriva äriühingu ärijuht. Kaasuses 4 oli selleks samas valdkonnas tegutsev väikeettevõtja, kes andis enda erialateadmiste pinnalt juhiseid Hiina sõjaväe küberspioonidele. Viimased viisid ellu ärisaladuste varguse. Kaasuses 5 olid ründajateks Hiinas asuvad eriteenistusega seotud häkkerid.

Rünnak seest: Kaasustes 2 ja 3 olid toimepanijaks äriühingu insenerid. Kaasuses 7 värbas Hiina luureametnik agendid äriühingu töötajate seast ning andis neile juhiseid paigaldada nuhkvara ühe teise töötaja arvutisse. Kaasuses 6 üritas sama luureametnik kasutada sama meetodit, kuid tema värbamiskatse nurjas FBI, kes võttis üle sihtmärgi ja luureametniku vahelise suhtluse ning kasutas tõendite kogumiseks kuriteo matkimist.

Inim- või tehniline spionaaž. Kaasused saab liigitada kolmeks selle alusel, kas tööstusspionaaži toimepanemisel kasutati agente, tehnilisi vahendeid või mõlemad. M. Lowenthal eristab tehnilisi luuremeetodeid (GEOINT, SIGINT, MASINT) ja inimluuret (HUMINT). [464] Üldistatult kogutakse luureinfot kahte moodi – kas inimeste või tehniliste vahendite abil. Seega, tööstusspioonid võivad rünnata, kas füüsilises ruumis, küberruumis või mõlemas. N. Eftimiades toob Hiina puhul esile „HUMINT-poolt võimaldatud küberspionaaži“ [465] ehk siis

[463] Selle mõiste on kasutusele võtnud M. Purre. Vt lähemalt: Purre, M. Riigireetmine ja riigireetur. – Juridica 2020/2. *Insider*'i ja *Insider Threat*'i mõistete kohta USA õiguskorras vt lähemalt: 32 CFR Part 117 § 1137.3(b) *Insider*: „julgeolekukontrolli läbinud töövõtja, kellel on volitatud juurdepääs mistahes Ameerika Ühendriikide valitsuse või tema töövõtja ressursile, sh personalile, hoonetele, teabele, varustusele, võrkudele, või süsteemidele”. *Insider Threat*: „tõenäosus, risk, või potentsiaal et *insider* kasutab oma volitatud juurdepääsu, teadlikult või mitteteadlikult, et kahjustada Ameerika Ühendriikide rahvuslikku julgeolekut“.

[464] Lowenthal, M. Chapter Five: Collection and the Collection Disciplines. The Stovepipes Problem; Kaitseväe Luurekeskuse järgi on NATO kuus peamist luuredistsipliini signaalluure (SIGINT), kujutisluure (IMINT), inimluure (HUMINT), luure avalikust allikast (OSINT), andurluure (MASINT) ja akustiline luure (ACINT). Vt: Eesti Kaitsevägi. Luurekeskus. Luureliigid. – https://mil.ee/uksused/luurekeskus/luureliigid/ (02.03.2025).

[465] *HUMINT enabled cyber espionage*. Vt lähemalt: Eftimiades, N. A Series on Chinese Espionage Vol. I Operations and Tactics. Vitruvian Press 2020, lk 1, 19.

olukorra, kus näiteks organisatsiooni sees pesitsev sisekahjurist agent ja välisriigis asuvad küberspioonid tegutsevad koordineeritult.

Kaasused 1, 2 ja 3 võib liigitada HUMINT operatsioonideks. Kaasused 4 ja 5 on puhas küberspionaaž, st välisriigis asuvad häkkerid murravad sisse arvutivõrkudesse. Kaasuses 6 võib aga täheldada nii inimspionaaži (töötajate meelitamine Hiinasse ja nende tähelepanu kõrvalejuhtimine) kui ka küberspionaaži elemente (arvutitesse sissemurdmine ja teabe kopeerimine). Sama muster on tuvastatav ka Kaasuses 7, mida võiks pidada heaks näiteks „HUMINT-poolt võimaldatud küberspionaažist“ [466] N. Eftimiadesi käsitluses. Operatsioon viiakse ellu neljas jaos: 1) luureametnik värbab agendid Prantsusmaa äriühingu Hiinas asuvas tehases; 2) luureametnik tuvastab agentide kaasabil töötaja, kes reisib tihti Prantsusmaa ja Hiina vahelt; 3) üks agentidest paigaldab töötaja arvutisse pahavara; 4) eriteenistuste häkkerid üritavad kasutada pahavara, et murda sisse äriühingu arvutisüsteemi Prantsusmaal.

Karistusõiguslik vastutus. Esmalt mainin, et isikute karistamine vandenõu (*conspiracy*) eest viitab, et kriminaliseeritud on juba kuriteo ettevalmistamine. Riigivastaste kuritegude ja arvutikuritegude ettevalmistamine on kriminaliseeritud nii Ameerika Ühendriikide kui Eesti õiguskorras.[467]

Teiseks märgin, et vastutus vandenõu eest omab süüdistaja seisukohalt teatavaid eeliseid, kuivõrd tulenevalt *Pinkerton* vs. *United States*[468] kohtulahendist on võimalik teatud tingimustel ühele vandenõu osalisele omistada teiste vandenõuliste täideviidud kuritegusid. Spionaažijuhtumite puhul on see eriti asjakohane, kuna näiteks Kaasuses 4 figureerivale Su Binile on võimalik omistada teod, mille panid toime Hiinas asuvad Hiina sõjaväeluure ametnikud tema juhistel. Seda enam, et Hiina sõjaväeluurajaid ei pruugi olla võimalik tuvastada.[469]

---

[466] Eftimiades, N. A.
[467] KarS § 235[1] ja KarS § 216[1] ning 18 U.S.C § 371.
[468] *United States v. Pinkerton*, 328 U.S. 640 (1946).
[469] Siiski tuleks rõhutada, et selline arusaam vandenõust või kuriteo kaastäideviimise kokkuleppest on Eesti karistusõigusele võõras. J. Sootaki sõnul ei tohi KarS § 22[1] rakendamisel kaastäideviimise kokkuleppele järgnev põhitegu jõuda kuriteokatse staadiumi. Kui kuritegu jõuab katse staadiumisse „järgneb vastutus üldkorras täideviimise ja osavõtu eest“. Vt: Sootak, J. KarS komm § 22[1], p 2.1. Esmapilgul tundub, et *conspiracy* mõiste Ameerika föderaalses karistusõiguses hõlmab endas nii kaastäideviimise kokkuleppe kui ka kaastäideviimise instituudi elemente. Kuid *conspiracy* instituudi võrdlemine Eesti karistusõigusele omaste instituutidega ei ole käesoleva magistritöös esemeks, mistõttu jätame siinkohal arutelu katki. Lisan vaid, et kaastäideviimise instituut Eesti õiguskorras tuleneb KarS § 21 lg 2 I lausest ning võimaldab ühele kaastäideviijale omistada teise kaastäideviija tegusid seni kuni ei esine „ekstsessi“. Vt: Pikamäe, P. KarS komm § 21, p 5.3.2.

Kolmandaks tuleks ära markeerida, et majandusspionaaži koosseisu kõrval leiavad kasutamist ka arvutikuritegude koosseisud. Ilma konkreetsesse kohtulahendisse ja Ameerika karistusõiguse menetluslikesse nüanssidesse süüvimata ei ole võimalik kindlalt väita, miks prokurörid otsustasid arvutikuritegevuse kooseisude kasuks. Kuid hüpoteesi korras võib spekuleerida, et majandusspionaaži koosseisuga kaasneva võõrriikliku seose tõendamine võib osutuda keeruliseks. Erialakirjanduses räägitakse küberrünnakute puhul „omistamise probleemist“[470]. Hiljuti omistas Eesti esmakordselt küberspionaaži GRU üksusele.[471] Kuigi Venemaa eriteenistused on ka varem Eestit rünnanud, on tegemist esmakordse juhtumiga, kui tegevus suudeti ka Venemaale omistada. Näiteks pronksiöö küberrünnakute puhul leidis R. Ottis 2008. aastal, et Venemaa osalus on tõenäoline (*plausible*), aga mitte tõendatud (*proven*).[472]

Neljandaks, majandusspionaaži ja arvutikuritegude kõrval torkavad silma veel karistusõiguse koosseisud, mille alusel karistatakse isikut strateegilise kauba ebaseaduslikku veo eest (Kaasus 4) ja teise isiku identiteedi ebaseadusliku kasutamise eest (Kaasus 5). Veel tasuks mainida Ameerika föderaalsele karistusõigusele omast võrgukelmuse (*wire fraud*) koosseisu, millega heidetakse ette osariikide vahelise kommunikatsioonivõrgustiku kasutamist kelmuse toimepanemiseks.[473] Endise föderaalprokuröri Nelson Dongi sõnul on võrgukelmuse koosseis majandusspionaaži juhtumites „tugikoosseis“ (*backstop*), mis läheb käiku, kui majandusspionaaži koosseisu ei suudeta tõendada.[474] Sama võib väita ärisaladuste varguse koosseisu (18 U.S. Code § 1832) – ehk siis käesoleva magistritöö käsitluse järgi ärispionaaži – koosseisu kohta, mille objektiivne koosseis ei sisalda võõrriigi osaluse elementi.

[470] Lin, H. Attribution of Malicious Cyber Incidents. – Columbia Journal of International Affairs 2016/70, No 1, lk 75–137; Tran, D. The Law of Attribution: Rules for Attributing the Source of a Cyber Attack. – Yale Journal of Law & Technology 2018/20, lk 376–441; Banks, W. Cyber Attribution and State Responsibility. – International Law Studies 2021/97, lk 1040–1072; Kaska, K., Aasmann, L. Julgeolekuasutuste roll küberjulgeoleku tagamisel ja seda mõjutavad suundumused rahvusvahelises õiguses. – Juridica 2020/2, lk 114 jj.

[471] Eesti Välisministeerium. Eesti omistas esimest korda riigivastased küberrünnakud kuriteo toimepanijatele, kelleks on Venemaa sõjaväeluure. (05.09.2024). – https://vm.ee/uudised/eesti-omistas-esimest-korda-riigivastased-kuberrunnakud-kuriteo-toimepanijatele-kelleks (02.03.2025).

[472] Ottis, R. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Cooperative Cyber Defence Centre of Excellence (2008). – https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (02.03.2025). Tõendamiseks oleks tarvis olnud Venemaa õiguskaitseorganite koostööd, mida ei järgnenud. Mis räägib muidugi enda eest.

[473] 18 U.S. Code § 1343.

[474] Hvistendahl, M. The Scientist and the Spy. Riverhead Books 2020, lk 152.

Nüüd, kus oleme käsitlenud tööstusspioonide tööriistakasti, on meil võimalik veendunumalt määratleda tööstusspionaaži tunnused:

1) salastatud teabe või ärisaladuse või isikuandmete hankimine;
2) ebaseaduslikult;
3) võõrriigi huvides või ülesandel.

Järgnevalt uurime, milliste Eesti karistusseadustiku koosseisude alusel on võimalik võtta isikut vastutusele tööstusspionaaži eest. Ühtlasi käsitleme Ameerika Ühendriikide kohtupraktika valguses mõningaid „tugikoosseise", mis võiksid tulla kasutusele, kui välisriigi osalust ei ole võimalik tõendada.

### 3.5 Tööstusspionaaži koosseis karistusseadustikus

Kui tööstusspionaaži ründeobjekt on riigisaladus või salastatud välisteave, tuleb kohaldamisele, kas KarS § 232 või § 234. Olenevalt sellest, kas toimepanija on Eesti Vabariigi kodanik või välismaalane. Kuid kas vastutuse alus võiks olla ka KarS § 233 pealkirjaga „Välismaalase poolt toimepandud Eesti Vabariigi vastu suunatud vägivallata tegevus"?

Kohtupraktikat on KarS § 233 kohta vähe. Kõik kaasused on lõppenud kokkuleppemenetluses ning lahendid on avalikustatud ainult piiratud ulatuses.[475] Karistusseadustiku kommentaarid jäävad samuti tavatult napisõnaliseks. [476] Sisuliselt piirduvad need seaduse teksti taasesitamisega.[477] Meediakajastusest nähtub, et KarS §-i 233 on rakendatud väga erinevatel tehioludel. Esiteks mõisteti 2024. aastal süüdi isik, kes rüvetas GRU juhistel punase värvi ja haakristidega Sinimägedes asuvaid monumente.[478] Teiseks mõisteti 2019. aastal süüdi isik, kes tegi koostööd GRU-ga „kogudes Eesti Vabariigi julgeoleku kahjustamist võimaldavat teavet ehk infot riigikaitseliste ja elutähtsat teenust tagavate objektide kohta". [479] Kolmandaks mõisteti 2017. aastal süüdi isik, kes tegi koostööd GRU-ga kogudes teavet „riigikaitseliste objektide ja elutähtsat teenust tagavate objektide kohta Eesti Vabariigi territooriumil, aga ka

[475] Harju Maakohtu lahendid: 1-24-2791, 1-19-6496, 1-18-1220, 1-17-4067.
[476] Kärner, M., Kiris, R. KarS komm § 233.
[477] Samas.
[478] Einmann, A. GRU andis Eesti monumentide rüvetamiseks väga täpsed juhised. – Postimees 03.01.2025.
[479] Einmann, A. GRU kasuks luuranud elektrik näitas, et eriteenistuste huvi pälvimiseks ei pea valdama riigisaladust. – Postimees 14.04.2020.

näiteks Kaitseväe ja Kaitseliidu sõjaliste liitlaste tehnika liikumise kohta Eestis“.[480] Samuti sai mainitud isik ülesandeid „hankida GRU-le Eesti Vabariigist soovitud esemeid, näiteks sidevahendeid.“[481] Neljandaks mõisteti 2017. aastal süüdi isik, kes valmistas FSB ülesandel „ette koodi, mille abil saaks ligipääsu ühe riigiasutuse wifi sisevõrku“. [482] A. Reintam küberturvalisuse ettevõttest CybExer Technologies väidab, et kõnealuse isiku tegevus oleks „võimaldanud sissetungijatel märkamatult jälgida kogu võrku, eskaleerida kasutaja õigusi, luua uusi tagauksi ning võimalik, et seejärel tekitada märkimisväärset kahju ka teistele riiklikele institutsioonidele“. [483] Lisaks KarS §-ile 233 mõisteti viimati mainitud isik süüdi ka arvutikuriteo ettevalmistamises KarS § 216[1] järgi.[484]

Kokkuvõtvalt võib väita, et KarS § 233 alla mahub nii vandalismiaktide toimepanemine kui ka avalikult kättesaadava teabe kogumine. Seda eeldusel, et tegutsetakse koostöös välisriigi eriteenistusega. Järelikult ei ole välistatud, et ka tööstusspiooni võiks võtta vastutusele KarS § 233 järgi, juhul kui tema tegevus on suunatud Eesti Vabariigi iseseisvuse ja sõltumatuse või territoriaalse terviklikkuse vastu.[485]

Seadusandja hinnangul jätab KarS § 233 aga liialt laia tõlgendamisruumi, kas konkreetne tegevus on „käsitatav Eesti Vabariigi iseseisvuse ja sõltumatuse või territoriaalse terviklikkuse vastu suunatud vägivallata tegevusena“. [486] Seda näiteks juhul, kui kogutakse infot mittesalajaste valdkondade kohta. Just selline olukord tekkis lahendis 1-21-1421, kui riigikohus leidis, et Hiina mistahes Eesti-suunalise luuretegevuse puhul ei saa *a priori* järeldada, et need on suunatud Eesti Vabariigi iseseisvuse ja sõltumatuse või territoriaalse terviklikkuse vastu.[487] Riigikohtu hinnangul ei tuvastanud kohtud asjaolusid, millest saaks järeldada Hiina sõjaväeluure sellist sihti.[488] Just selliste tõlgendamisraskuste ületamiseks täiendas Riigikogu

[480] KAPO. GRU jaoks luuranud mees mõisteti süüdi Eesti Vabariigi vastases kuriteos. (08.05.2024). – https://kapo.ee/et/content/gru-jaoks-luuranud-mees-m%C3%B5isteti-s%C3%BC%C3%BCdi-eesti-vabariigi-vastases-kuriteos/ (02.03.2025).
[481] Samas.
[482] Roonemaa, H. Vene spiooni sõnum Viru vanglast: mu kodumaa unustas mind. – Postimees 10.10.2018.
[483] Samas.
[484] Harju Maakohus 1-18-1220.
[485] Spekulatsioon: selline olukord võiks tekkida, kui tööstusspionaaži ründeobjekt on mittesalajane teave, mis puudutab Eesti riigi kasutuses olevaid piirivalve- või seiretehnoloogiaid, võimaldades Venemaal hõlpsamini annekteerida Ida-Virumaa.
[486] 642 SE. Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (terrorismivastase võitluse direktiivi ülevõtmine) eelnõu seletuskiri, lk 4.
[487] RKKKo 1-21-1421, p 114.
[488] Samas.

2019. aastal karistusseadustikku KarS §-iga 234[2], mille objektiivsesse koosseisu kuulub oluliselt laiem mõiste: Eesti Vabariigi julgeoleku vastu suunatud tegevus.

KarS § 234[2] kohtupraktika analüüsimisel ilmneb sama takistus, mis KarS § 233 puhul. Nimelt, kõik isikud peale ühe on mõistetud süüdi kokkuleppemenetluses ning kohtulahendid on avalikustatud ainult piiratud ulatuses. [489] Tuginedes ühele riigikohtu lahendile ja meediakajastusele on võimalik jagada juhtumid nelja gruppi.

Esiteks: endise KAPO ametniku juhtum 2019. aastast, mille kohta teame vaid, et isik lõi Eesti Vabariigi vastase suhte Vene eriteenistusega ning osales Eesti Vabariigi vastases luuretegevuses (Harju MKo 1-19-6812). Teiseks: juhtum, kus kaks isikut, kellest üks oli mereteadlane, lõid Eesti Vabariigi vastase suhte Hiina sõjaväeluurega ning kogusid ja edastasid suuresti strateegilise olemusega mittesalajast teavet (RKKKo 1-21-1421, Harju MKo 1-21-1256). Kolmandaks, kolme isiku tegevus Eesti Vabariigi siseministri ja ajakirjaniku autode lõhkumises (Harju MKo 1-24-2429, 1-24-2627). Neljandaks, Tartu Ülikooli professori Eesti Vabariigi vastane luuretegevus, mille käigus professor edastas Venemaa sõjaväeluurele strateegilise olemusega mittesalajast teavet (Harju MKo 1-24-2828).

Eelnevast nähtub, et Eesti Vabariigi julgeoleku vastu suunatud tegevus KarS § 234[2] lg 1 tähenduses võib seisneda nii vandalismiaktide toimepanemises kui ka teabe kogumises ja edastamises.[490] Arvestades, et tööstusspionaaži tunnusteks on teabe hankimine ebaseaduslikult välisriigi huvides või ülesandel, on KarS § 234[2] selgelt kõige asjakohasem koosseis.[491]

KarS § 234[2] puhul tuleks siiski rõhutada, et teabe hankimise „ebaseaduslikkus“ ei ole objektiivse koosseisu tunnus. KarS § 234[2] puhul võib teave olla kogutud ka seaduslikult, nt pildistatakse avalikus ruumis.[492] Tegevuse muudab ebaseaduslikuks asjaolu, et pildistatakse

[489] Harju Maakohtu lahendid: 1-19-6812, 1-21-1256, 1-24-2429, 1-24-2627, 1-24-2828; RKKKo 1-21-1421.
[490] KarS § 234[2] lg-s 1 sisalduv näidisloetelu mainib lisaks teabe kogumisele või edastamisele ka asja kahjustamist.
[491] Märkusena: erinevalt KarS §-st 234[2] ei ole KarS § 233 kohaldamisel võimalik rakendada kuriteoga saadud vara laiendatud konfiskeerimist (KarS § 234[2] lg 3, § 83[2]). Tööstusspionaaži kui majandusliku iseloomuga kuriteo puhul võib see olla oluline asjaolu, mida arvesse võtta.
[492] Tallinna Halduskohtu menetluses olevas vaidluses väidab PPA, et nende hoonete pildistamine või filmimine on keelatud. Vt lähemalt: ERR. Politsei hinnangul pole lubatud nende hooneid pildistada ega filmida. (25.03.2025). – https://www.err.ee/1609638304/politsei-hinnangul-pole-lubatud-nende-hooneid-pildistada-ega-filmida (07.04.2025).

välisriigi luure- või julgeolekuteenistuse huvides või ülesandel.[493] Võrdlusena, ärispionaaži koosseis ehk KarS § 377 sätestab sõnaselgelt objektiivse koosseisu tunnusena ärisaladuse ebaseadusliku saamise, kasutamise või avaldamise.

Praeguseks on karistusseadustikust kadunud Eesti Vabariigi vastase vandenõu nimetus, kuid koosseis ise on endiselt olemas ning kannab nime Eesti Vabariigi vastane suhe (KarS § $235^1$). KarS § $235^1$ näeb ette karistusõigusliku vastutuse KarS §-s $234^2$ sätestatud kuriteo ettevalmistamise eest. Täpsemalt eeldab KarS § $235^1$ objektiivne koosseis, et isik loob või peab suhet „välisriigiga, välisriigi organisatsiooniga või välisriigi ülesandel tegutseva isikuga“ eesmärgiga panna toime KarS §-s $234^2$ sätestatud kuritegu.

Lisaks sellele, et karistusseadustik võimaldab karistada spionaažikuriteo ettevalmistamist on võimalik karistada ka spionaažikuriteo kaastäideviijat (KarS § 21 lg 2 I lause), kihutajat (KarS § 22 lg 2) ja kaasaaitajat (KarS § 22 lg 3). Tööstusspionaaži puhul on võimalik karistada ka kuriteole kihutamise katse eest, kuivõrd KarS § 232, 233, 234 ja $234^2$ kuuluvad karistusseadustiku 15. peatüki 2. jakku ning nende eest ettenähtud karistuse ülemmäär on vähemalt kaheteistaastane vangistus (KarS § $22^1$ lg 1). Loomulikult nõuab KarS § $22^1$ kohaldamine, et tehtud oleks ka täiendav tegu (KarS § $22^1$ lg 2). J. Sootaki järgi välistab see võimaluse, et „karistataks üksnes mõtete eest“[494].

Juhul, kui tööstusspionaaži toimepanemiseks hangitakse ebaseaduslikult juurdepääs arvutisüsteemile, on võimalik vastutus ka KarS § 217 alusel. Sealjuures sisaldab KarS § 217 lg 2 kvalifitseeritud koosseisu, mille p-de 2 ja 3 järgi on võimalik mõista karmim karistus, kui isik hangib ebaseaduslikult juurdepääsu „riigisaladust, salastatud välisteavet või ainult ametialaseks kasutamiseks ettenähtud andmeid sisaldavale arvutisüsteemile“ või „elutähtsa valdkonna arvutisüsteemile“. KarS § $216^1$ alusel on karistatav ka KarS § 217 ja teiste arvutikuritegude ettevalmistamine.

[493] Läti riiklik julgeolekuteenistus pidas kinni Eesti kodaniku, kes väidetavalt pildistas või filmis kriitilist infrastruktuuri: ERR. Läti kinnitas spionaažis kahtlustatavate Eesti ja Ukraina kodaniku vahistamist. (11.03.2025). – https://www.err.ee/1609629428/lati-kinnitas-spionaazis-kahtlustatavate-eesti-ja-ukraina-kodaniku-vahistamist (07.04.2025).
[494] Sootak, J. KarS komm § 221, p 2.3.

Kui tööstusspionaaži ründeobjekt on ärisaladus, aga prokuratuur ei suuda tõendada toimepanijate seost välisriigiga, on võimalik esitada süüdistus ärispionaaži eest ehk KarS § 377 alusel.

Hiina tööstusspionaaži näidiskaasuste 4 ja 5 näitel võivad tööstusspioonid realiseerida ka isiku identiteedi ebaseadusliku kasutamise (KarS § $157^2$) või strateegilise kauba ebaseadusliku veo (KarS § $421^1$, § $421^2$) koosseisud. Strateegilise kauba vedu riiki, millele on kohaldatud Vabariigi Valitsuse või rahvusvahelisi sanktsioone, toob kaasa vastutuse KarS § $93^1$ alusel.[495]

Eestis on eraviisiline jälitustegevus kriminaliseeritud (KarS § 137).[496] Järelikult, kui isik jälgib andmete kogumise eesmärgiga äriühingut või temaga seotud füüsilist isikut ning seost võõrriigi eriteenistusega ei ole võimalik tõendada, võib vastutuse aluseks olla ka KarS § 137.

## 3.6 Vahekokkuvõte

Tööstusspionaaži ennetamine ja tõkestamine kuulub vastuluureasutuste pädevusse. JAS § 6 p 2 kohaselt on riigi vastu suunatud luuretegevuse ennetamine ja tõkestamine KAPO ülesanne. KAPO hinnangul hõlmab riigi vastu suunatud luuretegevuse mõiste ka tööstusspionaaži.[497] Ameerika Ühendriikide juhtiva[498] vastuluureasutuse FBI tegevust reguleerivate õigusaktide järgi kuulub Ameerika Ühendriikide vastaste kuritegude menetlemine FBI pädevusse.[499] Justiitsministeeriumi hinnangul kahjustab majandusspionaaž Ameerika Ühendriikide

[495] Soome pidas kinni isiku, kes väidetavalt üritas transportida Venemaal 30 kasti tuumajaama ehitamisega seotud dokumente. Väidetavalt kuulus osa materjalist ka sanktsioonide alla. Vt: Finnish Customs. Finnish Customs suspects the operaator of a nuclear power plant construction project of a regulation offence. 17.04.2025. – https://tulli.fi/en/-/finnish-customs-suspects-the-operator-of-a-nuclear-power-plant-construction-project-of-a-regulation-offence (17.04.2025).

[496] Ka „anglosfääri" riikides peavad eraõiguslikud juurdlus- ja luureettevõtted tegutsema seaduse alusel ja piirides, kuid tegutsemisvabadus ja võimalused riivata isikute eraelu on oluliselt laiemad. Sellest annab märku „eraluurebüroode" vilgas äritegevus nii Ameerika Ühendriikides kui ka Inglismaal. Mõned näited: Pinkerton (https://pinkerton.com/), Kroll Inc. (https://www.kroll.com/en), Control Risks (https://www.controlrisks.com/), Hakluyt (https://hakluytandco.com/), Black Cube (https://www.blackcube.com/). Eraluure kui nähtuse kohta vt lähemalt: Sage-Passant, L. Beyond States and Spies: The Security Intelligence Services of the Private Sector. Edinburgh University Press 2024.

[497] KAPO. Majandusjulgeolek.
– https://web.archive.org/web/20201021122615/https:/www.kapo.ee/et/content/majandusjulgeolek.html

[498] FBI. FAQ. What is the FBI's foreign counterintelligence responsibility? – https://www.fbi.gov/about/faqs/what-is-the-fbis-foreign-counterintelligence-responsibility (09.04.2025).

[499] FBI. FAQ. Where is the FBI's authority written down? – https://www.fbi.gov/about/faqs/where-is-the-fbis-authority-written-down (11.02.2025).

„majanduslikku tervist ja julgeolekut“ [500]. Võttes arvesse asjaolu, et FBI ja KAPO on mõlemad „politseilist tüüpi julgeolekuteenistused“ [501], ning Ameerika Ühendriikide pikka kogemust tööstusspionaaži vastu võitlemisel, võrdlesin FBI ja KAPO käsitlusi majandus- ja tööstusspionaažist.

Ameerika Ühendriikide õiguskord eristab majandusspionaaži ja ärisaladuste vargust, kusjuures eristavaks kriteeriumiks on toimepanija. Kui välisriik, välisriigi agent või välisriigi kontrolli all olev entiteet omandab USA valitsuse, ettevõtete, asutuste või isikute ärisaladusi, on tegemist majandusspionaažiga (18 U.S. Code § 1831). Kui kuriteost puudub võõramaine element, on tegemist ärisaladuste vargusega (18 U.S. Code § 1832). Oluline on märgata, et ründeobjekt on mõlemal juhul ärisaladus, mis on määratletud võimalikult laialt [18 U.S. Code § 1839(3)]. Eesti karistusseadustik ei sätesta majandus-, tööstus- ega ka ärispionaaži legaaldefinitsioone. Euroopa kontekstis on tegemist pigem reegli kui erandiga. S. Carli jt väitel on mainitud legaaldefinitsioonid olemas väheste riikide õiguskordades. [502]

Seetõttu põhineb KAPO käsitlus asutuse enda arusaamadel. KAPO eristab majandusluuret ja tööstusspionaaži, kusjuures eristamiskriteeriumiks on ründeobjekt. Majandusspionaaži ründeobjekt on riigi kohta käiv strateegiline informatsioon, tööstusspionaaži ründeobjektiks aga omandiõigused (informatsioon, tehnoloogia). Tööstusspionaaži alla arvab KAPO ka korporatiiv- või äriluure, mille ründeobjektiks on ideed, ärisaladused jms. KAPO järgi tegelevad majandus- ja tööstusspionaažiga välisriigid, ärispionaažiga äriühingud.[503]

M. Button ja S. Knickmeier eristavad majandus- ja tööstusspionaaži soodustatava isiku alusel. Mõlemal juhul on tegemist ärisaladuste ja konfidentsiaalse teabe sihitamise või omandamisega kodumaistelt äriühingutelt või riigiasutustelt. Majandus- ja tööstusspionaaži eristab aga asjaolu, et majandusspionaaži puhul soodustatakse välisriiki, tööstusspionaaži puhul aga eraõiguslikku

[500] U.S. Department of Justice. Criminal Resource Manual. Introduction to the Economic Espionage Act. – https://www.justice.gov/archives/jm/criminal-resource-manual-1122-introduction-economic-espionage-act (20.04.2025). Tsitaat: *„Congress, recognizing the importance of the protection of intellectual property and trade secrets to the economic health and security of the United States, enacted the Economic Espionage Act of 1996, Pub.L. 104-294, 110 Stat. 3489 (October 11, 1996)“*
[501] Heldna, E., lk 718.
[502] Carl, S., Kilchling, M., Knickmeier, S., and Wallwaey, E.
[503] Kaitsepolitseiamet. Mida peaks teadma tööstusspionaažist? – https://web.archive.org/web/20191103141731/https://www.kapo.ee/et/content/mida-peaks-teadma-t%c3%b6%c3%b6stusspionaa%c5%beist.html (06.04.2025).

entiteeti, nt äriühingut. Selle käsitluse järgi on Saksamaa õiguskorras majandusspionaaži koosseisuks StGB § 99, tööstusspionaaži koosseisuks aga GeschGehG § 23.[504]

M. Buttoni ja S. Knickmeieri käsitluse järgi on majandus- ja tööstusspionaaži koosseisud Eesti õiguskorras sätestatud vastavalt KarS §-des $234^2$ ja 377. Kõnealuse käsitluse kasuks räägivad järgmised asjaolud. Esiteks oli Saksamaa majandusspionaaži koosseis eeskujuks KarS § $234^2$ vastuvõtmisel.[505] Teiseks loodi Saksamaal tööstusspionaaži koosseis Euroopa Liidu direktiivi 2016/943 alusel.[506] Sama direktiivi tõttu täiendati ka KarS §-i 377.[507]

KAPO püüdlus eristada majandus- ja tööstusspionaaži abstraktsete ründeobjektide nagu omandiõigused ja strateegiline informatsioon alusel ei ole õiguslikult selge. Samas räägib KAPO käsitluse kasuks tõsiasi, et Eesti seadusandja ja erialaspetsialistide seas on juba kinnistunud arusaam tööstusspionaažist kui võõrriigi huvides toimepandavast kuriteost. Juba juurdunud keelekasutuse muutmine ei pruugi olla enam võimalik ning võib raskendada suhtlust.

Seetõttu seostame majandus- ja tööstusspionaaži välisriigi tegevusega ja ärispionaaži äriühingute tegevusega. Sisuliselt on ärispionaaži näol tegemist ebaausa konkurentsiga ehk siis olukorraga, kus teiste äriühingute vastu suunatud äri- või konkurentsiluure ületab ebaeetilisuse lävendi ja muutub ebaseaduslikuks. Eelnevast tulenevalt saame väita, et ärispionaaži koosseisuks on Eesti õiguskorras KarS § 377.

Järgnevalt uurisin, kas majandus- ja tööstusspionaaži on võimalik üksteisest õiguslikult eristada. Selleks püüdsin kasutada ründeobjekti kategooriat. KAPO järgi on majandusspionaaži ründeobjektiks riigi kohta käiv strateegiline teave. [508] Selline teave võib olla, kas salastatud teave, asutusesiseseks kasutamiseks mõeldud teave või muu avalikult kättesaadav teave. KAPO järgi on tööstusspionaaži ründeobjektiks omandiõigused (informatsioon, tehnoloogia). [509] Eeskätt käib siia alla salastatud teave. Riigisaladuse puhul saame rääkida näiteks riigikaitselisest leiutisest (RSVS § 7 p 6) või sõjalise otstarbega asja omadusi, projekteerimist,

[504] Button, M., Knickmeier, S.
[505] 642 SE seletuskiri, lk 6.
[506] WIPO. Overview of national and regional trade secret systems. Germany.
[507] 678 SE seletuskiri, lk 12–13.
[508] Kaitsepolitseiamet. Mida peaks teadma tööstusspionaažist?
[509] Samas.

valmistamist ja kohandamist käsitletavast teabest (RSVS § 7 p $6^1$).[510] Välisluureameti sõnul võib salastatud välisteave hõlmata salastatud tehnoloogiat, mida sisaldab relva- või IT-süsteem, mille kaitsevägi või muu Eesti riigiasutus on hankinud välisriigi kaitsetööstuse ettevõttelt.[511] M. Buttoni ja S. Knickermeier järgi võib tööstusspionaaži ründeobjekt olla ka ärisaladus või hoopis isikuandmed, nt äriühingu juhtorganite liikmete või töötajate isikuandmed.[512]

Karistusõiguslikult on asjakohane küsimus, kas ründeobjektiks on salastatud teave, asutusesiseseks kasutamiseks mõeldud teave või muu teave. Kui ründeobjektiks on salastatud teave, on töösusspionaaž karistatav riigireetmise (KarS § 232) või salakuulamise (KarS § 234) koosseisude alusel. Määravaks on siinkohal asjaolu, kas toimepanija on Eesti Vabariigi kodanik või välisriigi kodanik. Asutusesiseseks kasutamiseks mõeldud teabe kogumise või edastamise puhul tuleb kohaldamisele, kas KarS § 243 või KarS § $234^2$. Muu teabe puhul saab isikut karistada KarS § $234^2$ alusel. KarS § 233 või § 232 võivad tulla kaalumisele, kui ründeobjekt on mittesalajane teave ning tegevus on suunatud Eesti Vabariigi iseseisvuse ja sõltumatuse või territoriaalse terviklikkuse vastu.

Seega, majandusspionaaži potentsiaalsed koosseisud on KarS §-d 232, 233, 234, $234^2$ ja 243. Tööstusspionaaži puhul on nimekiri peaaegu identne: KarS §-d 232, 233, 234 ja $234^2$. Järelikult ei ole majandus- ja tööstusspionaaži eristamine karistusõiguslikult mõistlik.

Magistritöös mõistame tööstusspionaaži all tegu, mis seisneb võõrriigi huvides või ülesandel salastatud teabe, ärisaladuse või isikuandmete ebaseaduslikus hankimises. Kuna töö fookus ei ole salastatud teabel langeb põhirõhk KarS §-le $234^2$.

Selleks, et saada parem aimdus tööstusspionaaži toimepanijatest, meetoditest ning karistusõiguslikest valikutest tööstusspioonide vastutusele võtmisel, viisime läbi seitsme Hiina tööstusspionaaži juhtumi analüüsi ja sünteesi. Leidsime, et esmajärgus iseloomustab toimepanijaid side Hiinaga. Olgu selleks siis Hiina kodakondsus, etniline päritolu, töö Hiina ettevõttes või Hiinas tegutsevas lääne ettevõttes, teadustöö Hiina teadusasutuses või tööalane lähetus Hiinasse. Veel leidsime, et tööstusspionaaž võib lähtuda väljastpoolt organisatsiooni

[510] RSVS § 7 p $6^1$ alla võib kuuluda sõjalise otstarbega asja tootva äriühingu ärisaladus, mille äriühing on otsustanud riiklikult salastada. Vt lähemalt: 468 SE seletuskiri, lk 19.
[511] Eesti rahvusvahelises julgeolekukeskkonnas 2024, lk 87.
[512] Button, M., Knickmeier, S.

luureametnike ja häkkerite näol või ilmneda sisekahjuri (*insider threat*) kujul. Kahjuriks võib osutuda juhtorgani liige, töötaja või teenusepakkuja. Samuti avastasime, et spionaažikuriteo toimepanemisel kasutatakse lisaks agentidele ja tehnilistele vahenditele ka kahe kombinatsiooni, nt tegutseb äriühingu sees pesitsev sisekahjurist agent koordineeritult Hiina sõjaväe küberspioonidega.[513]

Kui prokuratuur suudab tõendada tegutsemist võõrriigi huvides, kohaldatakse Ameerika Ühendriikides majandusspionaaži koosseisu (18 U.S. Code § 1831). Juhul, kui seost võõrriigiga ei suudeta tõendada, kasutatakse muuhulgas ärisaladuste varguse (18 U.S. Code § 1832), arvutikuritegude (18 U.S. Code § 1030), võrgukelmuse (18 U.S. Code § 1343), strateegilise kauba ebaseadusliku veo (AECA, 22 U.S. Code § 2778; ITAR, 22 CFR 120-130) ja teise isiku identiteedi ebaseadusliku kasutamise (18 U.S. Code § 1028A) koosseise. Laialdaselt leiab spionaažikaasustes kasutamist Ameerika Ühendriikide vastase vandenõu koosseis, mis võimaldab karistada isikut kuriteo ettevalmistamises faasis ning omistada isikule teise isiku tegusid (18 U.S.C. § 371, 1349). Omistamine võib osutuda kasulikuks näiteks siis, kui arvutikuritegusid panevad toime Hiinas asuvad riigiametnikud, kuid kinni peetakse Ameerika Ühendriikides tegutsev agent, kelle ülesandeks on anda riigiametnikele infot sihtmärkide kohta.

Karistusseadustikus on olemas kõik analoogilised koosseisud tööstusspioonide heidutamiseks ja karistamiseks. Kui toimepanija on Eesti Vabariigi kodanik ja ründeobjekt on salastatud teave, on võimalik kohaldada riigireetmise koosseisu (KarS § 232). Kui tegemist ei ole kodanikuga, tuleb kohaldamisele salakuulamise koosseis (KarS § 234). Juhul, kui tegemist on mittesalajase teabega, tuleb kõige tõenäolisemalt kohaldamisele KarS § $234^2$. Kui mittesalajase teabe hankimist lugeda Eesti Vabariigi iseseisvuse ja sõltumatuse või territoriaalse terviklikkuse vastu suunatud vägivallata tegevuseks, on teoreetiliselt võimalik kohaldada ka KarS §-i 233 (välismaalane) või KarS § 232 (kodanik). Siiski tuleks arvestada, et erinevalt KarS §-st $234^2$ ei ole KarS § 233 kohaldamisel võimalik rakendada kuriteoga saadud vara laiendatud konfiskeerimist (KarS § $234^2$ lg 3, § $83^2$). Kuna tööstusspionaaž on majandusliku iseloomuga kuritegu, võib vara laiendatud konfiskeerimise võimalus olla oluline argument.

[513] *United States v. Mo Hailong* (Kaasus 1); *United States v.. Haitao Xiang* (Kaasus 2); *United States v. Xiaoqing Zheng* (Kaasus 3); *United States v. Su Bin* (Kaasus 4); *United States v. Li Xiaoyu, Dong Jiazhi* (Kaasus 5); *United States v. Yanjun Xu* (Kaasused 6-7).

Praeguseks on karistusseadustikust kadunud Eesti Vabariigi vastase vandenõu nimetus, kuid koosseis ise on endiselt olemas ning kannab nime Eesti Vabariigi vastane suhe (KarS § 235[1]). Lisaks sellele, et võimalik on karistada spionaažikuriteo ettevalmistamist, võimaldab karistusseadustik karistada lisaks täideviijale ka kaastäideviijat (KarS § 21 lg 2 I lause), kihutajat (KarS § 22 lg 2) ja kaasaaitajat (KarS § 22 lg 3). Tööstusspionaaži puhul on võimalik karistada isikut ka kuriteole kihutamise katse eest, kuivõrd KarS § 232, 233, 234 ja 234[2] kuuluvad karistusseadustiku 15. peatüki 2. jakku ning nende eest ettenähtud karistuse ülemmäär on vähemalt kaheteistaastane vangistus (KarS § 22[1] lg 1). Loomulikult nõuab KarS § 22[1] kohaldamine, et tehtud oleks ka täiendav tegu (KarS § 22[1] lg 2). J. Sootaki järgi välistab see võimaluse, et „karistataks üksnes mõtete eest“[514].

Juhul, kui Eesti Vabariigi vastase suhte tõendamine osutub keeruliseks, võimaldab Eesti õiguskord võtta vastutusele isikuid järgmiste tegude eest, millel on oluline puutumus tööstusspionaažiga: ärisaladuse ebaseaduslik omandamine (KarS § 377), arvutisüsteemi ebaseaduslikult juurdepääsu hankimine (KarS § 217), arvutikuriteo ettevalmistamine (KarS § 216[1]), strateegilise kauba ebaseaduslik vedu (KarS § 421[1], § 421[2]), rahvusvahelise sanktsiooni ja Vabariigi Valitsuse sanktsiooni rikkumine (KarS § 93[1]), teise isiku identiteedi ebaseaduslik kasutamine (KarS § 157[2]) ja eraviisiline jälitustegevus (KarS § 137).

Kokkuvõtvalt: Tööstusspionaaž on tegu, mis seisneb võõrriigi huvides või ülesandel salastatud teabe, ärisaladuse või isikuandmete ebaseaduslikus hankimises. Eesti õiguskorras on tööstusspionaaž karistatav, kas KarS § 232, 233, 234 või 234[2] alusel.

Järelikult on magistritöö esimene hüpotees  ümber lükatud.

[514] Sootak, J. KarS komm § 221, p 2.3.

# 4. Kaitsetööstuse äriühingu ärisaladus kui teave KarS § 234[2] tähenduses

Kuna töö fookus ei ole salastatud teabel langeb põhirõhk KarS §-le 234[2]. Täpsemalt tekib küsimus, kas ärisaladuse ebaseaduslik hankimine kaitsetööstuse äriühingust on Eesti Vabariigi julgeoleku vastane tegevus KarS § 234[2] lg 1 mõttes. Või veelgi täpsemalt: kas kaitsetööstuse äriühingu ärisaladus on teave KarS § 234[2] lg 1 tähenduses. Esmalt tuleb käsitlemisele RKKKo 1-21-1421. Tegemist on ainukese lahendiga KarS § 234[2] kohaldamisest, mis on avalikustatud täies ulatuses.

## 4.1 Riigikohtu kriminaalkolleegiumi 16. juuni 2023 otsus 1-21-1421

Menetluse käigus tuvastasid kohtud, et süüdistatav G. Mutso kogus järgmist teavet:

1) andmed Eesti mereteadlase T. Kõutsi kohta[515], sh asjaolu kohta, et T. Kõuts kuulub NATO merendusalastessse komisjonidesse ning tal on riigisaladuse luba ja juurdepääsusertifikaat NATO salastatud teabele;[516]
2) andmed ilmajaamade ja Eesti sadamate kohta;[517]
3) andmed küberjulgeoleku ning merendusega tegelevate Eesti teadlaste kohta;[518]
4) andmed Eesti Kaitseväe ohvitseri A kohta.[519]

Süüdistatav edastas Hiina sõjaväeluurele (HSL) järgmist teavet:

1) ülevaade enda suhtlusringkonnast;[520]
2) „info erinevatel teemadel“;[521]
3) T. Kõutsi elulookirjeldus;[522]
4) T. Kõutsilt saadud ilmajaamade lingid;[523]
5) Soome-Eesti raudteetunneli lõplik versioon.[524]

[515] RKKKo 1-21-1421, p 17 3).
[516] Samas, p 17 6).
[517] Samas, p 17 3).
[518] Samas, p 17 5).
[519] Samas, p 23.
[520] Samas, p 17 5).
[521] Samas.
[522] Samas, p 17 7).
[523] Samas, p 17 8).
[524] Samas, p 17 15).

Veel tuvastasid kohtud, et süüdistatav aitas T. Kõutsil üle lugeda kokkuvõtte enda ettekandest operatiivokeanograafiast ja selle rakendustest Läänemeres enne kui T. Kõuts edastas selle HSL-ile.[525] Samuti saatis süüdistatav T. Kõutsi kohtumisel HSL-i agendijuhiga, kus T. Kõuts andis üle kümme faili, mis sisaldasid „ülevaadet Venemaa Arktika mereala ja Põhja-meretee kohta ning andmeid EL-i rahastatud teadusprojekti SAFEICE kohta"[526].

Riigikohus eristab kahte liiki tegevusi: 1) tegevused, mis on suunatud Eesti Vabariigi iseseisvuse ja sõltumatuse või territoriaalse terviklikkuse vastu; 2) tegevused, mis on „vastuolus Eesti Vabariigi *julgeolekuhuvidega*"[527]. Esimesed tegevused, kui toime pandud Eesti Vabariigi kodaniku poolt, on karistatavad KarS § 232 alusel. Teised tegevused on karistatavad KarS § $234^2$ alusel. Riigikohus lisab, et Eesti Vabariigi julgeolekuhuvidega vastuolus oleva teo toimepanemine ei tähenda paratamatult, et toime oleks pandud ka tegu Eesti Vabariigi iseseisvuse ja sõltumatuse või territoriaalse terviklikkuse vastu.[528]

Järelikult eksisteerib riigikohtu tõlgenduses kaks selgelt eristuvat hüvede gruppi: 1) Eesti Vabariigi iseseisvus ja sõltumatus või territoriaalne terviklikkus; 2) Eesti Vabariigi julgeolekuhuvid.

Kolleegiumi hinnangul sätestab KarS § $234^2$ „loetelu välisriigi luure- või julgeolekuteenistuse teenistuja või agendi" sellistest tegevustest, mis on „seadusandja hinnangul juba *eelduslikult* suunatud Eesti Vabariigi julgeoleku vastu". [529] Tuginedes seaduse seletuskirjale lisab kohus, et mittesalajaste valdkondade kohta teabe kogumine on „Eesti Vabariigi julgeoleku vastu suunatud tegevuse tüüpnäide" [530]. Eelduse kehtestamisega toimub kolleegiumi hinnangul tõendamiskoormise „mõningane üleminek" [531]. Täpsemalt: KarS § $234^2$ lg-s 1 loetletud tegevuste puhul võib eeldada, et need ohustavad Eesti julgeolekut, kuid süüdistataval ja kaitsjal on „võimalus näidata, et teabe või asja kogumine, hoidmine, edastamine, üleandmine, muutmine või kahjustamine ei olnud konkreetsel juhul siiski suunatud Eesti Vabariigi julgeoleku vastu". [532]

[525] Samas, p-d 17 11) ja 12).
[526] Samas, p 17 15).
[527] Samas, p 114.
[528] Samas, p 109 jj.
[529] Samas, p 127.
[530] Samas, p 128.
[531] Samas.
[532] Samas.

Kolleegium leiab, et G. Mutso Eesti Vabariigi julgeoleku vastu suunatud tegevused on:

1) G. Mutso poolt teabe kogumine ja üleandmine HSL-ile;[533]
2) T. Kõutsi veenmine HSL-ile teavet andma;[534]
3) Eesti Kaitseväe kõrge ohvitseri A-ga kontakti otsimine eesmärgiga värvata ta koostööle HSL-iga.[535]

Kolleegium ei peatu pikemalt küsimusel, „kas üldse ja kui, siis milline julgeolekualane tähtsus oli eraldivõetult sellel konkreetsel teabel, mida G. Mutso ise või T. Kõuts G. Mutso mahitusel HSL-ile üle andis“[536].

Kolleegiumi hinnangul ohustas Eesti Vabariigi julgeolekut:

1) G. Mutso abil ülal hoitud infokanali olemasolu iseenesest;[537]
2) algelise struktuuriga agendivõrgustiku loomine Eestis;[538]
3) G. Mutso kaugem siht saada juurdepääs isikutele, kellel oli „tööalane kokkupuude NATO allasutustega“ ning juurdepääsuluba salajasele teabele.[539]

Ülaltoodust võib välja lugeda, et kui kohtud tuvastavad, et isik on loonud Eesti Vabariigi vastase suhte, tema siht on saada juurdepääs salastatud teabele ning ta on astunud samme agentide värbamiseks, pole KarS § $234^2$ kohaldamise seisukohast enam oluline, millise julgeolekualase tähtsusega teavet, kas kogutakse või edastatakse. Kolleegiumi hinnangul on välisriigi eriteenistusega suhet pidava isiku poolt mistahes mittesalajase teabe kogumine või edastamine eelduslikult Eesti Vabariigi julgeoleku vastane tegevus ning vastupidist peab tõendama süüdistatav (RKKKo 1-21-141, p 127-128).

Veelkord: G. Mutso juhtumi tehioludel pole oluline kogutud teabe sisu. Ja juhul, kui isik tegutseb välisriigi luure- või julgeolekuteenistuse huvides või ülesandel, ei ole teabe sisu oluline ka teistel tehioludel.

[533] Samas, p 129.
[534] Samas.
[535] Samas.
[536] Samas, p 130.
[537] Samas.
[538] Samas.
[539] Samas.

Arvestades, et teave mittesalajastest valdkondadest hõlmab potentsiaalselt kogu Eesti Vabariigi objektiivset tegelikkust, mis eksisteerib väljaspool salastatud teabe kaitseala, võib järeldada, et kui Eesti Vabariigi vastase suhte loonud isik teeb ühekordse päringu äriregistrist kaitsetööstuse äriühingu kohta, on tegemist teabe kogumisega KarS § $234^2$ tähenduses ja eelduslikult Eesti Vabariigi vastase tegevusega ning selline isik peab vastutuse välistamiseks tõendama vastupidist. Kui nii, on ka kaitsetööstuse äriühingu ärisaladuse kogumine eelduslikult Eesti Vabariigi vastane tegevus KarS § $234^2$ mõttes.

Järelikult, eelduslikult peab paika magistritöö teine hüpotees: Kaitsetööstuse äriühingu ärisaladus on teave KarS § $234^2$ tähenduses.

Kuna tegemist on eeldusega võiks edasi uurida, millistele argumentidele tuginedes saab süüdistatav tõendada vastupidist? Kas ja kuidas võiks süüdistatav tõendada, et hangitud ärisaladusel puudub igasugune seos Eesti Vabariigi julgeolekuga? Kas süüdistatav võiks väita, et ärisaladuse hankimine ohustab hoopis konkreetse äriühingu majandustegevust ning tuleks seetõttu kvalifitseerida KarS § 377 järgi?

Arvestades magistritöö piiratud mahtu oleks otstarbekas kitsendada küsimust. Selle asemel, et tuvastada kõikvõimalikke argumente, mis võiksid eelduse ümber lükata, võiks uurida, millistel juhtudel puuduvad igasugused mõistlikud argumendid. Ehk siis: millistel juhtudel on kaitsetööstuse äriühingu ärisaladuse seos Eesti Vabariigi julgeolekuga sedavõrd tugev, et pole võimalik väita, et ärisaladuse kogumine ei ohusta Eesti Vabariigi julgeolekut?

Et küsimusele vastata tuleb eelnevalt välja selgitada, milles seisneb Eesti Vabariigi julgeolek ning mis osa kaitsetööstuse äriühingu ärisaladusest omab selget puutumust Eesti Vabariigi julgeolekuga.

Akadeemilisel eesmärgil on võrdlemisi võimatu saada juurdepääsu konkreetse äriühingu ärisaladusele. Tõsi, jääb õhkõrn võimalus, et mõni äriühing satub tööstus- või ärispionaaži ohvriks ning on seetõttu sunnitud osalema kohtumenetluses. Kuid ka sel juhul on kohtul võimalik piirata ärisaladuse avalikustamist (KrMS § 12 lg 1 p 1, lg 4, lg $4^1$, lg $4^2$) ning karistada

saladuse kohustuse rikkumise eest (KarS § 331[5]).[540] Pealegi, spionaaži ohvriks langenud äriühing ei pruugi üldse soovida osaleda kohtumenetluses. Olgu selleks siis hirm mainekahju või ärisaladuse avalikustamise ees. S. Knickmeier leiab, et äriühingu vaatepunktist võib olla kasulikum teha koostööd julgeolekuasutusega nagu Saksamaa riiklik põhiseaduse kaitse amet (sks *Bundesamt für Verfassungsschutz*), mis tegeleb teabe kogumisega, kui saksa politseiga, mis allub legaliteedi põhimõttele (*Strafprozeßordnung*[541] § 152 lg 2) ning peab kuriteole viitava teabe korral algatama kriminaalmenetluse.[542]

Seega, käesoleva töö raames ei ole võimalik käsitleda konkreetse äriühingu ärisaladusi, vaid tuleb püüda kujundada mulje kaitsetööstuse ärisaladuse olemusest ja selle seotusest Eesti Vabariigi julgeolekuga. Siinkohal on abiks A. Sinisalu teoreetiline käsitlus Eesti Vabariigi julgeolekust ning intervjuud kaitsetööstuse äriühingute esindajatega.

## 4.2 Eesti Vabariigi julgeolek

Julgeoleku mõiste ebamäärasusest annavad märku ajakirjanduslikud katsed tuvastada julgeolekuohte. Eesti Vabariigi julgeolekut ohustavateks teguriteks on peetud muuhulgas tuumaenergiat[543], vaenulikus inforuumis elavaid venekeelseid elanikke[544],

[540] Mainitud sätted võeti vastu seoses ärisaladuse kaitse direktiivi (2016/942) ülevõtmisega. Vt lähemalt: 678 SE. Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seaduse eelnõu seletuskiri.
[541] *Strafprozeßordnung* (Deutschland). BGBl. 2024 I Nr. 109.
[542] Knickmeier, S. Spies without borders? The phenomena of economic and industrial espionage and the deterrence strategies of Germany and other selected European countries. – Security Journal 2020/33, lk 8; Võrdlusena, Eestis kehtib samuti legaliteedi põhimõte (KrMS § 6). JAS § 32 lg 1 järgi on julgeolekuasutus kohustatud edastama oma ülesannete täitmisel saadud teavet teisele riigiasutusele, „kui see on vajalik riigiasutusele pandud ülesannete täitmiseks". Teisisõnu, kui jagada KAPO või Välisluureametiga teavet, millest nähtuvad kuriteo tunnused, on neil seaduse järgi kohustus jagada seda teavet ka nt PPA-ga või KAPO menetlejatega; välja arvatud juhul, kui teabe edastamine kahjustaks julgeolekuasutuse ülesannete täitmist (JAS § 32 lg 1). Järelikult, Eestis on julgeolekuasutusele jäetud kaalutlusõigus otsustada, kas jagada kriminaalmenetlust toimetavate asutustega teavet, mis võib päädida menetluse alustamisega. Kas ja kuidas saab kasutada julgeolekuasutuste seaduse alusel kogutud tõendeid kriminaalmenetluses, on keerulisem teema. Vt: KrMS § 63 lg 1[1]; Grauberg, T., Nääs, O. Paneeldiskussioon teemal „Teabehange ja jälitus kriminaalmenetluses". – Juridica 2024/9-10, lk 671-682; Kergandberg, E. Julgeolek *versus* ehe jälitustegevus, „kah-jälitustegevus" ja teabehankeks maskeerunud eriti varjatud jälitustegevus Eesti õiguses. – Juridica 2024/9-10, lk 657-670.
[543] ERR. Rohelised: tuumaenergeetika on tõsine oht julgeolekule. (19.04.2022). – https://www.err.ee/1608569242/rohelised-tuumaenergeetika-on-tosine-oht-julgeolekule (04.03.2025).
[544] Palts, T. Tõnis Palts: suurim julgeolekuoht on vaenulikus inforuumis elavad venekeelsed. Saage aru, vasturelv on eestikeelne haridus. Eesti Päevaleht 23.02.2022. – https://epl.delfi.ee/artikkel/95992383/tonis-palts-suurim-julgeolekuoht-on-vaenulikus-inforuumis-elavad-venekeelsed-saage-aru-vasturelv-on-eestikeelne-haridus (04.03.2025).

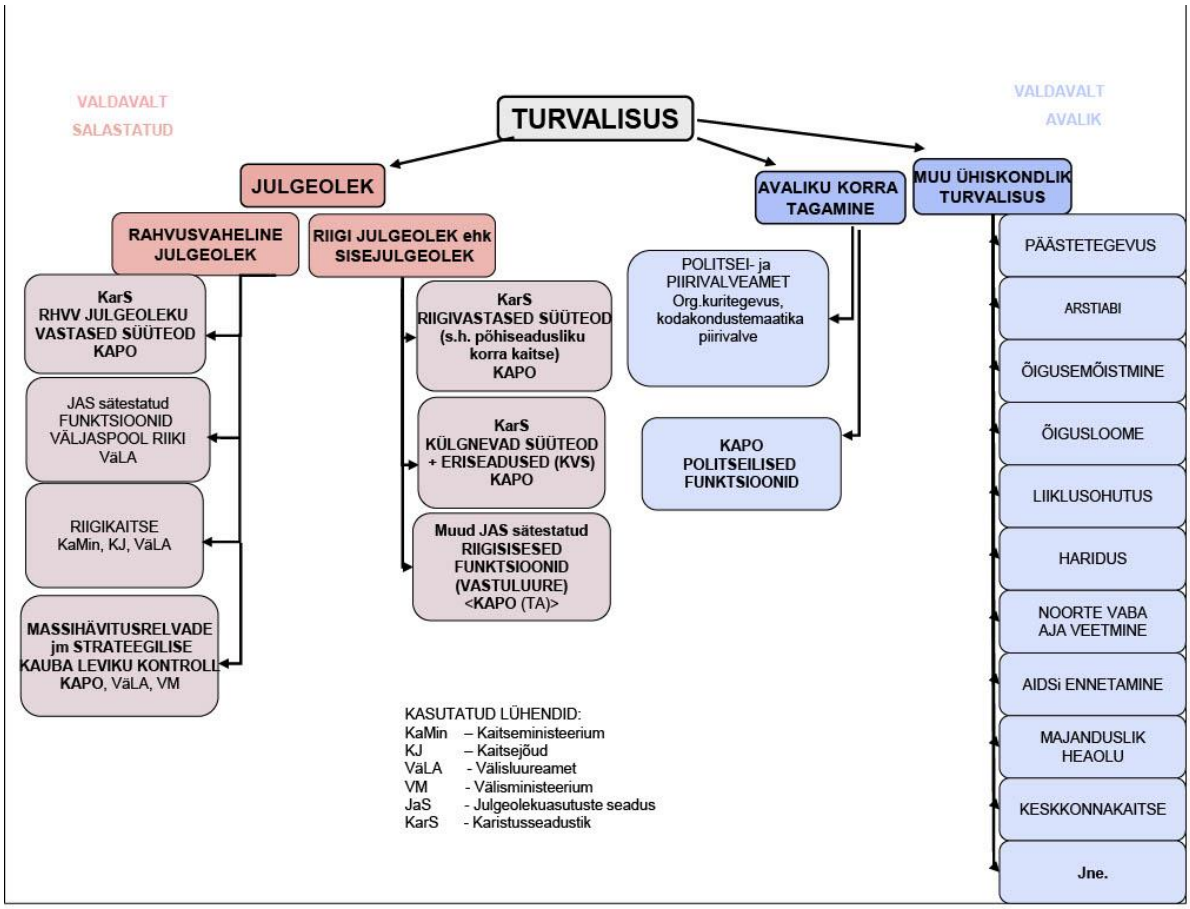
majanduspopulismi[545], kõrghariduse alarahastatust[546] ja Narva-Jõesuu muuli puudumist[547]. Lisaks tööstusjulgeolekule räägitakse veel „toidujulgeolekust“[548], „energiajulgeolekust“[549], „majandusjulgeolekust“ [550], „küberjulgeolekust“ [551]. Ühe parlamendierakonna nägemuses kuulub julgeoleku mõistesse ka „toimetulek“ [552].[553]

Ebaselge ja eklektiline arusaam julgeoleku mõistest ei ole omane ainult ajakirjandusele. Ka erialakirjanduses puudub üksmeel. R. Kiris ja M. Kärner väidavad, et julgeolek hõlmab lisaks Eesti Vabariigi iseseisvusele, sõltumatusele, territoriaalsele terviklikkusele ja põhiseaduslikule korrale muuhulgas „rahva ja riigi kestmist, õigusriiki, turumajandust, inimõigustel põhinevat väärtusruumi ja elanikkonna turvalisust“[554]. Sellise tõlgenduse kohaselt on julgeolekuohuks lastetud inimesed, sest nad ohustavad rahva kestmist; monopolid, sest nad ohustavad turumajandust; joobes juhid, sest nad ohustavad elanikkonna turvalisust. Tegemist on äärmiselt avara käsitlusega, mille karistusõiguslik kaitsmine on võimatu.

Julgeoleku mõistele pühendatud Juridica artikli kokkuvõttes tõdeb J. Jäätma: „Käesoleva artikli otstarbeks ei ole olla tõe kriteeriumiks julgeoleku mõiste avamisel, vaid esmajoones kirjeldada seda, kui keerulise mõistega on tegemist. Julgeoleku mõiste on ja jääb ka tõenäoliselt tulevikus üheselt määratlemata.“[555] Siit ka õppetund: julgeoleku mõiste sisuline ja terviklik käsitlemine magistritöö ühe alapeatükina ei ole mõeldav ega ka mõistlik.

[545] Paron, R. Raino Paron: majanduspopulism on oht julgeolekule. Finance Estonia 23.03.2022. – https://financeestonia.eu/raino-paron-majanduspopulism-on-oht-julgeolekule/ (04.03.2025).
[546] Nagel, H. Hannes Nagel: kõrghariduse alarahastatus on julgeolekuoht. – Postimees 31.03.2022.
[547] Külauudised. Julgeolekuoht Narva-Jõesuus vajab kiiret kõrvaldamist. (27.03.2022). – https://kylauudis.ee/2022/03/27/julgeolekuoht-narva-joesuus-vajab-kiiret-korvaldamist/ (04.03.2025).
[548] Eesti Põllumajandus-Kaubanduskoda. Toidujulgeolek. (12.11.2022). – https://epkk.ee/toidujulgeolek/ (04.03.2025).
[549] Vabariigi Valitsus. Lähme üle kliimaneutraalsele energiatootmisele tagades energiajulgeoleku. (19.06.2023). – https://valitsus.ee/lahme-ule-kliimaneutraalsele-energiatootmisele-tagades-energiajulgeoleku (04.03.2025).
[550] KAPO. Majandusjulgeolek. – https://kapo.ee/et/content/majandusjulgeolek/ (04.03.2025).
[551] Tikk-Ringas, E. Küberjulgeoleku õiguslik raamistik. – Juridica 2012/3, lk 274–283; Kaska, K. Aasmann, L.
[552] Sotsiaaldemokraadid. Toimetulek on julgeolek! – https://valimised.sotsid.ee/teemad/toimetulek-on-julgeolek/ (04.03.2025).
[553] Kuid julgeoleku mõiste ei voha ainult pisikeses piiririigis. D. W. Drezneri hinnangul on ka Ameerika Ühendriikides võimust võtnud ühiskonna julgeolekustumine. Paljuski on selles süüdi 11. septembri terrorirünnakud. (Drezner, D. W. How Everything Became National Security. – Foreign Affairs. September/October 2024). T. Saartsi hinnangul hakkas julgeolekustumine Eestis pihta pärast 2007. aasta pronksiööd. (Saarts, T. Kaitsedemokraatia militaarses infooaasis – Eesti lähitulevik? – Vikerkaar 2024/6.
[554] Kiris, R., Kärner, M. KarS komm § $234^2$, p 1.
[555] Jäätma, J. Julgeoleku mõiste. – Juridica 2020/2, lk 78.

A. Sinisalu käsitleb julgeolekut formaalselt. Katusmõisteks on turvalisus, mis jaotub kolmeks: julgeolek, avalik kord ja muu ühiskondlik turvalisus. Julgeoleku tagamise eest vastutavad enda pädevuste ulatuses valdavalt Kaitseministeerium, Kaitsevägi, Välisluureamet ja Kaitsepolitseiamet. Avaliku korra tagamise eest aga Politsei- ja Piirivalveamet. Muu ühiskondlik turvalisus kuulub Päästeameti, Sotsiaalministeeriumi, Haridusministeeriumi, kohtusüsteemi jt. pädevusse.[556]




**Joonis 1.** Turvalisuse skeem (autor: A. Sinisalu).[557]

A. Sinisalu jagab julgeoleku mõiste tinglikult kaheks: rahvusvaheline julgeolek ja riigi julgeolek ehk sisejulgeolek.[558] Rahvusvahelise julgeoleku tugisammasteks on riigikaitse ja

[556] Joonis 1.
[557] Kasutatud autori loal.
[558] Joonis 1. Märkusena: julgeoleku jagamine kaheks, mille tulemusena tekib konkurents Kaitse- ja Siseministeeriumi vahel ei pruugi olla julgeoleku tagamise vaatepunktist mõistlik. Nagu ütleb K. Pärt: „Riigi julgeolek kui seisund on tervik.“ [Vt: K. Pärt Suurem osa kõrge riskiga julgeolekuohte on mittesõjalised. ERR. (23.04.2025) – https://www.err.ee/1609672700/kristian-part-suurem-osa-korge-riskiga-julgeolekuohte-on-mittesojalised (23.04.2025).] Seda eriti olukorras, kus 2025. aasta riigieelarvet tutvustava infolehe alajaotusest

JAS-is sätestatud funktsioonid väljaspool riiki.[559] Teisisõnu: sõjaline tegevus ja eelhoiatus. Eelhoiatuse eest vastutavad Välisluureamet ja Kaitseväe luurekeskus; sõjaline tegevus kuulub Kaitseväe sõjaaja üksuste pädevusse.[560] Riigi julgeolek kitsas tähenduses moodustub A. Sinisalu järgi järgmistest valdkondadest, mis kõik kuuluvad KAPO pädevusse: 1) põhiseadusliku korra kaitse; 2) riigisaladuse kaitse ja selleks vastuluure korraldamine; 3) võitlus riigi julgeolekut ohustava korruptsiooniga; 4) võitlus terrorismiga, eelkõige selle ennetamine ja tõkestamine.[561]

Sellisel formaalsel käsitlusel on omad puudujäägid. Veidi liialdatult võib jääda mulje, et julgeolek ongi see ja ainult see, mis kaitseväe juhataja või julgeolekuasutuste peadirektorid ütlevad, et julgeolek on. Selline arusaam võib olla isegi ohtlik. Seda eriti olukorras, kus parlament jätab täitevvõimule vabamad käed, sisend eelnõudele tuleb KAPO-lt, õigusmõisted on määratlemata ja kohtulahendid pole avalikud. Tõsi, tänapäeva tegelikkus nõuabki tugevamat täitevvõimu, KAPO käes ongi ekspertiis, julgeolek ongi keeruline mõiste ning kohtulahendite avalikustamine võib seada ohtu meetodid ja taktika või võimaldada teha riigisaladuse kohta „liigseid järeldusi“[562]. Kuid kui lisada siia hulka veel seisukoht, et ainult KAPO peadirektor oskab öelda, mis on riigi julgeolek, võib tekkida õigustatud kahtlus, et tekkinud on tõemonopol.

Sest kui julgeoleku mõiste väljub avalikust käibest ning muutub tehniliseks sõnavaraks, mille kohta võivad arvamusi avaldada ainult eksperdid, võime leida end olukorrast, kus KAPO peadirektor ütleb, et ohtu julgeolekule ei ole, kuid rahvas siiski ohtu julgeolekule tajub. Olukord on analoogiline ka teiste ühiskonna toimimise jaoks oluliste mõistete puhul nagu monopol, majanduskasv, inflatsioon või sõda; kusjuures erimeelsused viimase tõlgendamises on kõige traagilisemate tagajärgedega. Sest ühiskond, kus ühed ütlevad, et käib sõda, ja teised ütlevad, et ei käi, ei kesta kuigi kaua. Mistõttu on ka mõistetav, miks Venemaa eesmärk on sõja

„Peamised sõnumid valitsemisalade kaupa“ leiab *hashtag*'i #riiktõhusamaks juurest kaks täiesti erinevat kõverat. Esimene neist on tagasihoidlikult negatiivse tõusunurgaga ning kujutab Siseministeeriumi valitsemisala eelarvet vahemikus 2022–2028. Teine aga jõuliselt positiivse tõusunurgaga ning kujutab Kaitseministeeriumi valitsemisala eelarvet samas ajavahemikus. Vt: Vabariigi Valitsus. 2025. aasta riigieelarve ja 2025–2028 riigi eelarvestrateegia. Peamised sõnumid valitsemisalade kaupa. KaM ja SiM. – https://valitsus.ee/2025-eelarve#kam (06.01.2025).

[559] Joonis 1.

[560] JAS § 7 p 1; KKS § 3 lg 1 p 1, 2; Kaitseväe põhimäärus § 7 lg 1, § 13 lg 2 p 1; Kaitseväe põhimäärus. – RT I, 28.06.2018, 8.

[561] Joonis 1; Sinisalu, A., Maiberg, H. Linn tuleb hävitada Jehoova auks ehk religioosse äärmusluse oht riigile. – Juridica 2024/8, lk 623.

[562] RKKKo 1-21-1421, p 141.

ja rahu piiri järkjärguline ähmastamine. Igal juhul tuleb demokraatlikule õigusriigile kasuks, kui rahva ja riigi arusaamad olulistest mõistest suures osas kattuvad. Seega tuleb olla valvas, et eksperdid ei saavutaks nende sõnade tähenduse üle liialt suurt võimu.

Lisaks formaalsusele võib kitsale riigi julgeoleku mõistele ette heita rekursiivsust. Nimelt nähtub A. Sinisalu käsitlusest, et riigi julgeolek seisneb muuhulgas võitluses riigi julgeolekut ohustava korruptsiooniga. Ühelt poolt on mõte selge: riigi julgeoleku mõiste lisamisega riigi julgeoleku mõistesse soovitakse eristada KAPO pädevust korruptsiooni vastu võitlemisel PPA pädevusest.[563] Teiselt poolt võib ette heita, et juba formaalse riigi julgeoleku mõiste sees kasutatakse uuesti riigi julgeoleku mõistet, et teha järjekordne formaalne eristus. Formaalsus ja täitevvõimu-keskne maailmapilt kahtlemata hõlbustavad riigiametnike ja haldusõiguslaste omavahelist arutelu, kuid ei pruugi olla need tunnused, mis suurendavad rahva arusaama riigi julgeolekust.

Samuti keskendub Sinisalu vastuluure käsitlus kitsalt riigisaladuse kaitsele. KarS §-iga $234^2$ ei kaitsta aga mitte ainult riigisaladust, vaid ka mittesalajast teavet. Ehk siis laiemalt võiks öelda, et KAPO ülesandeks on riigi vastu suunatud luuretegevuse ennetamine ja tõkestamine (JAS § 6 p 2). Muidugi ei ole mõistlik eeldada, et KarS §-st $234^2$ tuleneb KAPO-le kohustus kaitsta mistahes mittesalajast teavet ehk iga võimalikku infokildu Eesti Vabariigi inforuumis. Küsimus, millise teabe kaitsmine on osa KAPO ülesandest ennetada ja tõkestada riigi vastu suunatud luuretegevust, võiks olla seotud küsimusega, mis on teave KarS § $234^2$ tähenduses.

Vaatamata mõningatele puudujääkidele, mis on formaalsete käsitluste puhul paratamatud, on A. Sinisalu käsitlus kasulik teekaart, mis võimaldab tuvastada kaitsetööstuse valdkonnad, millel on oluline puutumus julgeolekuga. Kuid esmalt tuleks luua seos kaitsetööstuse ja julgeoleku vahel.

### 4.3 Eesti Vabariigi julgeolek ja Eesti kaitsetööstus

Eesti julgeolekupoliitika aluste kohaselt on Eesti sõjalise kaitse eesmärk „ennetada sõjalisi ohte ja vajaduse korral riiki edukalt kaitsta ning sõda võita“[564]. „Et heidutada vastast sõjalist

[563] Politsei- ja Piirivalveameti ja Kaitsepolitseiameti vaheline uurimisalluvus § 2 lg 2.
[564] „Eesti julgeolekupoliitika alused“ heakskiitmine. – RT III, 28.02.2023, 1. Vt Eesti julgeolekupoliitika alused, lk 7.

konflikti alustamist, võtab Eesti tugevdatud kaitsehoiaku, mis tugineb iseseisvale kaitsevõimele ja kollektiivkaitsele.“ [565] Kuigi julgeolekupoliitika alused sõnaselgelt kaitsetööstust ei maini, on vajadus kaitsetööstuse järgi tuletatav sõnapaarist „iseseisev kaitsevõime“[566].

Seos julgeoleku ja kaitsetööstuse vahel tuleneb ka Eesti kuulumisest NATO-sse ja Euroopa Liitu, kuivõrd julgeolekupoliitika aluste kohaselt toetub Eesti julgeolek liikmesusele NATO-s ja Euroopa Liidus.[567] Kaitsetööstuse arendamine on aga NATO ja – nüüd ka – Euroopa Liidu eesmärk.

NATO lepingu art 5 sätestab kollektiivkaitse põhimõte, mille kohaselt käsitatakse rünnakut ühe lepinguosalise vastu rünnakuna kõigi lepinguosaliste vastu ning lepinguosalistel on kohustus asuda rünnatud riigi kaitsele.[568] 2022. aasta Madridi tippkohtumisel vastu võetud alliansi strateegilise kontseptsiooni kolmanda põhimõtte kohaselt tagab art-st 5 tuleneva kohustuse täitmise „meie heidutus- ja kaitsevõime“[569]. NATO hinnangul on heidutus- ja kaitsevõime hädavajalikuks eelduseks „tehnoloogilise eelise säilitamine“[570]. Tehnoloogia tähtsusest NATO heidutusdoktriinis annavad mõista Walesi deklaratsioonis sisalduv üleskutse luua alliansi- ja Euroopa-ülene kaitsetööstus ning Brüsseli tippkohtumisel astutud sammud asutada tehnoloogiaettevõtete kiirendi DIANA ja NATO Innovatsioonifond.[571]

Euroopa Liidu kaitsetööstuse strateegia kohaselt võib käsitada EL-i kaitsevalmidust kui „liidu ja selle liikmesriikide püsivat valmisolekut kaitsta oma kodanike julgeolekut, oma territooriumi, strateegiliste varade ja elutähtsa taristu terviklust ning demokraatia põhiväärtusi ja -protsesse. Kaitsevalmiduse alla kuulub ka võime anda oma partneritele, näiteks Ukrainale,

[565] Samas.
[566] Samas.
[567] Samas, lk 2.
[568] Põhja-Atlandi leping. – RT II 2004, 5, 14.
[569] Välisministeerium. NATO. Alliansi strateegiline kontseptsioon. – https://www.vm.ee/suhted-teiste-riikide-ja-organisatsioonidega/nato/alliansi-strateegiline-kontseptsioon (14.01.2025).
[570] NATO. Deterrence and defence, 13.12.2024.
– https://www.nato.int/cps/iw/natohq/topics_133127.htm#maintain (14.01.2025).
[571] Vt punkt 14: NATO. Wales Summit Declaration, 05.09.2014. –
https://www.nato.int/cps/cn/natohq/official_texts_112964.htm (04.03.2025). Vt punkt 6 d): NATO. Brussels Summit Communique, 14.07.2021. – https://www.nato.int/cps/en/natohq/news_185000.htm (04.03.2025).

sõjalist abi“ [572]. Edasi rõhutab strateegiadokument, et kaitsevalmiduse saavutamiseks on „tingimata vaja tugevat EL-i kaitsetööstust“ [573].

Kaitsetööstuse seose julgeolekuga võib välja lugeda ka 22. juulil 2024 sõlmitud koalitsioonileppest, mille eesmärk on „tagada Eesti inimestele ja ettevõtetele igakülgne kindlustunne“ [574]. Kindlustunde saavutamise esimese samba „Hästi kaitstud Eesti“ raames kavatsetakse „suurendada laiapindseid julgeolekuinvesteeringuid“.[575] Eesmärk on kasvatada Eesti kaitsetööstuse käibemaht aastaks 2030 ühe miljardi euroni.[576] Kaitsetööstuse arendamisel lähtutakse põhimõttest, et „kohalik kaitsetööstus on osa meie laiapindsest riigikaitsevõimest“ [577]. Julgeolekuasutustest on kaitsetööstuse tähtsust julgeoleku tagamisel sedastanud Välisluureamet: „Eesti riik vajab heidutuse ja kaitsevõime tugevdamiseks uusi tehnoloogiaid [...]“[578]

Olles tuvastanud seose Eesti Vabariigi julgeoleku ja Eesti kaitsetööstuse vahel võime väita, et Eesti kaitsetööstuse vastane tegevus on ühtlasi Eesti Vabariigi julgeoleku vastane tegevus. Arvestades raskusi, mis kaasnevad kaitsetööstuse määratlemisel (vt 2. peatükk), oleks mõistlik tuvastada need kaitsetööstuse valdkonnad, kus seos Eesti Vabariigi julgeolekuga on kõige tugevam. Nii saaksime väita, et kui välisriigi luure- või julgeolekuteenistuste huvides või ülesandel tegutsev isik hangib ärisaladust nendest kaitsetööstuse valdkondadest realiseerib ta kindlasti KarS § $234^2$ koosseisu. Teisiti öeldult: sel juhul puuduvad süüdistataval mõistlikud argumendid lükkamaks ümber eeldust, et teabe kogumine mittesalajastest valdkondadest ohustab Eesti Vabariigi julgeolekut (RKKKo 1-21-1421, p-d 127 ja 128).

### 4.4 Eesti Vabariigi julgeoleku vastane tegevus

642 SE seletuskirja järgi on „Eesti Vabariigi julgeoleku vastase tegevuse“ mõiste tõlgendamisel abi muuhulgas riigi julgeolekuteabe hanke ja analüüsi kavast.[579] Tõsi, kõnealune kava annaks

[572] Euroopa Komisjon. Ühisteatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele. Uus Euroopa kaitsetööstuse strateegia: EL-i valmisoleku saavutamine reageerimisvõimelise ja keskse Euroopa kaitsetööstuse abil. Brüssel 05.03.2024, lk 1.
[573] Samas.
[574] Vabariigi Valitsus. Koalitsioonilepe 2024–2027. – https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2024-2027 (14.11.2024).
[575] Samas.
[576] Samas. Uued investeeringud ja ettevõtete kindlustunne. Eesti kaitsetööstuse arendamine.
[577] Samas.
[578] Eesti rahvusvahelises julgeolekukeskkonnas 2024, lk 87.
[579] 642 SE. Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (terrorismivastase võitluse direktiivi ülevõtmine) eelnõu seletuskiri, lk 5.

tõepoolest suurepärase ülevaate, milliseid tegevusi peavad Vabariigi Valitsus, julgeolekuasutused ja Kaitseväe kaitseväeluure Eesti Vabariigi julgeoleku vastaseks (JAS § 9 lg 2). Ja juhul, kui tööstusspionaaži kuulub nende tegevuste hulka, oleks ehk võimalik välja lugeda ka konkreetsed valdkonnad või isegi äriühingud, kus oht julgeolekule on kõige suurem. Kahjuks või õnneks on riigi julgeolekuteabe ja analüüsi kava riigisaladus (RSVS § 9 p 9), mistõttu peame tuginema muudele allikatele.

S. Hegmann ja F. Stuppi hinnangul on StGB § 99, mis oli Eesti seadusandja eeskujuks KarS § $234^2$ loomisel, abstraktne ohudelikt.[580] Saksa õigusteadlaste väitel seisneb abstraktne oht teise poole „paranenud võimalustes“ (*die verbesserten Möglichkeiten*).[581] Järelikult, kui KarS § $234^2$ on abstraktne ohudelikt, võiks mittesalajase teabe kogumise ja edastamise oht Eesti Vabariigi julgeolekule seisneda selles, et paraneb Eesti Vabariigi vastaste positsioon riikidevahelises sõjalises või mittesõjalises vastasseisus. Seega: mida suurema eelise annab kogutav teave Eesti Vabariigi vastastele, seda suurem on oht Eesti Vabariigi julgeolekule.

S. Hegmanni ja F. Stuppi seisukoht annab kasuliku kriteeriumi, mille alusel hinnata kogutava mittesalajase teabega kaasnevat ohtu Eesti Vabariigi julgeolekule. Samas võiks küsida, kas Eesti õigusteaduses on kujunenud selge seisukoht, kas KarS § $234^2$ on kahjustus- või ohudelikt. RKKK 1-21-1421 p-s 128 leiab kolleegium, et KarS § $234^2$ lg-s 1 „kirjeldatud koosseisutegude puhul saab eeldada, et need kahjustavad Eesti julgeolekut [...]“. Sõna „kahjustatakse“ kasutamine võiks viidata kahjustusdeliktile. Samas sedastab kolleegium sama otsuse p-s 130, et Eesti Vabariigi julgeolekut: „[O]hustas [...] juba G. Mutso abil ülal hoitud infokanali olemasolu iseenesest.“ Veel leiab kolleegium: „Ehkki tegemist oli algelise struktuuriga, kätkes see endas arvestatavat ohupotentsiaali.“[582]

R. Kiris ja M. Kärner peavad KarS §-i 234 ehk salakuulamise koosseisu abstraktseks ohudeliktiks.[583] Võrdlusena, J. Sootak peab salakuulamist kahjustusdeliktiks, öeldes, et riigisaladuse väljaandmine välisriigile kahjustab riigi välist julgeolekut.[584] Seda seisukohta toetab ka RSVS. Nimelt sätestatakse RSVS §-des 6-10 riigisaladuse liigid – nt julgeolekuasutuste riigisaladus – ning täpsustatakse iga liigi juures punkthaaval sinna alla

[580] 642 SE seletuskiri, lk 6; StGB-MK, § 99 vnr 3, 4.
[581] StGB-MK, § 99 vnr 3, 4. Vt ka § 93 vnr 24.
[582] RKKKo 1-21-1421, p 130.
[583] Kiris, R., Kärner, M, komm § 234, p 2.
[584] Sootak, J. Karistusõigus. Üldosa, lk 192.

kuuluvad teabekategooriad, nt „varjatult kogutud teave“ (RSVS § 9 p 4). Sealjuures on iga punkti juurde lisatud välistav tingimus: „välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut“ (RSVS § 9 p 3). Sõna „kahjustab“ kasutamine annab mõista, et riigisaladuse kogumise või edastamisega kahjustatakse Eesti Vabariigi julgeolekut. Järelikult võiks KarS § 234 olla kahjustusdelikt.

KarS § 234 ja KarS § $234^2$ kaitsevad sama õigushüve (Eesti Vabariigi julgeolek), kuid ründeobjektid on erinevad. Esimesel juhul on selleks salastatud teave, teisel juhul peamiselt mittesalajane teave. Salastatud teabe ründamisega riivatakse Eesti Vabariigi julgeolekut oluliselt intensiivsemalt kui siis, kui rünnatakse mittesalajast teavet. Sellest annab märku ka 642 SE seletuskiri, mis nimetab KarS §-i $234^2$ subsidiaarseks KarS §-de 231, 232, 233 või 234 suhtes.[585] J. Sootaki järgi seisneb kahe süüteokoosseisu subsidiaarsus selles, et kuigi õigushüved kattuvad, kaitseb üks koosseis ehk primaarkoosseis õigushüve „märksa intensiivsema või kaugemasse staadiumisse jõudnud ründe eest kui subsidiaarkoosseis“[586]. Järelikult kaitseb KarS § 234 Eesti Vabariigi julgeolekut märksa intensiivsema ründe eest kui KarS § $234^2$. Tuginedes J. Sootaki seisukohale[587], et kahjustus- ja ohudelikte eristatakse ründamise intensiivsuse järgi, saab väita, et KarS § $234^2$ kui süüteokooseis, mis kaitseb Eesti Vabariigi julgeolekut madalama intensiivsusega ründe eest, on ohudelikt.

J. Sootaki järgi seisneb abstraktne ohudelikt koosseisus ettenähtud teo „üldises ohtlikkuses“, st ohu saabumist või ohtliku olukorra tekkimist ei ole tarvis tõendada.[588] Teisiti öeldult, KarS § $234^2$ puhul ei ole vaja tõendada, et mittesalajase teabe kogumisega sattus ohtu Eesti Vabariigi julgeolek. RKKKo 1-21-1421 p-s 128 sätestatud tõendamiskoormise ümberpööramine seda eesmärki ka täidab: prokuratuur ei pea tõendama, et mittesalajase teabe kogumisega ohustati Eesti Vabariigi julgeolekut. Küll aga jääb süüdistatavale võimalus tõendada vastupidist. Järelikult võiks pidada KarS §-i $234^2$ sarnaselt oma saksa eeskujuga abstraktseks ohudeliktiks.

Tulles tagasi S. Hegmanni ja F. Stuppi seisukoha juurde, et oht seisneb vastase „paranenud võimalustes“[589], uurime edasi, millistel juhtudel saab vastane sedavõrd suure eelise, et

[585] 642 SE seletuskiri, lk 6.
[586] Sootak, J. Seadusainsus. Kui isiku tegu vastab mitmele süüteokoosseisule, siis mitme järgi ja kuidas ta tegelikult vastutab? – Juridica 2010/1, lk 15.
[587] Sootak, J. Karistusõigus. Üldosa, lk 192.
[588] Samas, lk 193.
[589] StGB-MK, § 99 vnr 3, 4. Vt ka: § 93 vnr 24.

süüdistatava jaoks osutub eelduse ümberlükkamine sisuliselt võimatuks. Tuginedes A. Sinisalu julgeoleku käsitlusele[590] väidan, et vastane saab olulise eelise, kui suudab hankida ärisaladust kaitsetööstuse äriühingutest, mis pakuvad tooteid või teenuseid, mida Kaitsevägi kasutab riigikaitses ehk otseses sõjalises tegevuses, nt droonirünnaku tõrjumisel või vasturünnaku korraldamisel. Samuti annavad vastasele olulise eelise tooted ja teenused, mida Kaitsevägi ja Välisluureamet kasutavad eelhoiatuse ülesande täitmisel ning KAPO kasutab vastuluures. Omalt poolt lisaksin veel loetellu Politsei- ja Piirivalveameti tegevuse riigipiiri kaitsmisel ja kübervaldkonna laiemalt.

Eelhoiatuse tähtsust illustreerivad nii Ameerika Ühendriikide luureandmed Venemaa vägede liikumise kohta enne täiemahulise sõja algust Ukrainas kui ka Iisraeli luure läbikukkumine 7. oktoobri rünnaku ärahoidmisel.[591] Eesti Vabariigi jaoks on eelhoiatus seda olulisem, et vastasseisus Venemaaga esineb märkimisväärne jõudude ebatasakaal. Mida varem me rünnakust teada saame, seda suurem on tõenäosus organiseerida vastupanu. Enamgi veel: Venemaa praegused ja ajaloolised katsed hävitada ja orjastada teisi rahvaid kinnitavad, et eelhoiatus võib määrata, kas ja kui palju Eesti rahvast ja kultuurist jääb püsima. Kaitsevägi kirjutab: „Sõjalise eelhoiatuse tagamine on üks olulisimaid ülesandeid luurekeskuse töös, kuna see võimaldab edastada õigeaegse info otsustajatele nii kaitseväes kui valitsuses, mille aluseks võetakse vastu näiteks otsus kuulutada välja reservväe mobilisatsioon.“[592] Seetõttu on ka loogiline, et eelhoiatus asetseb riigikaitse arengukava olulisemate arendustegevuste loetelus.[593]

Sama oluline on vastuluure. Venemaa tegevus Ukrainas näitab, et üheks oluliseks elemendiks Ukraina vastupanu murdmisel on olnud Vene eriteenistuste agendid Ukraina riigikaitse- ja julgeolekuasutustes.[594] Mainimata ei saa ka jätta, et Butša linn ei sattunud juhuslikult Vene

[590] Joonis 1.
[591] Lieber, D. Israel Missed Signs in Plain Sight Hamas Was About to Attack, First Oct. 7 Probe Finds. The Wall Street Journal 27.02.2025. – https://www.wsj.com/world/middle-east/israel-oct-7-inquiry-report-41ea7efa (04.03.2025). Tsitaat: *„In recent decades, military intelligence had strayed from the key mission of providing an early warning and become deeply involved in providing tactical intelligence for Israel's wider military operations.“.* Gustafson, K. jt. Intelligence warning in the Ukraine war, Autumn 2021-Summer 2022. – Intelligence and National Security 2024/ 39 (3), lk 400–419. Tsitaat: *„In that way, this case is also a success story for American, British and other partnered intelligence communities, whose diplomatic and media campaigns led to an enthusiastic and united response in support of Ukraine, but also restored the tarnished reputations of their intelligence services following the war in Iraq. Thus, warning intelligence during the run-up to, and since, the invasion of Ukraine represents an entirely new chapter in the political and diplomatic use of intelligence in international affairs.“*
[592] Eesti Kaitsevägi. Mida võiks teada kaitseväeluurest? – Ajakiri Sõdur 2025/1, lk 9.
[593] Riigikantselei. Riigikaitse arengukava 2022–2031. Tallinn 2021, lk 11 jj.
[594] Oleg Kulinitši juhtum: State Bureau of Investigation. Former Head of the Security Service of Ukraine (SBU) in the Autonomous Republic of Crimea Oleh Kulinich will stand trial. (03.07.2023). –

vägede massimõrva ohvriks. Nimelt elasid Butšas muuhulgas Ukraina julgeolekuasutuse SBU töötajad.[595] Eelhoiatuse ning luure ja vastuluure tähtsust rõhutab ka Eesti julgeolekupoliitika alusdokument.[596] Siseministeeriumi sisejulgeoleku osakonna juhataja Kristian Pärt kirjutab: „Venemaa relvajõududel on potentsiaali meid tulevikus sõjaliselt ohustada, aga ulatuslik mittesõjaliste ja hübriidsete meetodite rakendamine Eesti ja meie liitlaste vastu oli Kremlil aktiivselt töös eile, on täna ja on ka homme.“[597] Riigi julgeoleku tagamine mittesõjaliste ennetavate vahendite abil on julgeolekuolekuasutuste eesmärk (JAS § 2 lg 1).

Kui luure- ja vastuluure puhul on seos julgeolekuga selge, jagunevad piirivalve puhul arvamused kahte lehte. A. Sinisalu liigitab PPA tegevuse avaliku korra tagamise alla.[598] Sellele arvamusele vastanduvad Eesti poliitikas juba enam kui kümme aastat kõlanud hääled, mis soovivad taastada sõjaväelise piirivalve.[599] Viimati tõusetus teema Kristen Michali valitsuse koalitsioonilepingu lisas, kus käidi välja mõte suurendada PPA võimet tõkestada hübriidrünnakuid, sh muretseda tankitõrjerelvad.[600]

https://dbr.gov.ua/en/news/kolishnij-nachalnik-golovnogo-upravlinnya-sbu-v-ar-krim-oleg-kulinich-postane-pered-sudom (04.03.2025); SBU terrorismivastase üksuse juht: Melkozerova, V. Ukrainian spies accuse Kyiv's anti-terror chief of being a Russian mole. Politico 12.02.2025. – https://www.politico.eu/article/ukrainian-spies-russia-federal-security-service-fsb-security-service-of-ukraine-sbu-vasyl-malyuk/ (04.03.2025); Racz, A. Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist. FIIA Report 43. (16.06.2015) – https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf (23.04.2025); Watling, J., Reynolds, J. The Plot to Destroy Ukraine. Royal United Services Institute for Defence and Security Studies. Special Report, 15.02.2022. – https://static.rusi.org/special-report-202202-ukraine-web.pdf (04.03.2025). Tsitaat eeltoodud eriraportist, mis annab aimdust Vene eriteenistuste tegevuse ulatusest Ukraina riigi nõrgestamisel seestpoolt: (*„Meeting with Ukrainian security officials there is a widespread acknowledgement that many of their colleagues – even in some quite senior positions – are working for or sympathetic to Russia. A shadow structure has emerged inside the Ukrainian government to move information around known Kremlin assets.“*)

[595] 38. Eesti õigusteadlaste päevade paneel „Jälitus ja teabehange kriminaalmenetluses“ (26.09.2024). A. Sinisalu: „Kes natukene neid avalikke andmeid põhjalikumalt töötleb leiab seda, et Butša oli seotud Ukraina siseteenistuse SBU-ga. Et sinna läksid vene väed sisse. Nad teadsid täpselt, keda nad sealt otsivad, mida nad teevad. Nad kogusid aastate jooksul informatsiooni nendest inimestest, kes kuuluvad elimineerimisele ehk tapmisele.“

[596] Eesti julgeolekupoliitika alused, lk 8.

[597] Pärt, K.

[598] Joonis 1.

[599] Laur, S. Me vajame sõjaväelise piirivalve taastamist. – Postimees 04.03.2025; Saar, J., Kõuts, T. Jüri Saar ja Tarmo Kõuts: Eesti kohus on taastada sõjaväeline piirivalve. – Postimees 13.04.2017; ERR. SDE ja Reformierakond ei toeta sõjaväelist piirivalvet. (09.10.2018). – https://www.err.ee/867743/sde-ja-reformierakond-ei-toeta-sojavaelist-piirivalvet (04.03.2025); Nisametdinov, I. Keskerakond tahab taastada sõjaväestatud piirivalve ajateenijad piirile saates. ERR 09.10.2018. – https://www.err.ee/867689/keskerakond-tahab-taastada-sojavaestatud-piirivalve-ajateenijad-piirile-saates (04.03.2025); Sinikalda, M. EKRE soovib taastada sõjaväestatud piirivalve. – Postimees 04.01.2015.

[600] Pulk, M. Siseminister Läänemets „poolsõjaväestab“ piirivalve. – Postimees 20.07.2024.

L. Mälksoo jt. järgi sõltub territoriaalse üksuse tunnustamine riigina „teatud kindla territooriumi olemasolu[st], millel viiakse ellu võimu teatud rahva üle“ [601]. Sealjuures on riigipiir „just see element, mis lubab piiritleda teatud territooriumi ja eraldada see kõrval asetsevate riikide õiguskordadest“[602]. Ühtlasi tähistab Eesti piir Venemaaga Euroopa Liidu ja NATO idapiiri, mis loob selge seose piirivalve ja Eesti Vabariigi julgeoleku vahel. Seost tugevdavad juhtumid, kus Vene eriteenistused on värvanud agente salakaubavedajate seast kogumaks teavet Eesti piirivalve kohta.[603] Salakaubaveo puutumust julgeolekuga ilmestavad kaks traagilist juhtumit KAPO ametnikega: Piusa külas hukkus salakaubaveo kriminaalasja menetlemise raames Tarmo Laul ning Krimmi annekteerimise järgselt 2014. aasta 5. septembril rööviti Eesti-Vene piirilt Eston Kohver. [604] Endine KAPO peadirektor A. Sinisalu kommenteerib Kohveri juhtumit järgmiselt: „Me tundsime põhjendatud huvi, millega tegelevad salakaubavedajad Eesti kagupiirkonnas. [...] See, et osa nendest salakaubavedajatest olid seotud Vene eriteenistustega, oli selline üldine teadmine.“ [605] PPA Lõuna prefektuuri piirivalvebüroo juht Meelis Saarepuu sõnul toimetavad piiril nüüd ka Vene eriüksused.[606]

Veel on Venemaa eemaldanud poisid Narva jõelt ning korraldanud koostöös Valgevenega ränderündeid Euroopa Liidu idapiiri vastu. [607] Kõnealused ründeid nimetab KAPO „hübriidoperatsioonideks“ [608] ning need ei ähvarda ainult maismaapiiri. Venemaa ja Hiina

[601] Mälksoo, L., Land, K., Madise, L., Pisuke, H. PS komm § 122. – Eesti Vabariigi põhiseadus. Komm vlj. 5. vlj. Tartu: Sihtasutus Iuridicum, 2020.
[602] Samas.
[603] KAPO aastaraamat 2019–2020, lk 27; Prokuratuuri aastaraamat 2017. Inna Ombler. Tsitaat: „Topeltkodakondsusega isikuid iseloomustab see, et nad elavad reeglina Vene Föderatsioonis piirialadel ja nende puhul on tavaliselt tegemist salakaubavedajatega [...] Värbamise järgselt salakaubavedusid Eesti suunal teostades hakkavad nad täitma ka neid ülesandeid, mida eriteenistuse agendijuhid neile annavad, kogudes näiteks Eesti Vabariigist erinevat julgeolekut või kaitsevõimet puudutavat informatsiooni.“
[604] Anvelt, K. Täismahus: Tunnistajast tapjaks: Piusa õppetunnid. – Eesti Ekspress 14.02.2012; Kalev, M., Pere, B. Kuidas vabastati Eston Kohver. Suure avaliku lärmi varjus punus KAPO salaja teist plaani. – Eesti Ekspress 04.09.2024.
[605] Kalev, M., Pere, B.
[606] Breidaks, A. Lõuna piirivalvejuht: me näeme Vene eriüksusi piiril. On selge, et see on ärevust tõstnud. Postimees (12.04.2025).
[607] Einmaa, I.-M. Eesti loob võimaliku ränderünde ohjeldamiseks 1000-liikmelise kriisirühma. ERR 04.03.2025. – https://www.err.ee/1609497214/eesti-loob-voimaliku-randerunde-ohjeldamiseks-1000-liikmelise-kriisiruhma (04.03.2025); Nikolajev, J. Venemaa eemaldatud poide tõttu on Narva jõel piiririkkumiste arv kasvanud. ERR 25.09.2024. – https://www.err.ee/1609471057/venemaa-eemaldatud-poide-tottu-on-narva-joel-piiririkkumiste-arv-kasvanud (04.03.2025).
[608] KAPO aastaraamat 2023–2024, lk 10. Välisluureameti peadirektor ei poolda mõiste „hübriid“ kasutamist: Martin, A. Estonian spy chief: 'Hybrid schmybrid, what's happening is attacks'. The Record 17.02.2025. – https://therecord.media/estonian-spy-chief-russia-hybrid-attacks-are-real-attacks (05.03.2025). Tsitaat: *"I think the word 'hybrid' is misleading and soft… What's happening is attacks, cyberattacks, assassination plots, maybe in some parts it's actually state-sponsored terrorism what is going on."*

kontrolli all olevate laevade rünnakud merekaablitele kinnitavad ka merepiiri seire tähtsust.[609] Merepiiri seire seos julgeolekuga tuleneb asjaolust, et tegemist on mereväe kui ühe kaitseväe struktuuriüksuse põhiülesandega. [610] Riigipiiri vastu suunatud rünnakute ennetamine ja tõkestamine on ka NATO huvides, kuivõrd tekib küsimus, mis hetkest alates võiks hübriidrünnak tekitada NATO art-st 5 nähtuva kollektiivkaitse kohustuse.[611]

Piirivalve seost kaitse- ja julgeolekuvaldkonnaga toetab ka RHS § 169 lg 1 punkti 2 tõlgendus. 113 SE I seletuskirja kohaselt kohaldatakse kõnealust sätet, mis sisaldab „julgeolekuotstarbelise asja" mõistet, muuhulgas riigihangete suhtes, kus „kaitsevägi ja mittesõjalised jõud teevad koostööd samade ülesannete täitmiseks ja/või kus riigihanke eesmärk on kaitsta riigi julgeolekut oma territooriumil"[612]. Direktiivi 2009/81/EÜ põhjenduse 11 kohaselt võib selline tegevus hõlmata näiteks piirikaitset.

Järelikult on piirivalvel tugev seos julgeolekuga, mistõttu saab sama väita äriühingute kohta, mis pakuvad piirivalvele vastavaid tehnoloogiaid.

Küberkaitse (*cyber defense*) või küberturvalisuse[613] (*cyber security*) puhul on võimalik eristada vähemalt nelja gruppi asutusi/isikuid ja vastavaid tegevusvaldkondi:

1) Küberväejuhatuse tegevus Kaitseministeeriumi vastutusalas küberkaitse korraldamisel (Kaitseväe põhimäärus § 14 lg 2 p 1);
2) Välisluureameti ja KAPO tegevus riigisaladuse ja salastatud välisteabe kaitsmisel (JAS § 6 p 2, § 7 lg 1 p 2, 4);
3) RIA tegevus küberturvalisuse valdkonnas (RIA põhimäärus[614] § 8 lg 4);

[609] KAPO aastaraamat 2023–2024, lk 54; Kauranen, A. Finland's secret service says frequency of cable incidents is 'exceptional'. Reuters 04.03.2025. – https://www.reuters.com/world/europe/finlands-secret-service-says-frequency-cable-incidents-is-exceptional-2025-03-04/ (04.03.2025). Leicester, J., Burrows, E. At least 11 Baltic cables have been damaged in 15 months, prompting NATO to up its guard. Associated Press 28.01.2025. – https://apnews.com/article/nato-france-russia-baltic-cables-ships-damage-764964a275530915c2cc5af1125ec125 (04.03.2025).
[610] Kaitseväe põhimäärus § 3 lg 4 p 2, § 19 p 4, 5. Nimetatud ülesanded anti mereväele Vabariigi Valitsuse määrusega: Vabariigi Valitsuse 18. juuli 2022. a määrus nr 71 „Vabariigi Valitsuse määruste muutmine seoses Politsei- ja Piirivalveameti laevade üleandmisega Kaitseministeeriumi valitsemisalasse". – RT I, 21.07.2022, 1.
[611] Bajarunas, E. Using NATO's Article 5 Against Hybrid Attacks. CEPA 11.02.2025. – https://cepa.org/article/using-natos-article-5-against-hybrid-attacks/ (04.03.2025).
[612] 113 SE I. Riigihangete seaduse muutmise seaduse eelnõu seletuskiri, lk 6.
[613] Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2024–2030 „Läbivalt IT-vaatlikum Eesti". – https://www.mkm.ee/sites/default/files/documents/2024-07/Kyberturvalisuse%20strateegia%202024-2030_labivalt_IT_vaatlik_Eesti.pdf (04.03.2025).
[614] Riigi Infosüsteemi Ameti põhimäärus. – RT I, 27.12.2024, 10.

4) Muude asutuste ja isikute tegevus küberturvalisuse valdkonnas, sh isikud, kelle tegevus on reguleeritud küberturvalisuse seaduse[615] alusel.

Kui äriühing pakub tooteid ja teenuseid ainult Küberväejuhatusele, Välisluureametile või KAPO-le, on seos Eesti Vabariigi julgeolekuga selge. Kui tooteid ja teenuseid pakutakse teistele asutustele või isikutele, ei ole seos julgeolekuga enam üheselt mõistetav. Eraldi küsimus tekib, kui äriühingu tooted või teenused on nii kaitse- kui ka tsiviilotstarbelised ehk kahesuguse kasutusega tooted, kuidas sel juhul hinnata seost julgeolekuga? K. Hartley on püstitanud küsimuse seoses Euroopa kaitsetööstuse mõistega, et kas äriühing, mille müügitulust 50% tuleb kaitsetööstusest, on kaitsetööstusettevõte?[616] Sama moodi võiks küsida siin, et kas seos julgeolekuga on seda suurem, mida rohkem müügitulust tuleb julgeolekuga seotud allikatest? See võib olla üks argumentidest.

Seos Eesti Vabariigi julgeolekuga võib tuleneda ka kaitsetööstuse äriühingu seotusest NATO või Euroopa Liidu liikmesriikidega. Sellist tõlgendust toetab 468 SE-ga tehtav täiendus Vabariigi Valitsuse määrusesse[617], mis kehtestab riigisaladuse ja salastatud välisteabe kaitse korra. Kõnealune täiendus puudutab RSVS § 7 p-s $6^1$ sätestatud uut salastamisalust, mis on seotud sõjalise otstarbega asjaga. Muudatusega lisatakse Vabariigi Valitsuse määruse §-i 5 lõige $6^1$, kus kasutatakse väljendit: „[...] kui selle avalikuks tulek kahjustaks Eesti Vabariigi või muu EL või NATO liikmesriigi julgeolekut.“[618] 468 SE seletuskirjas selgitatakse, et Eesti riigikaitse on tihedalt integreeritud EL-i ja NATO sõjalise kaitsega, mistõttu olukorras, kus teabe avalikustamisega ei kahjustata vahetult Eesti Vabariigi julgeolekut, on siiski võimalik jaatada Eesti Vabariigi julgeoleku kahjustamist seeläbi, et kahjustatud on mõne teise NATO või EL-i liikmesriigi julgeolekut.[619] Seletuskiri rõhutab: „[T]eabe salastamise üle otsustades [tuleb] hinnata julgeolekuohtu tavapäraselt laiemalt.“[620] Järelikult, kaitsetööstuse äriühingu seotus NATO või EL liikmesriikide kaitsetegevusega võib samuti näidata, et ühingu äritegevusel on seos Eesti Vabariigi julgeolekuga.

[615] Küberturvalisuse seadus. – RT I, 21.06.2024, 15.
[616] Hartley, K. Europe’s Defence Industry: An Economic Outlook. Fondation pour la Recherche Strategique, 2013 juuli. – https://www.frstrategie.org/sites/default/files/documents/publications/notes/2013/201323.pdf (04.03.2025).
[617] Vabariigi Valitsuse 20. detsembri 2007. a määrus nr 262 „Riigisaladuse ja salastatud välisteabe kaitse kord“.
[618] 468 SE seletuskiri, lk 19.
[619] Samas, lk 19–20.
[620] Samas, lk 20.

Veel võiks küsida: mil määral mõjutab kaitsetööstuse äriühingu seost Eesti Vabariigi julgeolekuga asjaolu, et äriühingu tooteid või teenuseid kasutavad Ukraina riigikaitse- või julgeolekuasutused. Teisiti väljendatult: kas Ukraina julgeolekuhuvide edendamine tähendab paratamatult ka seost Eesti Vabariigi julgeolekuga?

Eesti julgeolekupoliitika kohaselt on Eesti huvides „aidata Ukrainal sõda võita ja säilitada iseseisvus ning taastada territoriaalne terviklikkus“[621]. Selle eesmärgi saavutamiseks toetab Eesti Ukraina liitumist Euroopa Liidu ja NATO-ga. Samuti on „Eesti Ukraina ülesehitamisel diplomaatiliselt aktiivne, annab kaitsealast abi, osaleb sõja tagajärjel hüvitatud taristu taastamisel, pakub oskusteavet Ukraina riigi ja majanduskeskkonna arendamiseks ning aitab sõjas vigastatute raviga. Eesti annab Ukrainale humanitaarabi“ [622]. Eesti koguabi suurus summas 1,2 miljardit eurot[623] annab mõista, et Eesti on alates 2014. aastast tegutsenud endise kaitseväe juhataja Riho Terrase sõnade järgi: „Ukraina võitlus on meie võitlus [...]“[624]

Kindlasti on Ukraina ja Eesti Vabariigi julgeolek omavahel seotud. Eraldi küsimus on, kas Eesti ja Ukraina julgeolek on ka jagamatu. Julgeolekupoliitika järgi toetub Eesti julgeolek „liikmesusele [NATO-s] ja Euroopa Liidus [...] ning tihedale koostööle liitlaste ja teiste rahvusvaheliste partneritega. Eesti käsitab iseenda ja liitlaste julgeolekut jagamatuna.“ [625] Pigem tuleks jaatada tõlgendust, mille kohaselt mõeldakse liitlaste all NATO ja Euroopa Liidu liikmeid. Eesti küll toetab Ukraina liitumist mainitud organisatsioonidega, kuid Ukraina ja Eesti Vabariigi julgeoleku lugemine jagamatuks tähendaks, et oleksime Venemaaga ametlikult sõjas. Tõsi, tänapäeva maailmas ei alga sõjad enam ametliku sõjakuulutusega – veel vähem alustab neid nõnda hübriidsõda viljelev Venemaa – kuid õiguslikus mõttes ei oleks korrektne (hetkel) käsitada Ukraina ja Eesti Vabariigi julgeolekut jagamatuna. Tunnistan, sellise juriidilise tõlgenduse puhul on raske leppida olukorraga, kus Ungari ja Eesti julgeolek on jagamatu, aga Ukraina ei ole meie liitlane.

See aga ei tähenda, et Eesti kaitsetööstuse äriühingu Ukraina-suunalist äritegevust ei võiks lugeda toetavaks argumendiks, kui vaja otsustada, kas kõnealuse äriühingu tegevus on seotud

[621] Eesti julgeolekupoliitika alused, lk 9.
[622] Samas.
[623] Välisministeerium. Eesti toetus Ukrainale. (10.01.2024). – https://www.vm.ee/uudised/eesti-toetus-ukrainale (04.03.2025).
[624] Eesti Kaitsevägi. Kaitseväe juhataja: Ukraina võitlus on meie võitlus. (06.04.2015). – https://mil.ee/uudised/kaitsevae-juhataja-ukraina-voitlus-on-meie-voitlus/ (04.03.2025).
[625] Samas.

Eesti Vabariigi julgeolekuga. Näiteks ostis Eesti riik hiljutise 100 miljoni euro suuruse Ukraina abipaketi raames kodumaiste kaitsetööstuse äriühingute Milrem, Threod ja Defsecintel toodangut.[626] Tegemist võiks olla ühe argumendiga, miks lugeda Milremi, Threodi ja Defsecinteli äritegevust seotuks Eesti Vabariigi julgeolekuga.

Võõrriigi eriteenistuste huvi konkreetsete äriühingute või ärivaldkondade vastu võib samuti viidata nende äriühingute või valdkondade seotusele Eesti Vabariigi julgeolekuga. Teisisõnu, kui on teada, et vastase eriteenistusi huvitavad teatud valdkonnad, võiks neid valdkondi pidada eelduslikult seotuks julgeolekuga. Paar näidet: 1) Venemaa sõjaväega seotud teadus-uurimiskeskus pani 2022. aastal välja ühe miljoni rubla suuruse auhinna sellele, kes suudab neile toimetada Eesti kaitsetööstusettevõtte Milrem Robotics mehitamata maastikusõiduki THeMIS.[627] 2024. aastal suurendati auhinda kahele miljonile rublale.[628] 2) E. Kannike sõnul on vene keelt rääkivad isikud postitanud SensusQ-ga seotud isikute isikuandmeid suhtlusplatvormile Telegram.[629] Mõistagi hirmutamise eesmärgil. 3) RKKKo 1-21-1421 kohaselt huvitab Hiina sõjaväeluuret „küberteema ja kõrgtehnoloogia ülekanne“[630].

Kõrgtehnoloogia kui julgeolekuga seotud valdkonna kasuks räägib asjaolu, et kõrgtehnoloogia ebaseaduslik omandamine annab vastasele selge eelise. Üks on eelis, mida pakub omandatud tehnoloogia kasutamine enda julgeoleku või majanduse tugevdamisel. Teine on eelis, mis tuleneb sellest, et vastane ei pidanud läbima ressursimahukat katse-eksitus faasi, mis kaasneb kõrgtehnoloogia arendamisega. Riskiinvestor P. Thiel väidab, et kõrgtehnoloogia ettevõtete puhul pole edukas mitte pioneer ehk *first mover*, vaid see, kes õpib[631] teiste vigadest ning teeb alles siis oma käigu, ehk *last mover*. P. Thiel nimetab seda nähtust „viimase käija eeliseks“ (*last mover advantage*).[632]

[626] Lauri, V. Riik tellib Eesti kaitsetööstuselt 100 miljoni eest toodangut Ukrainale.
[627] ERR. Venemaa pani välja auhinna Milremi sõiduki kättesaamiseks Ukrainast. (05.09.2022). – https://www.err.ee/1608705520/venemaa-pani-valja-auhinna-milremi-soiduki-kattesaamiseks-ukrainast (03.04.2025).
[628] RIA Novosti. ЦАСТ удвоил награду за добытую в ходе СВО эстонскую боевую платформу. (14.02.2024). – https://ria.ru/20240214/spetsoperatsiya-1927303799.html (03.04.2025).
[629] Priit Pruksi intervjuu Erik Kannikega, 31.01.2025.
[630] RKKKo 1-21-1421, p 17 9).
[631] Või varastab kokku teiste parimad ideed.
[632] Thiel, P., Masters, B. Zero to One: Notes on Startups, or How to Build the Future. New York: Crown Business 2014, lk 44–59. Tsitaat: „[...], *so being the first mover doesn't do you any good if someone else comes along and unseats you. It's much better to be the last mover – that is, to make the last great development in a specific market and enjoy years or even decades of monopoly profits.*“

EKTL-i kuuluvate äriühingute tegevusvaldkondadest võiks kõrgtehnoloogia hulka kuuluda näiteks küberkaitselahendused, kaitseotstarbelised infotehnoloogia-, elektroonika-, juhtimis- ja sidesüsteemid, lasersüsteemid või robootika. [633]

## 4.5 Kaitsetööstuse ärisaladus

Järgnevalt esitan Eesti kaitsetööstuse esindajate seisukohad ärisaladuse sisu ja selle seose kohta Eesti Vabariigi julgeolekuga. Intervjueeritavate hulka kuulusid Cybernetica AS juhatuse liige ja nõukogu esimees Oliver Väärtnõu, CybExer Technologies OÜ nõukogu liige Lauri Almann, Defensphere OÜ juhatuse liige Ingvar Pärnamäe, EKTL-i juhatuse liige Kalev Koidumäe, osaühingust Defsecintel Solutions eriprojektide juht Viido Naruskberg ning ettevõtte julgeolekuekspert, Milrem AS süsteemide arhitekt Silver Lätt ning Sensus Septima OÜ strateegiajuht Erik Kannike.

Aktsiaseltsi Cybernetica võib pidada Eesti digiühiskonna alustalaks. Cybernetica on välja arendanud digiallkirja, X-Tee ja e-hääletamise. [634] Ettevõte esitleb enda julgeolekualast tegevust järgmiselt: „Aastakümnete pikkuse ekspertiisiga kaitsevaldkonnas on Cybernetica eesmärk pakkuda terviklahendust, mis hõlmab piirivalvet, merendus- ja küberalast olukorrateadlikkust.“[635] Küberturvalisuse valdkonnas teeb Cybernetica koostööd muuhulgas Euroopa Kosmoseagentuuri, Euroopa Kaitsefondi ja USA õhujõudude uurimislaboriga. [636] Koostöö Euroopa Kaitsefondiga hõlmab andmevahetustehnoloogiate arendust projektis *Secure Digital Military Mobility System*, mille raames arendatav IT-platvorm vähendab liikmesriikide sõjaväesüsteemide killustatust, kiirendab relvajõudude liikumist EL-liikmesriikide vahel ning panustab seeläbi Euroopa Liidu strateegilisse autonoomiasse. [637] Infoturbealases teadustöös torkavad silma Cybernetica krüptograafia-alaseid projektid USA kaitseministeeriumi arenduskeskuse DARPA-ga (*Defense Advanced Research Projects Agency*) ja USA mereväe teadusuuringute agentuuriga. [638] Ettevõte aitab Ukrainal arendada andmevahetusplatvormi Trembita.[639]

[633] Eesti Kaitse- ja Kosmosetööstuse Liit. Majandusaasta aruanne (2023).
[634] Cybernetica. Company. Our story. – https://cyber.ee/company/our-story (11.04.2025).
[635] Cybernetica. Industries. Defence. – https://cyber.ee/industries/defence (11.04.2025).
[636] Cybernetica AS. Majandusaasta aruanne (2023).
[637] Samas.
[638] Samas.
[639] Cybernetica. Cybernetica to Update Ukraine’s data Exchange platform Trembita. (25.03.2024). – https://cyber.ee/resources/news/trembita-2-0/ (11.04.2025),

Cybexer Technologies OÜ on „spetsialiseerunud küberharjutusväljade loomisele ning sellega seotud tehnoloogia arendamisele“ [640]. Tehnoloogia võimaldab „digitaalsete teisikute abil pakkuda erinevaid koolitus- ja testkeskkondi. See võimaldab organisatsioonidel parandada oluliselt oma valmisolekut küberohtudega tegelemiseks simuleeritud riskivabas keskkonnas“ [641]. Ettevõte pakub oma teenuseid muuhulgas NATO-le, Euroopa Kaitseagentuurile, Suurbritannia armeele ning teeb koostööd ka Eesti riigiasutustega. Ühtlasi panustab ettevõte Ukraina julgeoleku tagamisse.[642]

Defensphere arendab ja toodab 360-kraadi olukorrateadlikkussüsteeme, põhiliselt soomukitele ja mehitamata maismaasõidukitele.[643] Samuti arendatakse virtuaalseid juhtimiskeskuseid, mis toovad reaalse maailma virtuaalmaailma ning tõstavad meeskonnaliikmete olukorrateadlikkust. [644] Süsteem kannab nime Vegvisir ning seisneb silme ette käivas seadmes.[645]

Defsecintel Solutions OÜ arendab automatiseeritud seirelahendusi ning tooteid sisejulgeoleku ja kaitsevaldkonnas. [646] Ettevõtte tooteks on „treileri baasile ehitatud mobiilne torn koos droonijaamaga – SurveilSPRIE ehk *mobile autonomous surveillance platform* (MASP), ning 4x4 sõidukitele paigaldatav süsteem CAIMAN, mis sisaldab erinevaid sensorsüsteeme seire teostamiseks“[647]. DefSecIntel on seotud ka piirivalvega. „Algatasime [...] Balti Droonimüüri, mille raames pakume välja kontseptsiooni ühendamaks Eesti ja rahvusvaheliste partnerite uuenduslikud lahendused idapiiri kaitseks,“ kommenteerib Defsecinteli juhatuse liige Jaanus Tamm uut Balti Droonimüüri algatust.[648] Ettevõtte uus projekt on vee peal liikuv mehitamata platvorm, millega on võimalik muuhulgas turvata ja patrullida.[649] Defsecintel oli üks Eesti

[640] Cybexer Technologies OÜ. Majandusaasta aruanne (2023).
[641] Samas.
[642] Cybexer Technologies. – https://cybexer.com/ (04.03.2025); Estdev. Estonia launches cyber range training exercises in Ukraine under the Tallinn Mechanism framework. (11.12.2024). – https://estdev.ee/en/articles/estonia-launches-cyber-range-training-exercises-ukraine-under-tallinn-mechanism-framework (13.04.2025).
[643] Priit Pruksi intervjuu Ingvar Pärnamäega.
[644] Samas.
[645] Vegvisir. – https://www.vegvisir.ee/ (14.04.2025).
[646] DefSecIntel Solutions OÜ. Majandusaasta aruanne (2023).
[647] Samas.
[648] Eesti kaitsetöösturid pakkusid välja droonimüüri idee Euroopa Liidu idapiiri tugevdamiseks. – Postimees 27.02.2025.
[649] Karnau, A. DefSecInteli uus projekt on mehitamata valvepaat. – Postimees 28.02.2025.

kaitsetööstuse ettevõtetest, kelle tooteid ostis Eesti riik 100 miljoni euro suuruse Ukraina abipaketi raames.[650]

EKTL-i põhitegevuste loetelus kõige tähtsamal kohal on „liikmete huvide esindamine, kaitsmine ja uute võimaluste loomine suhetes kaitsetööstuse toodangu tarbijate, arendajate ja tootjatega nii Eestis kui rahvusvaheliselt“[651]. 2025. aasta aprilli seisuga kuulub liitu 173 äriühingut.[652]

Milrem AS on süsteemiintegraator, kes pakub „terviklikku robootika võimekust“[653], mis hõlmab näiteks „mehitamata ja mehitatud süsteemide koostööd, pealisehitiste integratsiooni mehitamata süsteemidele, liidestamist juhtimissüsteemidesse ning mehitatud sõidukite kaugelt juhitavaks muutmist“[654]. Ettevõtte enda väitel on Milrem „Euroopa juhtiv süsteemiintegraator robootika ja autonoomsete süsteemide osas armeedele [...]“[655]. Ettevõtte tuntuim toode on THeMIS UGV (*unmanned ground vehicle*), mis on kasutuses 17-s riigis, millest kaheksa on NATO liikmed.[656] 15 THeMIS-t on kasutusel Ukraina armees sõjas Venemaa vastu.[657]

Sensus Septima OÜ pakub luureinfo haldamise platvormi SensusQ, teeb koostööd NATO-ga ning tegutseb Ukrainas.[658] Ettevõte on oma toodet tutvustanud ka PPA-le.[659] Küsimusele, kas toodet saab kasutada ka vastuluures, vastab E. Kannike: „Meie toodet saab kasutada seal, kus

[650] Lauri, V. Riik tellib Eesti kaitsetööstuselt 100 miljoni eest toodangut Ukrainale. ERR 24.03.2025.
[651] Eesti Kaitse- ja Kosmosetööstuse Liit. Majandusaasta aruanne (2023).
[652] Priit Pruksi intervjuu Kalev Koidumäega, 01.04.2025.
[653] Milrem AS majandusaasta aruanne 2023.
[654] Samas.
[655] Samas.
[656] Samas.
[657] Samas.
[658] SensusQ. – https://www.sensusq.com/ (04.03.2025); SensusQ. Development programm for Ukrainian state instutions. (01.05.2024) – https://www.sensusq.com/blog/development-program-for-ukrainian-state-institutions (04.03.2025); Moody, O. Nato's crystal ball? The programm that claims to predict war. The Times 28.01.2025. – https://www.thetimes.com/world/europe/article/natos-crystal-ball-the-program-that-claims-to-predict-war-qx3c70v8g (04.03.2025); Eesti Kaitsevägi. NATO õppus CWIX oli kaitseväelastele edukas. (21.06.2024). – https://mil.ee/uudised/nato-oppus-cwix-oli-kaitsevaelastele-edukas/ (06.03.2025).
[659] LinkedIn. SensusQ. – https://www.linkedin.com/posts/sensusq_sensusq-estonia-police-activity-7257367591931760640-y9Z9 (06.03.2025).

klient seda soovib kasutada. Me oleme loonud piisavalt mitmekülgse ja [kliendi vajadustele kohaldatava] platvormi. [Meie tootega saab teha] mis iganes täisluuretsükli[660] tegevusi.“[661]

K. Koidumäe hinnangul on kaitsetööstuse äriühingu ärisaladuseks toote omadused ja lõppkasutajad.[662] Nii mõistab ärisaladuse sisu ka S. Lätt.[663] E. Kannike lisab juurde äriühingu sisemised praktikad ehk teabe äriühingu töökorralduse kohta.[664] O. Väärtnõu juhib tähelepanu toote hinnale ja müügipraktikatele.[665] Müügipraktikad on kaitsetööstuses üpriski keerulised, kinnitab E. Kannike ja lisab: „Kuidas sa lähened kliendile on juba omaette meeletu töö ja meeletu vaev. Selle kaitsmine on üpriski oluline.“[666]

K. Koidumäe järgi hõlmavad toote omadused eelkõige komponente, võimeid ning töötamise ja kasutamisega seonduvaid põhimõtteid.[667] Ühtlasi rõhutab ta toote elutsükli toetust puudutava teabe tähtsust.[668] Selle seisukohaga nõustub ka V. Naruskberg, kes selgitab, et lisaks toote ostjale on oluline kaitsta ka seda, milliseid teenuseid pakutakse pärast ostu.[669] Seda enam, et K. Koidumäe hinnangul võib kaitsetööstuse toote eluiga ulatuda aastakümnetesse.[670]

DefSecInteli julgeolekuekspert leiab, et ärisaladus hõlmab ka tarneahelat ehk teavet ettevõtte koostööpartnerite kohta. [671] O. Väärtnõu arvates on ärisaladusega kaitstud ka teave selle kohta, kes äriühingu töötajatest tegelevad äriühingu jaoks kriitiliste tehnoloogiate arendamisega.[672] Töötajate teemal märgib DefSecInteli julgeolekuekspert, et ärisaladusega on kaitstud teave,

[660] Erinevad riigid ja ühe riigi erinevad eriteenistused võivad kirjeldada luuretsüklit erinevalt. 18-st valitsusasutusest koosnev USA luurekogukond eristab kuut faasi: planeerimine (*planning*), kogumine (*collection*), töötlemine (*processing*), analüüs (*analysis*), levitamine (*dissemination*) ja hindamine (*evaluation*). Vt lähemalt: United States Intelligence Community. How the IC Works. The Six Steps in the Intelligence Cycle. – https://www.intelligence.gov/how-the-ic-works (13.04.2025). Kanada välisluure nimetab enne planeerimist esimese faasina *requirements and direction*, mis seisneb sisendi saamises valitsuselt luureinfo kogumise prioriteetide kohta. Eestis on luuretsükli alguspunktiks riigi julgeolekuteabe ja analüüsi kava (JAS § 9 lg 2), mis koostatakse Vabariigi Valitsuse, julgeolekuasutuste ja kaitseväeluure koostöös. Vt lähemalt: CSIS Public Report 2019. The Intelligence Cycle. – https://www.canada.ca/en/security-intelligence-service/corporate/publications/2019-public-report/the-intelligence-cycle.html (13.04.2025).
[661] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[662] Priit Pruksi intervjuu Kalev Koidumäega.
[663] Priit Pruksi intervjuu Silver Lättiga.
[664] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[665] Priit Pruksi intervjuu Oliver Väärtnõuga.
[666] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[667] Priit Pruksi intervjuu Kalev Koidumäega.
[668] Samas.
[669] Priit Pruksi intervjuu Viido Naruskbergi ja julgeolekueksperdiga.
[670] Kagge, R. jt.
[671] Priit Pruksi intervjuu Viido Naruskbergi ja julgeolekueksperdiga.
[672] Priit Pruksi intervjuu Oliver Väärtnõuga, 09.04.2025.

mis puudutab palkade kujunemist; kuid isikuandmete puhul võiks tegemist olla pigem andmekaitsemääruse kaitsealaga.[673]

Järelikult, intervjueeritavate hinnangul koosneb kaitsetööstuse ärisaladus neljast teabekategooriast: toote omadused, toote lõppkasutajad, koostööpartnerid ja praktikad. Toote omaduste alla kuuluvad vastused järgmistele küsimustele: 1) Kui palju toode maksab? 2) Mida tootega teha saab? 3) Kuidas toodet kasutada? 4) Millest toode koosneb? 5) Kuidas toodet hooldatakse? Ühesõnaga: hind, komponendid, võimed, töötamise ja kasutamisega seonduvad põhimõtted ning elutsükli toetust puudutav teave. Äriühingu koostööpartnerite all mõeldakse sisuliselt tarneahelat ehk suhete võrgustikku, mille abil toode valmib. Äriühingu praktikate puhul vajavad ärisaladuse kaitset vastused küsimustele: 1) Kuidas müüakse kliendile? 2) Milline näeb välja äriühingu töökorraldus? 3) Kes tegelevad äriühingu jaoks kriitiliste tehnoloogiate arendamisega? 4) Kuidas juhtorganite liikmeid ja töötajaid motiveeritakse ja tasustatakse? Lühidalt: müügipraktikad, töökorraldus, tööülesanded ja tasustamissüsteem.

Arvestades magistritöö piiratud mahtu ei ole võimalik analüüsida süvitsi, kas ettevõtjate arusaam ärisaladuse sisust kattub ärisaladuse määratlusega EKTÄKS § 5 lg-s 2. Teisisõnu, kas ülalmainitud neli teabekategooriat täidavad järgnevat kolme tingimust. Esiteks, teave „ei ole kogumis või üksikosade täpses paigutuses ja kokkupanus üldteada või kergesti kättesaadav nende ringkondade isikutele, kes tavaliselt kõnealust laadi teabega tegelevad“ (EKTÄKS § 5 lg 2 p 1). Teiseks, teabel on „kaubanduslik väärtus oma salajasuse tõttu“ (EKTÄKS § 5 lg 2 p 2). Kolmandaks, teabe „üle seaduslikku kontrolli omav isik on asjaoludest lähtuvalt võtnud vajalikke meetmeid, et hoida seda salajas“ (EKTÄKS § 5 lg 2 p 3). Riigikohtu tsiviilkolleegiumi kompaktsemas sõnastuses on ärisaladus teave, mis on „salajane või raskesti kättesaadav, millel on kaubanduslik väärtus ning mille salajases hoidmiseks kasutatakse vajalikke meetmeid“[674]. Lisaks suuremale töömahule eeldaks sügavam analüüs ka sisendit kaitsetööstuse äriühingute õigusnõustajatelt, mille kogumine ei olnud ajaliste piirangute tõttu võimalik.

Vähemalt esmapilgul ei riku ükski mainitud teabekategooriatest karjuvalt ühtegi kolmest tingimusest. Ehk siis esmapilgul pole põhjust väita, et mainitud teave võiks olla üldteada või

[673] Priit Pruksi intervjuu Viido Naruskbergi ja julgeolekueksperdiga.
[674] RKTKo 2-20-13897, p 12.

kergesti kättesaadav konkurentidele, st teistele kaitsetööstuse äriühingutele. Samuti pole põhjust arvata, et mainitud teabel puuduks kaubanduslik väärtus. Vastasel juhul ei oleks kaitsetööstuse äriühingute juhtivtöötajad, kes igapäevaselt ärisaladusega kokku puutuvad, neid kategooriaid üldse maininudki. Intervjueeritavad on juba enda töö- või juhatuse liikme lepingu tõttu teadlikud, millist liiki teavet nad on kohustatud kaitsma. Ja eelduslikult on kõnealuste teabekategooriate määratlemises osalenud ka õigusnõustajad.

Mõistagi on tegemist pinnapealse hinnanguga, mis sügavamal analüüsil võib osutuda ekslikuks. Näiteks võib vaielda, kas teave tasustamissüsteemi kohta on üldteada või kergesti kättesaadav. E. Kannike hinnangul võib äriühingu töökuulutuste ajaloo analüüsimisel teha tõsiseltvõetavaid järeldusi tasustamissüsteemi kohta.[675] Küsimus on muidugi, kas vajadus viia läbi taoline ajalooline andmeanalüüs tähendab, et teave on üldteada või kergesti kättesaadav. Vastuargumendina võib väita, et taolise analüüsi pinnalt saab teha üldisi järeldusi palgasüsteemi kohta, kuid mitte detailide kohta. Ja detailid võivadki olla just need, mis väärivad kaitsmist, kuivõrd võimaldavad äriühingul värvata talenti paremini kui konkurent. Ehk siis taolisel teabel on „kaubanduslik väärtus oma salajasuse tõttu“ (EKTÄKS § 5 lg 2 p 2).

Samuti tuleks arvestada, et äriühingu huvides on alati laiendada ärisaladuse mahtu ning piirata juhtorganite liikmete, töötajate ja teenusepakkujate võimalusi jagada avalikkusega äriühinguga seotud teavet. Sama põhimõtte kehtib riigiametites, kus ametnike esmane reaktsioon on tembeldada teave asutusesiseseks kasutamiseks. Nii leidis ajaleht Postimees ajakirjandusliku eksperimendi raames.[676] Erialakirjanduses ja ajakirjanduses kutsutakse seda nähtust „ülesalastamiseks“[677]. Seega pole välistatud, et intervjueeritavad serveerisid mulle äriühingu juhtkonna ja õigusnõustajate koostöös konstrueeritud mahukaid teabekategooriaid, mis ei pruugi võistlevas kohtumenetluses kehtima jääda.

---

[675] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.

[676] Oidsalu, M., Pulk, M. Postimehe eksperiment paljastas avaliku teabe jagamise „musta turu“. (04.01.2022). – https://arvamus.postimees.ee/7597438/voim-ja-julgeolek-meelis-oidsalu-meinhard-pulk-postimehe-eksperiment-paljastas-avaliku-teabe-jagamise-musta-turu (21.04.2025). Tsitaat: „Ametnike reaktsioonid ajakirjaniku päringutele andsid märku sellest, et pooltes ministeeriumites vohab ülesalastamise harjumus.“ Vt ka Andmekaitseinspektsiooni aastaraamat 2024. Avalik teave – kas piisavalt kättesaadav? Tsitaat: „Üha enam on tõstatunud küsimus, kas dokumentidele ei kehtestata mitte liiga kergekäeliselt piiranguid. Kontrollides asutuste dokumendiregistreid, võib sellega ka osaliselt nõustuda, kuigi dokumentide sisu teadmata siduvat hinnangut anda ei saa.“

[677] 11. septembri terrorirünnakute järel kerkis Washingtoni lähistele 67 terrorismi-vastase võitlusega tegelevat juhtimiskeskust, kusjuures paljud neist tegelesid samade ülesannetega. Ühtlasi hoogustus ülesalastamine. Vt lähemalt: Priest, D.; Arkin, W. M. A hidden world, growing beyond control. The Washington Post (July 19, 2010) – https://www.pulitzer.org/cms/sites/default/files/content/washpost_tsa_item1.pdf (03.01.2024); Priest, D., Arkin, W. M. Top Secret America: The Rise of the New American Security State. Little, Brown and Company 2011.

Kuid nagu öeldud, jääb see küsimus mõne teise teadustöö lahendada. Küll aga kommenteerin veidi pikemalt ärisaladuse kolmandat tingimust ehk meetmeid, mida äriühingud kasutavad enda ärisaladuse kaitsmiseks. K. Koidumäe väitel on ärisaladuse kaitsemeetmete nurgakiviks teadmisvajaduse põhimõte: teatud asju teavad ainult need, kes teadma peavad.[678] I. Pärnamäe kasutab sama mõtte väljendamiseks „lahterdamise" (*compartmentalization*) mõistet, mis tema sõnul seisneb selles, et ettevõttes töötavate isikute juurdepääsuprivileegid ei ole võrdsed.[679] Teisiti öeldult, ettevõtte huvides on teadlikult vältida olukorda, kus ühel isikul on liiga lai vaade arvutisüsteemides olevale teabele.[680] O. Väärtnõu väitel järgib Cybernetica rangelt mainitud põhimõtet ning teavet klassifitseeritakse vastavalt sellele, kas see kuulub jagamiseks äriühingu sees, koostööpartneritega või avalikkusega.[681] Koostööpartnerite puhul välditakse teatud riike ja nende riikide ettevõtteid, kahtluse korral küsitakse arvamust julgeolekuasutustelt ning koostöö korral sõlmitakse alati konfidentsiaalsuskokkulepe.[682] Samas möönab O. Väärtnõu, et eraõiguslikul kaitsel on omad piirid.[683] Näiteks pole tema hinnangul mõtet minna vaidlema võõrriigiga tema territooriumil asuvasse arbitraažikohtusse.[684] E. Kannike hinnangul aitavad kaitsetööstuse ettevõtjal ellu jääda lisaks eelmainitule: valvsus, küberhügieen, taustakontrolli oskused ning julgeolekualase taustaga meeskonnakaaslased.[685]

### 4.6 Kaitsetööstuse ärisaladuse seos Eesti Vabariigi julgeolekuga

K. Koidumäe sõnul võiks ärisaladus ja Eesti Vabariigi julgeolek olla omavahel seotud toote lõppkasutaja kaudu, kuivõrd teave lõppkasutaja kohta annab teavet ka riigi võimelünkade kohta. Teisisõnu: kui vastane teab, et kaitsevägi on teatud kaitsetööstuse äriühingu klient, annab see ühtlasi teavet, kus on kaitseväe nõrgad kohad. K. Koidumäe hinnangul on ärisaladuse seos Eesti Vabariigi julgeolekuga tugev, kui äriühingu pakutava toote lõppkasutajaks on Kaitsevägi. Arvesse tuleb muidugi võtta ka seda, et Balti riigid on üks sõjaline operatsiooniruum, mistõttu ei saa päris eitada seost Eesti Vabariigi julgeolekuga, kui kliendiks on teiste Balti riikide

[678] Priit Pruksi intervjuu Kalev Koidumäega.
[679] Priit Pruksi intervjuu Ingvar Pärnamäega.
[680] Edward Snowdeni näide illustreerib tabavalt, mis võib juhtuda, kui ühel isikul on liiga suured juurdepääsuprivileegid: Nimelt töötas Snowden USA signaalluureasutuses NSA (*National Security Agency*) süsteemiadministraatorina. Vt lähemalt: U.S. House of Representatives. (U) Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden. (15.09.2016). – https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_declassified.pdf (17.04.2025).
[681] Priit Pruksi intervjuu Oliver Väärtnõuga.
[682] Samas.
[683] Samas.
[684] Samas.
[685] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025, 31.01.2025.

kaitseväed. Sama argumenti saab laiendada ka teiste NATO liikmesriikide kaitsevägedele. Kuid juhul kui Eesti kaitsetööstuse äriühing pakub tooteid ainult mittevaenulikele kolmandatele riikidele (nt Austraalia) on juba keerulisem väita, et selle äriühingu ärisaladuse hankimisega ohustatakse Eesti Vabariigi julgeolekut.[686]

L. Almann nendib, et ärisaladuse avalikustamise mõju liitlassuhetele võiks olla üks komponent, mille kaudu hinnata ärisaladuse seost riigi julgeolekuga. Samas võib L. Almanni mõttekäigust välja lugeda seisukoha, et juriidiliste hinnangute andmisel tuleks eelistada konkreetsust ja kammitsetust, seda eriti karistusõiguses. Teisiti öeldult, L. Almann ei tundu pooldavat hüpoteetiliste ja kaudsete seoste loomist. [687]

V. Naruskberg möönab, et seos julgeolekuga võiks tekkida lõppkasutaja kaudu. Kui äriühingu klient on Eesti kaitsevägi, on ärisaladuse ja Eesti Vabariigi julgeoleku vahel side loodud. Seejuures võiks eriti kriitiline olla teave, mis puudutab toote elutsüklit: kas Eesti on võimeline toodet koha peal hooldama? kas selleks on olemas väljaõppe või varuosabaas? või on tarvis varuosasid tellida kuskilt kaugelt, nt Lõuna-Koreast? Veel võib julgeolekuga olla seotud teave kaitsetööstuse äriühingu teenusepakkujate kohta, nt telekommunikatsiooni ettevõtte pakutavate teenuste kohta kriisiolukorras. DefSecInteli julgeolekuekspert jätkab selle mõttelõngaga ja sõnab, et seos julgeolekuga võib tuleneda ka äriühingu tegevusvaldkonnast. Kui äriühing pakub elutähtsat teenust, võivad teenuse pakkumise tingimused kriisiolukorras olla seotud julgeolekuga. [688]

V. Naruskberg lisab, et sellise teabe puhul on tõenäoline, et ärisaladus on ühtlasi ka „templi all“ ehk riigisaladusega kaitstud. [689] See ei pruugi aga tõsi olla. Seda näiteks põhjusel, et 642 SE seletuskiri sisaldab näidisloetelu mittesalajasest teabest, mille alla kuulub ka teave elutähtsate teenuste toimepidavuse kohta. [690] Kui elutähtsate teenuste toimepidavus oleks alati riigisaladusega kaitstud, ei oleks mõtet mainida seda seoses KarS §-ga 234[2], mille kaitsealasse kuulub peamiselt mittesalajane teave. Tõsi on muidugi see, et „katkematu side korraldamine ja katkematule sidele kehtestatud nõudeid puudutav teave“ on sätestatud infrastruktuuri ja teabe kaitse riigisaladusena (RSVS § 10 p 8).

[686] Priit Pruksi intervjuu Kalev Koidumäega.
[687] Priit Pruksi intervjuu Lauri Almanniga.
[688] Priit Pruksi intervjuu Viido Naruskbergi ja julgeolekueksperdiga.
[689] Samas.
[690] 642 SE seletuskiri, lk 4.

E. Kannike nõustub, et kõige hõlpsamini saab luua seose Eesti Vabariigi julgeolekuga lõppkasutaja kaudu.[691] Seos julgeolekuga on tugev, kui klient on riigiasutus või kriitilise taristu ettevõte.[692] Samas tuleb arvestada, et väga paljud Eesti kaitsetööstuse äriühingud ei ole müünud oma tooteid Eesti riigile.[693] Seda kinnitab ka I. Pärnamäe, kelle hinnangul jääb kodumaine turg Eesti kaitsetööstuse jaoks „tagasihoidlikuks“[694]. Näiteks L. Almanni sõnul müüb CybExer Technologies Eesti riigile alla ühe protsendi oma käibest.[695] Ühesõnaga, Eesti kaitsetööstus on suuresti ekspordile orienteeritud tööstusharu, mistõttu võiks esimese hooga väita, et seos Eesti Vabariigi julgeolekuga jääb teoreetiliseks. Küll aga leiab E. Kannike, et kriisiolukorras läheksid Eesti kaitsetööstuse tooted käiku, mistõttu tuleks arvesse võtta ka Eesti kaitsetööstuse toodangu hüpoteetilisi kasutajaid.[696] Teisisõnu, kui Eesti riigiasutus võiks kriisiolukorras olla konkreetse äriühingu kliendiks, on selle äriühingu ärisaladusel seos Eesti Vabariigi julgeolekuga.

Veel märgib E. Kannike, et seos julgeolekuga võib seisneda ka toote lõppkasutuses. Näiteks, kui mingit tehnoloogiat kasutatakse õhu- või mereseires, võib teave tehniliste omaduste kohta osutuda sõjaliselt väärtuslikuks. Teisisõnu, kui vastasel peaks õnnestuma hankida sellist teavet, satuks ohtu Eesti Vabariigi julgeolek. E. Kannike lisab veel, et lahingutegevus Ukrainas võib anda vihjeid, milline ärisaladus on julgeolekualase kaaluga. Nimelt on ukrainlased hästi kaardistanud Venemaa sõjatööstuse ettevõtete tarneahelaid ning rünnanud tarnijate tehaseid.[697] Järelikult võiks julgeolekuga olla seotud ärisaladus, mille sisuks on teave äriühingu tarneahelate kohta.[698]

I. Pärnamäe sõnul võiks riigikaitseliste sundkoormiste koondkava[699] anda signaali, millised äriühingud on riigi julgeoleku jaoks olulised. Teisisõnu, milliste äriühingute tooteid ja teenuseid vajab riik sõjaolukorras. I. Pärnamäe mainib nelja kategooriat: 1) logistikaettevõtted; 2) ettevõtted, mis tegelevad sõjavarustuse hooldamisega olukorras, kus välismaalt midagi

[691] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[692] Samas.
[693] Samas.
[694] Kagge, R. jt.
[695] Priit Pruksi intervjuu Lauri Almanniga.
[696] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[697] The Kyiv Independent. Ukrainian drones hit Russian explosives, fiiber optic factories near Moscow. (05.04.2025). – https://kyivindependent.com/ukrainian-drones-hit-russian-fiber-optic-factory-east-of-moscow/ (13.04.2025).
[698] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[699] Vt lähemalt magistritöö alapeatükk 2.4.

tellida ei saa; 3) tootmisettevõtted, mida oleks võimalik ümber seadistada sõjalise otstarbega asjade (nt droonide) tootmisele; 4) ettevõtted ja teadusasutused, kus tegeletakse unikaalse arendustegevusega, mille vastu on globaalne huvi. Viimasesse kategooriasse võiks arvata näiteks krüptograafia valdkonna, kus Eestil on laialdased kogemused. Samuti võiks riigi julgeoleku jaoks olla olulised äriühingud, mille ärisaladus on seotud strateegilise kaubaga, kuivõrd strateegilise kauba mõistega ütleb riik selgelt: „Neid tehnoloogiaid tahame kontrollida.“ [700]

I. Pärnamäe sõnul kinnitab ka vastase huvi, et konkreetse äriühingu ärisaladus on oluline Eesti Vabariigi julgeolekule. RKKK otsuses 1-21-1421 käsitletud Hiina sõjaväeluure viide kübervaldkonnale ning avalik tasu, mida Venemaa lubas Milremi mehitamata maismaasõiduki eest, on kaks avalikku näidet vastaste eelistustest.[701] „Ma olen enam kui kindel, et see on jäämäe tipp,“ ütleb I. Pärnamäe. „Ametkondadel täna on Eestis kindlasti rohkem infot, mis selle jäämäe veealusest osast tegelikult huvipakkuv osa on.“[702] Mõistlikult võttes võiks jäämäe veealune osa olla kirjas riigi julgeolekuteabe hanke ja analüüsi kavas. Kuid kui vastab tõele, et ametnike huvi Eesti kaitsetööstuse vastu võrreldes poliitikute huviga on leige – nagu väidab I. Pärnamäe – ei pruugi see eeldus paika pidada.[703] Sel juhul võiks vastase sihtmärkide analüüs ja süntees anda ühelt poolt olulise enesekindluse kodumaisele tööstusele, et tegeletakse olulise asjaga, ja teiselt poolt juhise riigile, milliste ettevõtete kaitsmisega tuleks tegeleda. „Mõnikord lihtsalt on nii, et kui sa ise ei saa aru enda väärtusest, siis vaata, kuidas sind teised vaatavad ja kus teised näevad sinu väärtust,“ ütleb I. Pärnamäe.[704]

## 4.7 Vahekokkuvõte

KarS § 234[2] lg 1 objektiivne koosseis eeldab Eesti Vabariigi julgeoleku vastast tegevust, mille toimepanijaks on, kas välisriigi luure- või julgeolekuteenistuse teenistuja või selle huvides või ülesandel tegutsev isik. Sama säte näeb ette Eesti Vabariigi julgeoleku vastaste tegevuste näidisloetelu, mis sisaldab muuhulgas teabe kogumist. Riigikohtu kriminaalkolleegium

[700] Priit Pruksi intervjuu Ingvar Pärnamäega.
[701] RKKKo 1-21-1421, p 17 9); ERR. Venemaa pani välja auhinna Milremi sõiduki kättesaamiseks Ukrainast; RIA Novosti.
[702] Samas.
[703] Riigi julgeolekuteabe hanke ja analüüsi kava töötatakse välja täitevvõimu poliitikute, julgeolekuasutuste ja kaitseväeluure koostöös (JAS § 9 lg 2). Kuid arvestades, et vastuluure puhul on tegemist valdkonnaga, millega enamus inimesi – sh poliitikuid – igapäevaselt kokku ei puutu ning ei oska seetõttu ka erinevate väidete paikapidavust hinnata, on julgeolekuametnike mõju selle dokumendi sisule märkimisväärne.
[704] Priit Pruksi intervjuu Ingvar Pärnamäega.

selgitab otsuse 1-21-1421 p-s 127, et näidisloetelus sisalduvad tegevused on eelduslikult suunatud Eesti Vabariigi julgeoleku vastu ning vastupidist peab tõendama süüdistatav. Tuginedes seaduse seletuskirjale selgitab kohus, et mittesalajaste valdkondade kohta teabe kogumine on Eesti Vabariigi julgeoleku vastu suunatud tegevuse „tüüpnäide“[705]. Kolleegium ei peatu pikemalt küsimusel, „kas üldse ja kui, siis milline julgeolekualane tähtsus oli eraldivõetult sellel konkreetsel teabel, mille G. Mutso ise või T. Kõuts G. Mutso mahitusel“ Hiina sõjaväeluurele üle andis. [706] Seega, eelduslikult ei oma kogutud teabe sisu KarS § 234[2] kohaldamisel tähtsust. Oluline on vaid tuvastada, kas isik on välisriigi luure- või julgeolekuteenistuse teenistuja või selle huvides või ülesandel tegutsev isik, ning kas see isik kogub mistahes sisuga teavet – salastatud või mittesalajast teavet. Seega sisaldab teave KarS § 234[2] lg 1 mõttes eelduslikult ka ärisaladust, sh kaitsetööstuse äriühingu ärisaladust.

Järelikult, eelduslikult peab paika magistritöö teine hüpotees: kaitsetööstuse äriühingu ärisaladus on teave KarS § 234[2] tähenduses.

Järgnevalt uurisin, millistel tingimustel ei ole eeldust võimalik ümber lükata. Teisisõnu, millistel juhtudel on välistatud, et süüdistatav võiks väita, et kaitsetööstuse äriühingust ärisaladuse kogumine välisriigi luure- või julgeolekuteenistuste huvides või ülesandel ei ohusta Eesti Vabariigi julgeolekut. Selleks määratlesime Eesti Vabariigi julgeoleku mõiste ning lõime seose Eesti kaitsetööstuse ja Eesti Vabariigi julgeoleku vahel.

Eesti Vabariigi julgeoleku mõiste avamisel tuginesime A. Sinisalu käsitlusele, mis lähtub katusmõistena turvalisusest ning keskendub täidesaatva riigivõimu asutuste pädevustele. A. Sinisalu järgi jaotub turvalisus kolmeks: julgeolek, avalik kord ja muu ühiskondlik turvalisus. Julgeoleku tagamise eest vastutavad enda pädevuste ulatuses valdavalt Kaitseministeerium, Kaitsevägi, Välisluureamet ja Kaitsepolitseiamet. Avaliku korra tagamise eest vastutab Politsei- ja Piirivalveamet. Muu ühiskondlik turvalisus kuulub Päästeameti, Sotsiaalministeeriumi, Haridusministeeriumi, kohtusüsteemi jt. pädevusse.[707]

A. Sinisalu käsitluses on julgeolek tervik, mis koosneb kahest komponendist: rahvusvaheline julgeolek ja riigi julgeolek ehk sisejulgeolek. Rahvusvahelisel julgeolekul on omakorda kaks

[705] RKKKo 1-21-1421, p 128.
[706] Samas, p 130.
[707] Joonis 1.

olulist elementi: eelhoiatus ja sõjaline tegevus. Eelhoiatuse eest vastutavad Välisluureamet ja Kaitseväe luurekeskus; sõjaline tegevus kuulub Kaitseväe pädevusse. Riigi julgeolek kitsas tähenduses moodustub ülesannetest, mis kuuluvad kõik KAPO pädevusse: 1) põhiseadusliku korra kaitse; 2) riigisaladuse kaitse ja selleks vastuluure korraldamine; 3) võitlus riigi julgeolekut ohustava korruptsiooniga; 4) võitlus terrorismiga, eelkõige selle ennetamine ja tõkestamine.[708]

Tegemist on käsitlusega, mille puuduseks võib pidada formalismi ja täitevvõimu-keskset maailmapilti, kuid käesoleva töö vajadusi silmas pidades on see igati kasulik teekaart.

Eesti Vabariigi julgeoleku ja kaitsetööstuse vahelise seose võib välja lugeda Eesti julgeolekupoliitika alustest, kus räägitakse heidutuse puhul „iseseisva kaitsevõime“ [709] tähtsusest. Samuti NATO hinnangutest, mis näevad artiklis 5 sisalduva heidutus- ja kaitsevõime hädavajaliku eeldusena „tehnoloogilise eelise säilitamist“ [710] ning EL-i kaitsetööstuse strateegiast, mis rõhutab, et kaitsevalmiduse saavutamiseks on „tingimata vaja tugevat EL-i kaitsetööstust“[711]. Aga ka 22. juulil 2024 sõlmitud koalitsioonileppest, mille kohaselt on „kohalik kaitsetööstus [...] osa meie laiapindsest riigikaitsevõimest“[712].

Leidsin, et seos kaitsetööstuse ja Eesti Vabariigi julgeoleku vahel võiks olla tugev järgmistes valdkondades: 1) otsene sõjaline tegevus; 2) eelhoiatus; 3) vastuluure; 4) küberkaitse ja küberturvalisus; 5) piirivalve. Veel leidsin, et konkreetse kaitsetööstuse äriühingu ja Eesti Vabariigi julgeoleku vahelise seose tõendamisel saab tugineda järgmistele asjaoludele, mille võiks jaotada sarnaselt strateegilise kauba kriteeriumitega[713] nelja kategooriasse:

1) Lõppkasutajaga seotud asjaolud, nt toodete või teenuste pakkumine Eesti Vabariigi julgeoleku tagamisega seotud valitsusasutusele, NATO või Euroopa Liidu liikmesriigile või Ukrainale.

[708] Samas; Sinisalu, A., Maiberg, H.
[709] Eesti julgeolekupoliitika alused, lk 7.
[710] NATO. Deterrence and defence, 13.12.2024.
– https://www.nato.int/cps/iw/natohq/topics_133127.htm#maintain (14.01.2025).
[711] Euroopa Komisjon. Ühisteatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele. Uus Euroopa kaitsetööstuse strateegia: EL-i valmisoleku saavutamine reageerimisvõimelise ja keskse Euroopa kaitsetööstuse abil. Brüssel 05.03.2024, lk 1.
[712] Vabariigi Valitsus. Koalitsioonilepe 2024–2027. – https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2024-2027 (14.11.2024).
[713] StrKS § 2 lg 11.

2) Lõppkasutusega seotud asjaolud, nt toote või teenuse arendamine Eesti Vabariigi julgeoleku jaoks olulistes valdkondades nagu seda on otsene sõjaline tegevus, eelhoiatus, vastuluure, küberkaitse ja küberturvalisus, mereseire ja piirivalve.
3) Muud julgeolekualased kaalutlused, nt Eesti Vabariigi vastaste huvi konkreetse äriühingu või teenuse vastu. Näideteks tõin Venemaa huvi SensusQ[714] ja Milremi[715] toodete vastu ning Hiina sõjaväeluure huvi kübervaldkonna[716] vastu.
4) Toote või teenuse omadustega seotud asjaolud, nt kõrgtehnoloogilise toote või teenuse pakkumine.

Uurimaks, mil määral nõustuvad ettevõtjad ülaltoodud teoreetiliste seisukohtadega, intervjueerisin äriühinguid, kes pakuvad tooteid, mida saab kasutada julgeolekualaselt olulistes valdkondades nagu otsene sõjaline tegevus, eelhoiatus, vastuluure, küberkaitse ja -turvalisus ning piirivalve.

Intervjueeritavate seisukohtadest ilmneb, et kaitsetööstuse ärisaladus koosneb neljast teabekategooriast: toote omadused, toote lõppkasutajad[717], koostööpartnerid ja praktikad. Toote omaduste alla kuuluvad vastused järgmistele küsimustele: 1) Kui palju toode maksab? 2) Mida tootega teha saab? 3) Kuidas toodet kasutada? 4) Millest toode koosneb? 5) Kuidas toodet hooldatakse? Ühesõnaga: hind[718], komponendid[719], võimed[720], töötamise ja kasutamisega seonduvad põhimõtted[721] ning elutsükli toetust puudutav teave[722]. Äriühingu koostööpartnerite all mõeldakse sisuliselt tarneahelat[723] ehk suhete võrgustikku, mille abil toode valmib. Praktikate puhul vajavad ärisaladuse kaitset vastused küsimustele: 1) Kuidas müüakse kliendile? 2) Milline näeb välja äriühingu töökorraldus? 2) Kes tegelevad äriühingu jaoks kriitiliste tehnoloogiate arendamisega? 4) Kuidas juhtorganite liikmeid ja töötajaid motiveeritakse ja tasustatakse? Lühidalt: müügipraktikad[724], töökorraldus[725], tööülesanded[726],

[714] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[715] ERR. Venemaa pani välja auhinna Milremi sõiduki kättesaamiseks Ukrainast; RIA Novosti.
[716] RKKKo 1-21-1421, p 17 9)
[717] Priit Pruksi intervjuu Kalev Koidumäega.
[718] Priit Pruksi intervjuu Oliver Väärtnõuga.
[719] Priit Pruksi intervjuu Kalev Koidumäega.
[720] Samas.
[721] Samas.
[722] Samas; Priit Pruksi intervjuu Viido Naruskbergi ja julgeolekueksperdiga.
[723] Priit Pruksi intervjuu Viido Naruskbergi ja julgeolekueksperdiga.
[724] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025; Priit Pruksi intervjuu Oliver Väärtnõuga.
[725] Samas.
[726] Samas.

tasustamissüsteem[727]. Käsitlesin põgusalt ka ülalmainitud teabe vastavust EKTÄKS § 5 lõikes 2 sätestatud kriteeriumitele, sh meetmeid, mida äriühingu rakendavad ärisaladuse kaitseks.

Ärisaladuse seost julgeolekuga toetavad intervjueeritavate hinnangul peamiselt kaks asjaolu: toote lõppkasutaja ning valdkond, kus toodet kasutatakse.

K. Koidumäe ja V. Naruskberg leiavad, et kui toote lõppkasutajal on selge riiklik seos – näiteks hangib toodet Kaitsevägi – on seos julgeolekuga loodud.[728] Samas juhivad I. Pärnamäe ja E. Kannike tähelepanu asjaolule, et Eesti riik ei hangi hetkel eriti Eesti kaitsetööstuse toodangut.[729] Seetõttu võiks väita, et Eesti kaitsetööstuse seos Eesti Vabariigi julgeolekuga on teoreetiline. Samas möönab E. Kannike, et kriisi- ja sõjaolukorras on tõenäoline, et kodumaise kaitsetööstuse tooted võetakse kasutusele.[730] Järelikult võiks jaatada ärisaladuse seost Eesti Vabariigi julgeolekuga, kui äriühingu tooteid on võimalik kasutada kriisi- või sõjaolukorras.

Veel tuleks arvestada, et julgeolekupoliitika aluste järgi on Eesti Vabariigi ja tema liitlaste julgeolek jagamatu.[731] K. Koidumäe sõnul moodustavad Balti riigid ühe operatsiooniruumi, mistõttu võiks ärisaladuse seos Eesti Vabariigi julgeolekuga tulla kõne alla ka olukorras, kus äriühingu klient on Balti riikide või NATO liikmesriikide kaitseväed.[732] Kuigi Ukraina ei ole NATO liikmesriik, annab Eesti Vabariigi julgeolek ja Ukraina julgeolek ühise eksistentsiaalse vastase kaudu seotud, mistõttu võib äritegevust Ukrainaga lugeda asjaoluks, mis räägib julgeolekualase seose kasuks. Seda enam, et Eesti koguabi suurus Ukrainale on seni 1,2 miljardit eurot.[733]

Rääkides tegevusvaldkondadest tõid V. Naruskberg ja julgeolekuekspert esile kriitilise taristu, nt telekommunikatsiooni.[734] E. Kannike mainis õhu- ja mereseiret.[735] Ükski intervjueeritavatest ei seadnud otseselt kahtluse alla teiste tegevusvaldkondade – eelhoiatus,

[727] Priit Pruksi intervjuu Viido Naruskbergi ja julgeolekueksperdiga, 10.04.2025.
[728] Samas; Priit Pruksi intervjuu Kalev Koidumäega, 01.04.2025.
[729] Kagge, R. jt; Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[730] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[731] Eesti julgeolekupoliitika alused, lk 2.
[732] Priit Pruksi intervjuu Kalev Koidumäega, 01.04.2025.
[733] Välisministeerium. Eesti toetus Ukrainale. (10.01.2024). – https://www.vm.ee/uudised/eesti-toetus-ukrainale (04.03.2025).
[734] Priit Pruksi intervjuu Viido Naruskbergi ja julgeolekueksperdiga, 10.04.2025.
[735] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.

vastuluure, otsene sõjaline tegevus, küberkaitse ja küberturvalisus – seost Eesti Vabariigi julgeolekuga.

I. Pärnamäe sõnul võiks strateegilise kauba nimekirjad ja riigikaitseliste sundkoormiste koondkava anda signaali, millised tegevusvaldkonnad ja äriühingud on riigi julgeoleku jaoks olulised.[736]

Järelikult, magistritöö teine hüpotees on leidnud kinnitust. RKKK otsuse 1-21-1421 järgi on kaitsetööstuse äriühingu ärisaladus eelduslikult teave KarS § $234^2$ lg 1 mõttes. Tuginedes magistritöös esitatud teoreetilisele raamistikule ja kaitsetööstuse ettevõtjate sisendile saab väita, et eelduse ümberlükkamine on ebatõenäoline, kui toote lõppkasutaja või valdkond, kus toodet kasutatakse, on tugevalt seotud Eesti Vabariigi julgeolekuga.

[736] Priit Pruksi intervjuu Ingvar Pärnamäega, 15.04.2025.

# Kokkuvõte

Magistritöös lükkasin ümber esimese hüpoteesi leides, et tööstusspionaaž on Eesti õiguskorras karistatav. Kinnitust leidis aga teine hüpotees: kaitsetööstuse äriühingu ärisaladus on eelduslikult teave KarS § $234^2$ tähenduses. Detailide osas suunan lugeja tähelepanu vahekokkuvõtetele vastavalt kolmanda ja neljanda peatüki lõpus. Järgnevalt käsitlen mõningaid ettepanekuid, mis vajaksid edasist arutelu.

Kaitsmaks riiklikult olulisi tehnoloogiavaldkondi Hiina eest täiendas Taiwani parlament riigi julgeoleku seaduse (*National Security Act*) tööstusspionaaži koosseisu „riikliku võtmetehnoloogia" (*national core key technology*) mõistega. [737] Mõiste alla kuuluvad tehnoloogiad, mille „väljavool välisriiki, Mandri-Hiinasse, Hongkongi, Macaosse või vaenulike võõrjõudude kätte põhjustaks tõsist kahju riigi julgeolekule, tööstuslikule konkurentsivõimele või majandusarengule"[738] ning mis täidavad ühe järgmistest tingimustest:

a) nende kontrolli nõuab rahvusvaheline leping, riigikaitse vajadused või riigi võtmetaristu kaitse;[739]
b) „need võivad aidata meie riigil luua juhtivaid tehnoloogiaid või oluliselt edendada tähtsate tööstusharude konkurentsivõimet"[740].

Ettepaneku konkreetse tehnoloogia paigutamiseks riikliku võtmetehnoloogia nimistusse teeb riiklik teadus- ja tehnoloogianõukogu, mis konsulteerib selleks pädevate asutustega, sh ekspertidega.[741]

Kuigi seadusandja tahe KarS § $234^2$ kehtestamisega oli luua võimalikult paindlik koosseis kaitsmaks Eesti Vabariigi julgeolekut ka mittesalajastes valdkondades, võiks õigusselguse põhimõttele tuginedes küsida, kas ka Eesti karistusõigusesse võiks tuua „riikliku võtmetehnoloogia" mõiste?

[737] National Security Act. Executive Yuan. (08.06.2022).
[738] Samas, art 3 lg 4.
[739] Samas, p 1.
[740] Samas, p 2.
[741] Mao, L., Yu, D., Tien, D.

Esimene variant oleks lisada „riikliku võtmetehnoloogia“ mõiste KarS § 234[2] loetelusse ehk siis täpsustada, et riiklikku võtmetehnoloogiat sisaldava ärisaladuse kogumine on Eesti Vabariigi vastane tegevus.

Teine variant oleks luua Eesti Vabariigi vastaste süütegude jakku erikoosseis, mis kriminaliseeriks riiklikku võtmetehnoloogiat sisaldava äriseaduse ebaseadusliku saamise, kasutamise või avaldamise. Arvestades, et tööstusspionaaži näol on tegemist ühelt poolt äriühinguga seotud süüteoga ja teiselt poolt riigivastase süüteoga võiks sanktsioonirežiim väljendada mõlemaid aspekte. Sarnaselt KarS §-iga 377 võiks karistuseks olla, kas rahaline karistus või vangistus, kuid erinevalt KarS §-s 377 sätestatud kuni kaheaastasest vangistusest võiks vangistuse pikkus olla sarnane KarS §-iga 234[2] ehk siis kaks- kuni viisteist aastat.

Nõnda oleks karistusseadustiku riigivastaste süütegude jaos neli erinevat spionaaži ründeobjekti: 1) salastatud teave ehk riigisaladus ja salastatud välisteave; 2) asutusesiseseks kasutuseks mõeldud teave; 3) riiklikku võtmetehnoloogiat sisaldav ärisaladus; 4) muu mittesalajane teave.

Esiteks annaks „riikliku võtmetehnoloogia“ mõiste julgeolekualase väärtusega ärisaladusele eristaatuse ning kinnitaks kaitsetööstuse äriühingutele, kes ei soovi töödelda salastatud teavet, et õiguskord kaitseb nende äritegevust kui mitte võrdväärselt ettevõtetega, kes töötlevad salastatud teavet, siis rohkem kui tavalisi äriühinguid. Teiseks annaks „riikliku võtmetehnoloogia“ mõiste võimaluse luua tööstusspionaaži heidutamiseks kvalifitseerivaid koosseise. Näiteks võiks arvutisüsteemile ebaseadusliku juurdepääsu hankimise korral olla arvutisüsteem, mis sisaldab riikliku võtmetehnoloogiaga seotud ärisaladust, kaitstud võrdväärselt elutähtsa valdkonna arvutisüsteemiga (KarS § 217 lg 2 p 3) või arvutisüsteemiga, mis sisaldab salastatud teavet või ainult ametialaseks kasutamiseks ettenähtud andmeid (KarS § 217 lg 2 p 2). Veel saaks täiendada KarS § 266 lg-t 2 nähes ette raskema sanktsiooni, kui tungitakse omavoliliselt sisse riikliku võtmetehnoloogia arendamisega tegeleva äriühingu maa-alale, hoonesse, või ruumi. Nii panustaks riik karistusõigusliku heidutuse abil kaitsetööstuse äriühingute valduse kaitsesse. Riikliku võtmetehnoloogia nimekirja koostamine saaks toimuda täitevvõimu juhtimisel strateegilise kauba komisjoni laadses kollektiivorganis, millel oleks õigus kaasata ka eksperte.

Riikliku võtmetehnoloogia mõiste sätestamise kahjuks räägivad samuti mitmed kaalukad argumendid. Esiteks, kas Eestil on üldse hetkel tehnoloogiaid, mida võib pidada võtmetehnoloogiaks? K. Koidumäe leiab, et võtmetehnoloogia oleks tiibrakett [742] või küberrelv.[743] Viimane oleks aga juba eos riigisaladusega kaitstud, kuna selle väljaarendamisega tegeleks Kaitseväe küberväejuhatus. O. Väärtnõu sõnul peaks riiklik võtmetehnoloogia olema, kas riigi ja erasektori koostöös välja arendatud või esialgselt väljaarendatud äriühingu poolt, kuid siis muutunud mingil põhjusel riigi jaoks eriti oluliseks.[744] Praegusel hetkel ei oska O. Väärtnõu nimetada Eestis riiklikku võtmetähtsusega tehnoloogiat, kuid see võib ajas muutuda.[745] Teiseks, vahetegu ärisaladuse ja riigisaladuse vahel on põhimõtteline: üks kuulub eraõigusesse, teine haldusõigusesse. Sellele juhib tähelepanu ka O. Väärtnõu: „Mina hoiaks riigisaladuse ja ärisaladuse lahus. Ärisaladuse kaitse organiseerin mina ja riigisaladuse kaitse organiseerib riik.“[746] Kui tekitada ärisaladuse ja riigisaladuse vahele mingisugune vahevorm nimega „riikliku võtmetehnoloogiaga seotud ärisaladus“, ei oleks enam selge, kes selle kaitsega peaks tegelema ning millised eeldused peaksid olema täidetud selle kaitse saamisele. Ei saa tekkida olukorda, kus julgeolekuasutus peab kaitsma äriühingu ärisaladust, kuid samas ei oleks äriühingul kohustust kehtestada rangeid turvameetmeid või alluda julgeolekukontrollile. Teisisõnu, ei saa olla õigusi ilma kohustusteta. Sellele viitab ka KAPO, kui kirjutab, et ametkondadel tuleks üle hinnata õiguskord, et „ettevõtetel oleks selge ülevaade oma õigustest, kohustustest ja vastutusest“. [747] Mõistagi ei ole ettevõtjad huvitatud rangematest turvameetmetest või kohustusest alluda julgeolekukontrollile, sest sel juhul oleks protsess identne riigisaladuse töötlemise loa taotlemisega. Ühtlasi tähendab uute mõistete lisandumine õiguskorda, et süsteem läheb keerulisemaks, mis muudab ettevõtjaid arusaadavalt ärevaks. Kolmandaks, ärisaladuse kaitsmine riigi ja kaitsetööstuse äriühingute koostöös tähendaks, et riik ja kaitsetööstuse ettevõtted suudavad teha koostööd. I. Pärnamäe hinnangul vähemalt hetkel riigi ja kodumaise kaitsetööstuse partnerlus ei toimi.[748] Neljandaks, kuigi märksõna „võtme“ võiks mõjuda distsiplineerivalt, võib ka võtmetehnoloogiate nimekiri muutuda strateegilise kaubaga sarnaseks pikaks, abstraktseks nimistuks. Mistõttu tekiks karistusõigusliku vastutuse korral küsimus kooskõlast määratletusnõudega. Viimaks,

[742] Eestis on tehtud paar aastat ettevalmistusi tiibrakettide tootmiseks: Lauri, V. Asjatundjad: Eesti võiks koostöös lähiriikidega toota tiibrakette. ERR (26.04.2025). – https://www.err.ee/1609676501/asjatundjad-eesti-voiks-koostoos-lahiriikidega-toota-tiibrakette (26.04.2025).
[743] Priit Pruksi intervjuu Kalev Koidumäega.
[744] Priit Pruksi intervjuu Oliver Väärtnõuga.
[745] Samas.
[746] Samas.
[747] KAPO aastaraamat 2024-2025, lk 34.
[748] Priit Pruksi intervjuu Ingvar Pärnamäega.

õigusselguse taotluse vastu räägib soov säilitada strateegilist ebamäärasust riiklikult oluliste tehnoloogiavaldkondade osas. Lihtsalt väljendades: miks anda vastasele teekaart, kus asuvad kroonijuveelid?[749]

Lõpetuseks mõni sõna magistritöö pealkirjas kõlava laiema missiooni kohta. Nimelt, kuidas saab Eesti õigusteadus kaitsta Eesti kaitsetööstust tööstusspionaaži eest? I. Pärnamäe sõnul tuleb esmalt ära otsustada, kas Eesti kaitsetööstust on üldse kaitsmist väärt.[750] Sest kui Eesti riik leiab, et kodumaine kaitsetööstus ei toeta julgeolekut, ei ole ka mõtet rääkida juriidilistest sammudest. Aga oletame, et vastab tõele koalitsioonileppes sisalduv põhimõte, et „kohalik kaitsetööstus on osa meie laiapindsest riigikaitsevõimest"[751]. Mida on õigusteadusel siis öelda?

Esiteks muidugi seda, mida ma juba ütlesin: karistusseadustiku koosseisud tööstusspioonide vastutusele võtmiseks on olemas. Riigikohtu tõlgendus teabe mõistele KarS § $234^2$ lg-s 1 omakorda lihtsustab KAPO tööd (RKKK 1-21-1421, p 127 ja 128). Õiguslünka ei ole.

Teine küsimus on, kas julgeolekuga seotud ärisaladust peaks kaitsma kuidagi karmimalt. Üks võimalus on muidugi ärisaladus riigisalastada. RSVS § 7 p $6^1$ sellise võimaluse annab, juhul kui tegemist on „sõjalise otstarbega asjaga". Probleem on pigem selles, et parem on toimetada maailmas, kus salastatud teabega kokku ei puutu. Seda kinnitasid kõik intervjueeritavad. Teine võimalus on kohustada julgeolekuasutusi ulatuslikumalt sekkuma kaitsetööstuse äriühingute ärisaladuse kaitsesse. Õiguslik alus selleks on olemas, kuivõrd KAPO kohustus on ennetada ja tõkestada riigi vastu suunatud luuretegevust ning Välisluureameti ülesanne on korraldada ja kontrollida elektroonilist teabeturvet (JAS § 6 p 2, § 7 p 4). Sel juhul tuleks aga tõlgendada sõnasid „riik" ja „elektrooniline teabeturve" nii, et sinna alla kuuluksid ka äriühingud, kes ei töötle riigisaladust. See aga eeldaks „kaitsetööstuse" või „võtmetehnoloogiate" mõistete määratlemist, et piirata isikute ja esemete ringi, keda ja mida julgeolekuasutused on kohustatud kaitsma. Iseasi on muidugi, kas kõik kaitsetööstuse äriühingud üldse soovivad sellist kaitset. Või kas KAPO-l kui Siseministeeriumi asutusel on taoliseks tegevuseks üldse vahendeid. E. Kannike väitel oleks kaitsetööstus huvitatud suuremast riigipoolsest abist taustakontrollide tegemisel või füüsilise perimeetri kaitsel, aga ta mõistab, et riik on väike ja kõigeks ressurssi

[749] Tõenäoliselt muudeti riigikaitseliste sundkoormiste koondkava põhjusega „haldusesiseseks planeerimisdokumendiks". Vt: 417 SE seletuskiri, lk 30.
[750] Priit Pruksi intervjuu Ingvar Pärnamäega.
[751] Vabariigi Valitsus. Koalitsioonilepe 2024–2027. – https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2024-2027 (14.11.2024).

ei jätku.[752] Märkusena: JAS § 32 lg $3^1$ alusel võib edastada „teisele isikule“ julgeolekuasutuse ülesannete täitmisel saadud teavet, kui see on vajalik julgeolekuasutuse ülesannete täitmiseks. Samuti võib julgeolekuasutus edastada riigi osalusega äriühingule julgeolekuasutuse ülesannete täitmisel saadud teavet, „kui see on vajalik selle ülesannete täitmiseks ning kui see ei kahjusta julgeolekuasutuse ülesannete täitmist“ (JAS § 32 lg 3). Mainitud sätete alusel oleks julgeolekuasutusel võimalik jagada kaitsetööstuse äriühinguga või riigi osalusega kaitsetööstuse äriühinguga teabehankega saadud teavet, et paremini kaitsta kõnealuseid ühinguid tööstusspionaaži eest. Kolmas võimalus on piirata avalikku teavet. Kõik ettevõtjad leidsid, et kaaluda võiks piiranguid äriregistris kättesaadavale teabele, juhul kui äriühing tegutseb riigi jaoks olulises sektoris. V. Naruskberg märgib, et kaaluda võiks ka juurdepääsu piiramist tegevuslubasid puudutavale teabele.[753] Samas tuleb aduda, et kui kõik riigid läheksid avaliku info piiramise teed, halveneks ka Eesti ettevõtjate võimalused teha taustakontrolle koostööpartneritele. Samuti tuleb silmas pidada ülesalastamise ohtu.

Viimasena võiks arutleda, mida teha olukorras, kus äriühingud sooviksid rohkem kaitset, aga riigil ei ole võimalik seda anda? Näiteks, kui kaitsetööstuse äriühing otsustab tööle võtta vastuluurejuhi – mis on Ameerika Ühendriikides[754] üpriski tavaline – siis, millised on sellise isiku võimalused korraldada äriühingu vastuluuret? Täpsemalt, milliseid meetmeid saab ta kasutada riskide tuvastamiseks ja nende maandamiseks? Sisuliselt on see küsimus õigusselgusest eraviisilise jälitustegevuse koosseisu (KarS § 137) ja andmekaitsemääruse kaitseala kohta. Usun, et ekspertide huvi taha see tõenäoliselt ei jääks. Vähemasti kaitsetööstuse kogemus on näidanud, et endistel kaitseväelastel on märkimisväärne huvi siirduda pärast teenistuse lõppu eraettevõtlusesse. Kas selline võimalus tuleks anda ka endistele julgeolekuasutuste ametnikele? See on kahtlemata õiguslik küsimus.

Mõistagi oleks parem, kui juba koolitatud ja kogemusega ametnikke oleks võimalik hoida riigiametis. See aga nõuab ühiskondlikku arusaama, et „julgeoleku tagamiseks ei piisa sõjaks valmistumisest“[755]. Nagu kirjutab K. Pärt: „Sarnaselt sõjalise kaitsevõimega on vajalik tagada mittesõjaliste julgeolekuvõimete püsirahastus ja stabiilne areng.“[756]

[752] Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
[753] Priit Pruksi intervjuu Viido Naruskbergi ja julgeolekueksperdiga.
[754] Hiljuti otsis vastuluure juhti (*director of counterintelligence*) USA kaitsetööstusettevõte Anduril: https://www.anduril.com/open-roles/?location=&department=&search=&gh_src= (27.04.2025).
[755] Pärt, K.
[756] Samas.

## *In Defense of the Defense Industry: Countermeasures against Industrial Espionage*

A new Cold War is upon us. Victory will depend on military might and economic growth. The defense industry delivers both. A major risk for the industry are foreign governments. The threat is most acute for high-tech firms operating close to countries with a history of intellectual property theft. If this logic holds, Taiwan leads the list – and Estonia trails close behind. In light of Estonia's light economic footprint, its success in the global defense market hinges on a strategic emphasis on innovation. It does not make sense to make things that others make better and cheaper, argues Ingvar Pärnamäe, CEO of the defence company Vegvisir and former Vice Chancellor of Defence Investments at the Estonian Ministry of Defence (MoD).[757] "Our cyber defence industry did not appear out of thin air, but as a reaction to the Bronze Night[758] in 2007. We turned our experience into value on a global scale," he adds.[759]

However, Estonia's proximity to Russia raises the risk that its innovations could be plundered. The move to restrict AI chip exports to Estonia suggests the United States quietly acknowledged the nation's precarious position.[760] Tanel Tammet, a professor at the Tallinn University of Technology, reflects on the factors that may have influenced the decision of the Biden administration. "If you allow countries like Estonia, Hungary, and Greece to buy [these chips], there's a chance that they might be secretly transferred to China," he notes.[761] However, espionage threats are not limited to hostile states. Kalev Koidumäe, the CEO of Estonia's Defense and Aerospace Industry Association, argues that the fragmented nature of the European defense market encourages competition between major defense contractors, which may escalate into espionage.[762] Given the close ties between such companies and their national governments, it can be difficult to ascertain whether the ultimate beneficiary is a foreign state or a foreign firm – a distinction that further complicates regulatory and security responses.

[757] Priit Pruks's interview with Ingvar Pärnamäe.
[758] Juurvee, I., Mattiisen, A.-M. The Bronze Soldier Crisis of 2007. Revisiting an Early Case of Hybrid Conflict. ICDS (21.08.2020). – https://icds.ee/en/the-bronze-soldier-crisis-of-2007/ (20.04.2025)
[759] *Ibid.*
[760] Department of Commerce. Bureau of Industry and Security. Framework for Artifical Intelligence Diffusion.
[761] Tammet, T.
[762] Priit Pruks's interview with Kalev Koidumäe.

The Estonian defense industry's troubles are compounded by an ongoing rift with its national government. "A meaningful partnership has yet to emerge," says I. Pärnamäe.[763] According to him, while politicians increasingly recognize the potential role of domestic defense companies in national security, civil servants remain hesitant.[764] The cause of this reluctance is unclear, but the surge in investment has clearly caught the bureaucracy off guard. The Chancellor of the MoD admits that the oversight of defense investments is weak and the security department is understaffed.[765] The Estonian Internal Security Service (ISS) concedes that the public authorities lack experience in industrial security matters.[766] While many countries, including the United States, have national industrial security programs, Estonia has neither such a program nor a plan to develop one. The ISS has also pointed to the regulatory ambiguity in this area, suggesting that existing legal provisions are insufficiently clear.[767] What is more, the recent surge of funding has placed the defense sector under scrutiny from the ISS's anti-corruption department.[768] Whether Estonia's underfunded Ministry of the Interior can simultaneously address industrial security policy, corruption risks, and combat the constant threat of Russian hybrid attacks remains an open question.[769]

From an academic perspective, the phenomenon of industrial espionage in Estonia has not been subject to serious study since 2004.[770] Despite its growing relevance, both the ISS and the Foreign Intelligence Service (FIS) have produced only limited commentary amounting to brief references in annual reports.[771] In this light, the present thesis seeks to make a meaningful contribution to an underexplored yet critically important field.

When it comes to the protection of intellectual property, private law mechanisms are only effective to the extent that the infringer is motivated to participate in litigation. That is not how spies operate. Indeed, even burdensome administrative law measures collectively known as "non-military means of prevention"[772] – such as surveillance, background investigations, deportations, or entry bans – often prove insufficient to deter espionage activities. To deter and

[763] Priit Pruks's interview with Ingvar Pärnamäe.
[764] *Ibid.*
[765] Hindre, M. Kuusk kaitseministeeriumist: sisekontrolli pole ja julgeolek on alamehitatud.
[766] KAPO annual report 2024–2025, p 34.
[767] KAPO annual report 2024–2025, p 34. 32 CFR part 117.
[768] Kaitsepolitseiameti aastaraamatu esitlus 2025.
[769] Vabariigi Valitsus. 2025. aasta riigieelarve ja 2025–2028 riigi eelarvestrateegia. Peamised sõnumid valitsemisalade kaupa. KaM ja SiM; Pärt, K.
[770] Koort, E.
[771] *E.g.* Välisluure aastaraamat 2024, p 87 jj.
[772] Security Authorities Law § 2 lg 1.

punish those who willingly act on behalf of foreign powers, it is often necessary to resort to the nuclear option of the legal system: criminal law.

According to the ISS – an agency noted for imprisoning Russian agents – criminal liability for espionage in the West is no longer "a hypothetical possibility, but rather an expected reality."[773] In a time of war, the time for half-measures is over. „I shed no tears for those voluntarily willing to co-operate with the Russian special services," declares Arnold Sinisalu, the former director general of the ISS.[774] And in the aftermath of Russia's invasion of Ukraine and the horrors of Bucha, this sentiment is widely shared in Estonia.

Industrial espionage is espionage. For this reason, jurisdictions such as the United States and the United Kingdom have enacted legislation specifically criminalizing it.[775] By contrast, the Estonian Penal Code does not explicitly mention economic or industrial espionage. To be fair, the absence of such provisions is not uncommon, as studies by S. Carl and others illustrate.[776] Accordingly, this thesis initially advances the hypothesis that industrial espionage is not criminalized under Estonian law. To assess the validity of that claim, it is first necessary to clarify the concept of industrial espionage – beginning with a distinction between intelligence collection and espionage, and between industrial, economic, and corporate espionage.

As noted by M. Lowenthal, while "all intelligence is information; not all information is intelligence."[777] Intelligence is defined by its utility to decision-makers. A. Zegart echoes this view: "Intelligence is information that gives policymakers an advantage over their adversaries."[778] Intelligence collection, therefore, is the gathering of information relevant to decision-making.[779] But this need for actionable intelligence is not unique to state actors. Non-state actors – including corporations[780], terrorist groups[781], drug cartels[782], and biker gangs[783]

[773] Klemm, J. (koost). KAPO aastaraamat 2022–2023, p 20.
[774] 38. Eesti õigusteadlaste päevade paneel „Jälitus ja teabehange kriminaalmenetluses" (26.09.2024), 11:46–11:51.
[775] Economic Espionage Act of 1996; National Security Act 2023, Section 2.
[776] Carl, S., Kilchling, M., Knickmeier, S., and Wallwaey, E.
[777] Lowenthal, M. Chapter One: What is Intelligence?
[778] Zegart, A., p 79.
[779] Decision can be made at the strategic, operational or tactical level. See: Eesti Kaitsevägi. Luurekeskus. Luure tasandid.
[780] SCIP. Code of Ethics; Madureira, L. et al. Competitive intelligence: A unified view and modular definition.
[781] European Council on Foreign Relations. Mapping Palestinian Politics. Security Forces. Internal Security Force (ISF) – Hamas.
[782] Schilis-Gallego, C., Lakhani, N. 'It's a free-for-all': how hi-tech spyware ends up in the hands of Mexico's cartels.
[783] Mobley, B. W., Wege, C. A., p 690; Rambo, R., Holder, D. UnIntelligence. The Corporate Counterintelligence Podcast. Episode 13 with Matthew Hedger.

– are equally motivated by the value of information. Put simply, in competitive environments, having an edge over a rival can mean the difference between death and survival.

Not all intelligence collection constitutes espionage. As N. Polmar and T. Allen explain, espionage is defined as "intelligence activity aimed at gathering information through secretive means."[784] H. Tiido, citing J. Rislakki, makes the same point: "intelligence collection, broadly construed, can be legal, while espionage is inherently illicit and involves covert means, including agents and technical surveillance".[785] In short, espionage is a subset of intelligence, characterized by the use of unlawful or clandestine methods.

In seeking to define industrial espionage, this thesis draws on the institutional knowledge of the FBI and ISS, which are both counterintelligence agencies with investigative authority.[786] In the United States, the Economic Espionage Act of 1996 (EEA) distinguishes between two offences:

- Economic espionage (18 U.S.C. § 1831), where the misappropriation of trade secrets benefits a foreign government; and
- Theft of trade secrets (18 U.S.C. § 1832), where no foreign government involvement is present.

By contrast, Estonian law contains no statutory definitions for economic, industrial, or corporate espionage. The ISS offers an informal typology[787] based on two criteria:

- The identity of the perpetrator: foreign governments conduct industrial or economic espionage, while private actors engage in corporate espionage.
- The nature of the target: economic espionage is said to target strategic state information; industrial espionage is thought to target property rights (technology, information).

The perpetrator-based distinction finds some support in the Estonian Penal Code. It could be argued that § 377 of the Penal Code, concerning the unlawful acquisition of trade secrets, aligns best with the concept of corporate espionage. Regarding economic or industrial espionage –

[784] Polmar, N., Allen, T.
[785] Risklakki, J.
[786] FBI. FAQ. What is the FBI's foreign counterintelligence responsibility?; FBI. FAQ. Where is the FBI's authority written down?; JAS § 6 p 2; Heldna, E.
[787] Kaitsepolitseiamet. Mida peaks teadma tööstusspionaažist? (03.11.2019). – https://web.archive.org/web/20191103141731/https:/www.kapo.ee/et/content/mida-peaks-teadma-t%c3%b6%c3%b6stusspionaa%c5%beist.html (08.02.2025).

defined here as espionage carried out by foreign governments – the Penal Code contains several provisions that may apply. If the target is classified information, the offence may fall under § 232 (treason) or § 234 (espionage), depending on the nationality of the offender. If the information is classified for internal use, § 243 or § 234² may apply. [788] If the information is unclassified, § 234² remains applicable. Under certain circumstances, the acquisition of unclassified public information – if it poses a threat to the independence and sovereignty, or the territorial integrity of the Republic of Estonia – may warrant the application of § 232 or § 233. [789]

However, distinguishing between economic and industrial espionage within the framework of the Penal Code proves challenging. Strategic state-related information may fall under several classifications: state secrets, classified information of foreign states (e.g., NATO or EU classified information), information classified as internal information, or unclassified information. Consequently, a range of provisions – §§ 232, 233, 234, 234², or 243 – may be applicable. At the same time, industrial espionage – defined here as involving the targeting of technology or intellectual property – could also fall under §§ 232, 233, 234, or 234². This overlap highlights that Estonian law does not provide a legal distinction between economic and industrial espionage based solely on the type of information targeted. The only clear legal boundary lies in differentiating between acts committed by state actors and those carried out by private individuals. The remaining question, then, is whether espionage conducted by foreign governments should be called economic espionage, following the terminology of the U.S. Code, or whether the term industrial espionage is more appropriate.

M. Button and S. Knickmeier differentiate between economic and industrial espionage based on the identity of the beneficiary. According to their view, when a foreign state stands to benefit, the act constitutes economic espionage; when the beneficiary is a private entity, it is classified as industrial espionage. Importantly, the nature of the targeted material – confidential information or trade secrets – remains the same in both cases. [790] Within this framework, German law distinguishes between the two through StGB § 99 (economic espionage) and GeschGehG § 23 (industrial espionage). Notably, StGB § 99 served as the legislative model

[788] § 243: Communication of internal information. § 234[2]: Intelligence activities against the Republic of Estonia and support of.
[789] § 233: Non-violent acts committed by alien against the Republic of Estonia
[790] Button, M.; Knickmeier, S.

for § 234² of the Penal Code.[791] Meanwhile, both § 377 and GeschGehG § 23 implement the EU trade secrets directive.[792]

Nevertheless, given the linguistic conventions and institutional practice in Estonia, where both the ISS and FIS associate industrial espionage with state-sponsored activity, and given that the parliament has used the term "industrial espionage" in draft legislation concerning industrial security policy, it is more appropriate in the Estonian legal context to distinguish industrial and corporate espionage, rather than economic and industrial espionage.[793]

Accordingly, this thesis proposes the following definition: Industrial espionage is the acquisition of classified information, trade secrets, or confidential information for the benefit of a foreign state.

It is worth noting that while industrial espionage targets classified information of economic value – such as proprietary technologies – Estonian criminal law does not differentiate classified information by its domain.[794] Whether the content is economic, political, or military, it is subject to the same legal treatment. Under the Penal Code, classified is classified.

Thus, the first hypothesis is rebutted. Industrial espionage is a criminal offence under Estonian law, and depending on the circumstances, the applicable provisions are Penal Code §§ 232, 233, 234, or 234².

Drawing on an analysis of seven Chinese espionage cases in the United States, this thesis also examines how prosecutors have approached the prosecution of industrial espionage offences.[795] In the United States, successful prosecution under the Economic Espionage Act (18 U.S. Code § 1831) requires proof that the conduct served the interests of a foreign government. Where such a link cannot be established, prosecutors typically rely on a range of "backstop"[796] offences, including:

- Theft of trade secrets (18 U.S. Code § 1832);

[791] 642 SE seletuskiri, p 6.
[792] WIPO; 678 SE seletuskiri, pp 12–13.
[793] Eesti rahvusvahelises julgeolekukeskkonnas 2024, p 87; Riigisaladuse ja salastatud välisteabe seaduse, riigihangete seaduse ning riigilõivuseaduse muutmise seaduse (tööstusjulgeolek) eelnõu seletuskiri.
[794] Administrative law does: see State Secrets and Classified Information of Foreign States Act §§ 6-10.
[795] *United States* vs. *Mo Hailong*; *United States* vs. *Haitao Xiang*; *United States* vs. *Xiaoqing Zheng*; *United States vs. Su Bin*; *United States v. Li Xiaoyu, Dong Jiazhi*; *United States* vs. *Yanjun Xu*.
[796] Hvistendahl, M., p 152.

- Computer fraud and abuse (18 U.S. Code § 1030);
- Wire fraud (18 U.S. Code § 1343);
- Illegal export of strategic goods (22 U.S. Code § 2778, 22 CFR 120–130).

A widely used tool in espionage-related cases is the charge of conspiracy against the United States (18 U.S. Code §§ 371, 1349), which enables liability for preparatory acts and facilitates attribution[797] of conduct committed by co-conspirators, such as cyber intrusions by intelligence or military officers in China, to U.S.-based operatives who provide them with targeting information.

Although the specific offence of conspiracy against the Republic of Estonia no longer exists by name, its substance remains within Penal Code § $235^1$.[798] Thus, Estonian law also permits punishment for the conspiracy to commit industrial espionage. In addition to the principal offender, the law also permits the punishment of the joint principal offenders (§ 21(2)), abettors (§ 22(2)), and aiders (§ 22(3)). Where the underlying offence carries a maximum penalty of at least twelve years' imprisonment, individuals may also be prosecuted for the attempt of instigation to criminal offence (§ $22^1$(1)), provided that some overt act has occurred to move the offence beyond mere thought (§ $22^1$(2)). According to J. Sootak, the requirement of an overt act ensures that criminal liability cannot arise from intentions alone.[799]

In cases where proving the existence of a relationship with a foreign government proves too onerous, Estonian law allows for prosecution under a range of offences closely tied to industrial espionage, including:

- Illegal acquisition, use, or disclosure of a business secret[800] (§ 377),
- Illegal obtaining of access to computer systems (§ 217),
- Preparation of computer-related crime (§ $216^1$),
- Illegal carriage of strategic goods (§§ $421^1$, $421^2$),
- Violation of international sanctions and sanctions of Government of the Republic (§ $93^1$),
- Unauthorised surveillance (§ 137).

[797] *Pinkerton v. United States*.
[798] § $235^1$: relationship antagonistic to Republic of Estonia.
[799] Sootak, J. KarS komm § 221, p 2.3.
[800] The term the English translation of the Penal Code uses for a trade secret.

The existence of a variety of "backstop" offences ensures that Estonian prosecutors have the tools to respond to industrial espionage, even in the absence of evidence directly linking the conduct to a foreign government.

The second hypothesis is based on the premise that, in cases involving the collection of classified information, the applicable legal provisions are clearly defined. When the perpetrator is an Estonian citizen, the act constitutes treason under § 232 of the Penal Code. If carried out by a foreign national, it is categorized as espionage under § 234. However, when the object of the offence is a trade secret, identifying the applicable legal provision is not straightforward. The choice is between Penal Code § 377, which concerns the unlawful acquisition of trade secrets, and § $234^2$, which pertains to intelligence activities against the Republic of Estonia and support thereof – an offence against the security of the Republic of Estonia.

The only authoritative sources for determining whether trade secrets fall within the scope of Penal Code § $234^2$(1) are as follows:

1. The explanatory memorandum to the bill (in Estonian: *eelnõu seletuskiri*) 642 SE;
2. The judgment of the Criminal Chamber of the Supreme Court in case No. 1-21-1421; and
3. § 99 of the German Criminal Code, which served as a model during the legislative drafting of Penal Code § $234^2$.

According to the explanatory memorandum of 642 SE, the notion of "information" within the meaning of § $234^2$ of the Penal Code encompasses "public information, information classified as internal information, state secrets, and classified information of foreign states."[801] The memorandum clarifies that the provision aims to criminalize situations where "a foreign intelligence or security service, or a person acting in its interests or on its behalf, collects information regarding unclassified domains."[802]

The explanatory memorandum relies on cases described in the annual reports of the ISS, which demonstrate that "foreign intelligence interests may also lie in influencing Estonia's domestic decisions or conditions and in the collection of unclassified or information classified as internal information, or even public information (e.g., databases of credit institutions, employment

[801] 642 SE seletuskiri, p 6.
[802] *Ibid*, p 4.

registry data, personal information, private and professional email correspondence, social networks, location of specific facilities, movement of military convoys, resilience of vital services, etc.)."[803]

From the explanatory memorandum, it is evident that the concept of "information" is intended to cover as broad a range of subject matter as possible. The sole substantive criterion is that the collection of the information must amount to "activity against the security of the Republic of Estonia." As further noted, this concept cannot be exhaustively defined. It is a fluid and evolving notion, shaped by the nature of security threats and the state's security policy at any given time.[804]

Based on the foregoing, I formulate the second hypothesis of this thesis as follows: The trade secrets of a defense industry company constitute "information" within the meaning of Penal Code § 234²(1).

The hypothesis may be challenged on three grounds. First, trade secrets are not explicitly mentioned in the illustrative list provided in the explanatory memorandum to the bill that the courts use to discover evidence about legislative intent. Second, the examples of unclassified information cited in the memorandum reveal a state-centric approach to the notion of "information." This is evident from the classification of information as "public information", "information classified as internal information", "state secrets", or "classified information of foreign states" – all of which are legal terms derived from acts belonging to administrative law, specifically the Public Information Act and the State Secrets and Classified Information of Foreign States Act.[805] Third, Penal Code § 234² is situated in the chapter of the Penal Code addressing offences against the state, specifically in the section concerning acts against the Republic of Estonia. According to R. Kiris and M. Kärner, the protected legal interest under § 234² is the security of the Republic of Estonia.[806]

The purpose of § 234² is therefore to safeguard the state, and more precisely, the security of the Republic of Estonia. This raises the fundamental question: Why should a trade secret – an asset belonging to a private company – fall within the scope of this criminal provision? After all, a company, as a private legal person, operates primarily in pursuit of private interests (see

[803] *Ibid.* Also see: counterintelligence chapters in ISS's annual reports for 2013 and 2014.
[804] *Ibid.*
[805] 642 SE seletuskiri, p 6.
[806] Kiris, R., Kärner, M., komm § 234², p 1

Act on the General Part of the Civil Code § 25(1) and Commercial Code § 2(1)). Furthermore, one of the defining features of a trade secret is the fact that "it has commercial value due to its secrecy" (see Restriction of Unfair Competition and Protection of Business Secrets Act § 5(2)(2)). It is therefore legitimate to ask why a provision designed to protect the security of the Republic of Estonia should extend its protection to the commercial value of assets owned by a private company.

It is notable that the explanatory memorandum to Bill 642 SE references "banking databases," "professional emails," and "the continuity of vital services." [807] This implies legislative acknowledgment that private-sector entities may, in fact, hold information of strategic interest to foreign actors – thus justifying state protection. This interpretation gains particular traction in relation to the defense industry, where public and private interests are deeply intertwined. Defense companies, after all, cater exclusively to sovereign states. [808] As observed by G. Allen and D. Berenson, the United States Defense Industrial Base (DIB) operates largely in isolation from the broader economy, given that its only client is the state. [809] Furthermore, in many jurisdictions – though not in Estonia[810] – defense firms are often state-owned. [811]

While the use of open-ended legal concepts such as "security of the Republic of Estonia" and "information" does not, according to the case law of the Supreme Court[812], violate the principle of legal certainty, it remains essential – in the interest of legal clarity and the rule of law more broadly – that academic inquiry into the precise meaning of such terms persists, even in sensitive areas such as national security.

As § 234² falls under the section of the Penal Code dedicated to crimes against the state, any extension of its scope to cover trade secrets must be grounded in a clear connection between the specific trade secret and the security of the Republic of Estonia. Put simply, § 234² should protect only that information whose acquisition by a foreign power would pose a credible threat to the security of the Republic of Estonia.

[807] 642 SE seletuskiri, p 4.
[808] Nicastro, L.A. The U.S. Defense Industrial Base: Background and Issues for Congress. Congressional Research Service, p 6; Carril, R., Duggan, M.
[809] Allen, G.; Berenson, D.
[810] Recently, the government granted the Minister of Finance the authority to establish a company that will produce military-grade explosives. See: ERR. Riik asutab põlevkivist lõhkeaine tootmiseks ettevõtte Hexest.
[811] Priit Pruks's interview with Kalev Koidumäe.
[812] RKKKo 1-22-3155, p 40; RKKKo 1-16-10888/62, p 48.

To confirm or refute the hypothesis, one must first clearly define what constitutes a trade secret under Estonian law and within the defense sector. Only then can a meaningful assessment be made as to whether these trade secrets intersect with the security interests of the Republic of Estonia.

The objective elements of Penal Code § 234²(1) require that an act be directed against the security of the Republic of Estonia, and that it be committed either by a member of a foreign intelligence or security service, or by a person acting in the interests of, or pursuant to the instructions of, such a service. The same provision contains a non-exhaustive list of activities presumed to threaten the security of the Republic of Estonia, among which the collection of information is expressly included.

In Judgment No. 1-21-1421, paragraph 127, the Criminal Chamber of the Supreme Court clarified that the listed activities are presumptively considered acts directed against the security of the Republic of Estonia. Accordingly, the burden shifts to the defendant to rebut this presumption. [813] Drawing on the explanatory memorandum to Bill 642 SE, the Court underscored that the collection of unclassified information constitutes a "typical example"[814] of conduct that may be contrary to the security security of the Republic of Estonia. Importantly, however, the Chamber did not assess the national security value of the specific information transmitted by G. Mutso – or by T. Kõuts at her direction – to China's military intelligence. [815] As a result, the judgment suggests that, in principle, the substantive content of the information collected is immaterial to the application of § 234².

The key consideration is whether the actor is affiliated with, or acting on behalf of, a foreign intelligence or security service, and whether they have gathered any form of information. Since trade secrets are undeniably informational in character, they presumptively fall within the expansive interpretation of "information" envisaged by § 234²(1).

It follows that the second hypothesis of this master's thesis is in principle confirmed: The trade secrets of a defense industry company constitute "information" within the meaning of Penal Code § 234²(1).

[813] RKKKo, p 128.
[814] *Ibid.*
[815] *Ibid.*, p 130.

The analysis next focused on circumstances where the presumption is not open to challenge – that is, where a defendant cannot plausibly claim that gathering trade secrets from a defence company on behalf of a foreign intelligence or security service does not threaten the security of the Republic of Estonia. Accordingly, the concept of security was defined, and a link was established between the Estonian defense industry and the security of the Republic of Estonia.

In defining the concept of security, this thesis adopts the interpretation advanced by A. Sinisalu, who conceptualizes public safety (in Estonian: *turvalisus*) as an overarching framework comprising various executive branch responsibilities. According to Sinisalu, public safety encompasses three core domains: security, public order, and other public safety-related concerns. The primary responsibility for security rests with the Ministry of Defence, the Estonian Defence Forces, the FIS, and the ISS. Public order, in turn, falls under the jurisdiction of the Police and Border Guard Board. Broader societal safety matters – including civil protection, health, education, and justice – are managed by institutions such as the Rescue Board, the Ministry of Social Affairs, the Ministry of Education, the judiciary, and others.[816]

Sinisalu classifies security into two primary categories: international security and state security (or internal security). International security includes two main functions: early warning and military action. The FIS and the Intelligence Center of the Defence Forces (in Estonian: *Kaitseväe luurekeskus*) are tasked with the former, while the Defence Forces bear responsibility for the latter, including the use of lethal force in armed conflict. State security, in the narrow sense, comprises the tasks assigned exclusively to the ISS: 1) the protection of the the constitutional order; 2) the protection of state secrets and the conduct of counterintelligence operations; 3) the prevention and combating of corruption endangering state security; 4) the prevention and combating of terrorism.[817]

Though formal and institutional, this framework serves as the foundation for analysis in this thesis.

The link between Estonia's defense industry and the security of the Republic of Estonia is implicitly recognized in Estonia's security policy, which prioritizes the maintenance of "independent defense capabilities" as a core component of deterrence.[818] Similarly, NATO

[816] Figure 1.
[817] *Ibid.* Sinisalu, A., Maiberg, H.
[818] Eesti julgeolekupoliitika alused, p 7.

doctrine emphasizes technological superiority as fundamental to deterrence and the effective implementation of Article 5.[819] The EU Defence Industrial Strategy echoes this position, underscoring the strategic necessity of a European defense industry.[820] Moreover, the coalition agreement of 22 July 2024 affirms that "the local defense industry is part of Estonia's comprehensive national defense."[821]

I argue that the link between the defense industry and the security of the Republic of Estonia is particularly strong in the following domains:

1. The use of lethal force in armed conflict;
2. Early warning systems;
3. Counterintelligence activities;
4. Cyber defense and cybersecurity; and
5. Border surveillance.

To assess when a specific defense company can be demonstrably linked to the security of the Republic of Estonia, this thesis introduces an analytical framework structured around four categories. This framework is modelled on the evaluative criteria employed by the Strategic Goods Commission in determining whether a particular good possesses the characteristics of a strategic item warranting export control.[822]

1. End-user factors: For instance, whether the company supplies the Estonian government, a NATO/EU member state, or Ukraine.
2. End-use factors: Whether the product or service supports key functions like military operations, early warning, or cyber defense.
3. Other security indicators: For example, interest from hostile states (e.g., Russia's interest in SensusQ[823] and Milrem[824], or China's interest[825] in Estonia's cyber technologies).

[819] NATO. Deterrence and defence, 13.12.2024.
[820] Euroopa Komisjon. Ühisteatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele.
[821] Vabariigi Valitsus. Koalitsioonilepe 2024–2027. Uued investeeringud ja ettevõtete kindlustunne. Eesti kaitsetööstuse arendamine.
[822] StrKS § 2 lg 11.
[823] Priit Pruks's interview with Erik Kannike, 31.01.2025.
[824] RIA Novosti.
[825] RKKKo 1-21-1421, p 17 9)

4. Product characteristics: Including high-tech or dual-use features.

To assess how these conceptual frameworks align with practical realities, I conducted interviews with defense companies operating in security-sensitive areas. The interviewees identified four key categories of trade secrets:

- Product characteristics (e.g., cost[826], capabilities[827], components[828], principles of use[829], and maintenance[830]);
- End users;[831]
- Partners (e.g., supply chain);[832]
- Business practices (e.g., sales strategy[833], internal policies[834], staff roles[835], and compensation models[836]);

I then briefly assessed whether the information in question satisfies the requirements set out in § 5(2) of the Restriction of Unfair Competition and Protection of Business Secrets Act. Additionally, I examined various confidentiality measures employed by companies, such as „compartmentalization“[837].

The interviewees generally confirmed that the link between trade secrets and security arises from two primary factors:

1. The identity of the end user (e.g., the Estonian Defence Forces), and
2. The company’s field of activity.

K. Koidumäe and V. Naruskberg argued that when the end user has a clear affiliation with the Estonian government, the security relevance is self-evident. [838] In contrast, I. Pärnamäe and E. Kannike observed that the Estonian government's procurement from domestic defense firms

[826] Priit Pruks’s interview with Oliver Väärtnõu.
[827] Priit Pruks’s interview with Kalev Koidumäe.
[828] *Ibid.*
[829] *Ibid.*
[830] *Ibid.*
[831] *Ibid.*
[832] Priit Pruks’s interviews with Viido Naruskberg and a security expert.
[833] Priit Pruks’s interviews with Oliver Väärtnõu and Erik Kannike, 10.04.2025.
[834] *Ibid.*
[835] *Ibid.*
[836] Priit Pruks’s interviews with Viido Naruskberg and a security expert.
[837] Priit Pruks’s interview with Ingvar Pärnamäe.
[838] Priit Pruks’s interviews with Kalev Koidumäe, Viido Naruskberg, and a security expert.

remains limited.[839] For example, L. Almann notes that only about 1% of CybExer Technologies' revenue comes from the Estonian government, highlighting the export-oriented nature of the Estonian defense industry and supporting I. Pärnamäe's assertion that the government is hesitant to procure from domestic companies.[840] However, E. Kannike acknowledged that in times of war or crisis, reliance on domestic production would likely increase – thereby underscoring the need to protect the trade secrets of domestic defense companies should such circumstances arise.[841]

It is also essential to consider Estonia's security doctrine, which links its security with that of its allies.[842] K. Koidumäe notes that the Baltic states form a single operational theater, and that a company supplying NATO or regional defense forces likely serves Estonia's security interests.[843] Although Ukraine is not a NATO member state, its security is existentially tied to Estonia's due to their shared threat from Russia, making business relationships with Ukraine particularly relevant – especially in light of Estonia's €1.2 billion in total aid.[844]

With respect to strategic domains, V. Naruskberg and DefSecIntel's security expert cited the telecommunications infrastructure, and E. Kannike referenced air and maritime surveillance.[845] None of the interviewees questioned the security relevance of sectors such as early warning, cyber defense, or direct military operations. Finally, I. Pärnamäe identified strategic goods lists and the National Defence Duties Plan as potential indicators of the companies and sectors deemed vital to national security.[846]

According to Supreme Court judgment No. 1-21-1421, trade secrets held by a defense industry company are presumptively considered "information" under Penal Code § 234²(1). Drawing on the theoretical framework and insights from industry interviews, this presumption is unlikely to be rebutted when the company's end user or operational domain is closely tied to the security of the Republic of Estonia.

[839] Priit Pruks's interview with Ingvar Pärnamäe and Erik Kannike.
[840] Priit Pruks's interviews with Lauri Almann, Ingvar Pärnamäe.
[841] Priit Pruks's interview with Erik Kannike, 10.04.2025.
[842] Eesti julgeolekupoliitika alused, p 2.
[843] Priit Pruks's interview with Kalev Koidumäe.
[844] Välisministeerium. Eesti toetus Ukrainale.
[845] Priit Pruks's interviews with Erik Kannike (10.04.2025); Viido Naruskberg and a security expert.
[846] Priit Pruks's interview with Ingvar Pärnamäe.

To conclude, a few reflections on the broader mission implied by the title of this thesis. Specifically, how Estonian legal scholarship might contribute to strengthening the defense of Estonia's defense industry.

As I. Pärnamäe has observed, the fundamental question is whether the Estonian defense industry is worth defending in the first place. [847] If the state does not regard its domestic defense industry as relevant to its security, then any discussion of legal mechanisms for its protection becomes essentially moot. However, if one accepts the principle set forth in the government's coalition agreement – that "the domestic defence industry is a component of our broad-based national defence capability"[848] – the next logical question is: what role can the law play in supporting that objective?

First, as previously noted, the Penal Code already contains provisions enabling the prosecution of industrial espionage. The Supreme Court has further clarified the definition of "information" under § 234²(1), thereby facilitating the work of the ISS (RKKK 1-21-1421, paras. 127 and 128). In other words, there is no legal vacuum in this regard.

The second question is whether trade secrets with national security implications should be afforded stronger protection. One potential approach would be to classify such information as a state secret. Section 7(6¹) of the State Secrets and Classified Information of Foreign States Act allows for this where the matter concerns an "object with a military purpose." However, a more salient consideration is that enterprises often prefer to operate in environments free from classified information – a view unanimously shared by the experts interviewed. In short, most businesses prefer to avoid dealing with classified information altogether.

An alternative approach would be to impose a broader duty on security services to protect the trade secrets of defense companies. A legal basis for such a measure exists: the ISS is tasked with preventing and combating intelligence activities directed against the state, while the FIS is tasked with safeguarding electronic information systems (State Secrets and Classified Information of Foreign States Act §§ 6(2) and 7(4)). However, this would require an interpretative expansion of the terms "state" and "electronic information security" to include private entities that do not handle classified information. Such an extension would, in turn,

[847] *Ibid.*
[848] Vabariigi Valitsus. Koalitsioonilepe 2024–2027. Uued investeeringud ja ettevõtete kindlustunne. Eesti kaitsetööstuse arendamine.

necessitate clear definitions of key terms such as "defense industry" and "critical technologies" to precisely determine the scope of entities and assets eligible for protection. Whether all defense-related enterprises would welcome such involvement remains an open question – particularly given that the ISS, as an agency under the resource-constrained Ministry of the Interior, may lack the capacity to provide meaningful support. According to E. Kannike, the defense industry could benefit from greater state assistance with background checks and physical security measures; however, he also acknowledges the limitations imposed by Estonia's small size and finite resources.[849] It should also be emphasized that a balance must be maintained between the responsibilities of the state and those of the industry. It would be unreasonable for an increased duty of protection on the part of security authorities not to be matched by a corresponding obligation on the part of industry to undergo vetting and invest in appropriate security measures.

Another option would be to restrict the availability of certain public information. All industry representatives interviewed supported the idea that limitations should be considered for publicly accessible data in the commercial register – particularly for companies operating in sectors critical to national security. V. Naruskberg further suggested that access to information related to operating licences may also merit restriction.[850] Naturally, if such measures were adopted universally, Estonian businesses could face increased challenges in conducting due diligence on prospective partners. Moreover, the potential risk of „over-classification"[851] must be carefully considered and weighed against the intended benefits.

An additional question arises in cases where defense companies seek a higher level of protection than the state is able – or willing – to provide. For instance, what if a defense company were to employ a counterintelligence officer, an arrangement not uncommon in the United States[852]? What legal tools would such an individual have at their disposal to carry out counterintelligence activities? More specifically, what lawful measures could be taken to identify and mitigate security threats? This issue primarily concerns the legal boundaries of unauthorized surveillance under Penal Code § 137, as well as the applicability of EU's data protection regulations. There appears to be sufficient interest among experts to transition from

[849] Priit Pruks's interview with Erik Kannike, 10.04.2025.
[850] Priit Pruks's interviews with Viido Naruskberg and a security expert.
[851] Priest, D., Arkin, W. M.
[852] The U.S. defense company Anduril was recently looking for a director of counterintelligence. See: https://www.anduril.com/careers/

public service, and the defense sector has already demonstrated that former military personnel are willing to move into private industry. Should similar opportunities be extended to former counterintelligence officers? This, too, presents an important legal question worthy of further consideration.

Ideally, the state would retain experienced officials. Achieving this, however, requires a broader societal understanding that "ensuring security involves more than preparing for war." [853] As Kristian Pärt, an official at the Ministry of the Interior, aptly notes, "Much like military capabilities, non-military security capabilities require consistent funding and stable development." [854] In short, Estonia needs both: shells for the Defence Forces and the capacity to attract top talent to the ISS.

[853] Pärt, K.
[854] *Ibid.*

## Kasutatud allikad

Kasutatud Eesti ja Euroopa Liidu õigusaktid ning rahvusvahelised lepingud


1. Avaliku teabe seadus. – RT I, 30.12.2024, 5.
2. Diplomaatiliste suhete Viini konventsioon. – RT II 2006, 16, 0.
3. Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
4. Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus. – RT I, 07.12.2018, 2.
5. Euroopa Liidu leping. – C 202/1, 7.6.2016.
6. Euroopa Parlamendi ja Nõukogu direktiiv 2009/43/EÜ, 6. mai 2009, kaitseotstarbeliste toodete ühendusesisese veo tingimuste lihtsustamise kohta. – ELT L 14/1, 10.6.2009.
7. Euroopa Parlamendi ja Nõukogu direktiiv 2009/81/EÜ, 13. juuli 2009, millega kooskõlastatakse teatavate kaitse- ja julgeolekuvaldkonnas ostjate poolt sõlmitavate ehitustööde ning asjade ja teenuste riigihankelepingute sõlmimise kord ja muudetakse direktiive 2004/17/EÜ ja 2004/18/EÜ. – ELT L 216/76, 20.08.2009.
8. Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2016/943, 8. juuni 2016, milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset. – ETL L 157/1, 15.06.2016.
9. Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) – ELT L 119/1, 4.5.2016.
10. Euroopa Parlamendi ja Nõukogu määrus (EL) 2019/25, 16. jaanuar 2019, mis käsitleb kauplemist teatavate kaupadega, mida on võimalik kasutada surmanuhtluse täideviimiseks, piinamiseks või muuks julmaks, ebainimlikuks või alandavaks kohtlemiseks või karistamiseks. – ELT L 30/1 31.1.2019.
11. Euroopa Parlamendi ja Nõukogu määrus (EL) 2021/697, 29. aprill 2021, millega luuakse Euroopa Kaitsefond ja tunnistatakse kehtetuks määrus (EL) 2018/1092, ELT L 170/149, 12.5.2021.
12. Euroopa Parlamendi ja Nõukogu määrus (EL) 2023/1525, 20. juuli 2023, mis käsitleb laskemoona tootmise toetamist. – ELT L 185/7, 24.7.2023.

13. Euroopa Parlamendi ja Nõukogu Määrus (EL) 2023/2418, 18. oktoober 2023, millega luuakse instrument Euroopa kaitsetööstuse tugevdamiseks ühishangete kaudu (EDIRPA). – ELT L-seeria, 26.10.2023.
14. Julgeolekuasutuste seadus. – RT I, 14.03.2023, 25.
15. Kaitseväe korralduse seadus. – RT I, 12.12.2024, 5.
16. Kaitseväe põhimäärus. – RT I, 28.06.2018, 8.
17. Karistusseadustik. – RT I, 12.12.2024, 6.
18. Kriminaalmenetluse seadustik. – RT I, 12.12.2024, 7.
19. Küberturvalisuse seadus. – RT I, 21.06.2024, 15.
20. Nõukogu määrus (EÜ) nr 428/2009, 5. mai 2009, millega kehtestatakse ühenduse kord kahesuguse kasutusega kaupade ekspordi, edasitoimetamise, vahendamise ja transiidi kontrollimiseks. – ELT L 134, 29.5.2009.
21. Politsei- ja Piirivalveameti ja Kaitsepolitseiameti vaheline uurimisalluvus. – RT I, 07.05.2019, 4.
22. Põhja-Atlandi leping. – RT II 2004, 5, 14.
23. Relvaseadus. – RT I, 12.12.2024, 3.
24. Riigihangete seadus. – RT I, 07.06.2024, 11.
25. Riigikaitseliste sundkoormiste seadus. – RT I, 10.03.2022, 13.
26. Riigikaitseseadus. – RT I, 14.03.2023, 31.
27. Riigi Infosüsteemi Ameti põhimäärus. – RT I, 27.12.2024, 10.
28. Riigisaladuse ja salastatud välisteabe seadus. – RT I, 12.12.2024, 11.
29. Strateegilise kauba seadus. – RT I, 12.12.2024, 12.
30. Siseministri 6. juuni 2001 määrus nr 76 „Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord“. – RT I, 02.08.2017, 7.
31. Sõjaliste kaupade ühine Euroopa Liidu nimekiri, mille nõukogu võttis vastu 19. veebruaril 2024. – C/2024/1945, 1.3.2024.
32. Tsiviilseadustiku üldosa seadus. – RT I, 31.12.2024, 48.
33. Vabariigi Valitsuse 18. mai 2023. a korraldus nr 131 „Vabariigi Valitsuse tegevusprogrammi 2023–2027“ „kinnitamine“ muutmine. – RT III, 06.03.2024, 6.
34. Vabariigi Valitsuse 5. märtsi 2021. a korraldus nr 104 „Tegevusalade riigikaitseliste sundkoormiste koondkava kinnitamine“. – RT III 09.03.2021, 3.

35. Vabariigi Valitsuse 18. juuli 2022. a määrus nr 71 „Vabariigi Valitsuse määruste muutmine seoses Politsei- ja Piirivalveameti laevade üleandmisega Kaitseministeeriumi valitsemisalasse“. – RT I, 21.07.2022, 1.
36. Vabariigi Valitsuse 23. septembri 2016. a määrus nr 106 „Riigikaitseobjekti kaitse kord“. – RT I, 12.03.2019, 33.
37. Vabariigi Valitsuse 22. detsembri 2011. a määrus nr 171 „Strateegiliste kaupade nimekiri“. – RT I, 04.06.2024, 2.
38. Vabariigi Valitsuse 20. detsembri 2007. a määrus nr 262 „Riigisaladuse ja salastatud välisteabe kaitse kord“. – RT I, 29.12.2024, 16.
39. Väljasõidukohustuse ja sissesõidukeelu seadus. – RT I, 06.07.2023, 125.
40. Äriseadustik. – RT I, 06.07.2023, 131.

Kasutatud välisriikide õigusaktid

1. Arms Export Control Act (AECA) of 1976, Public Law 90–629, 94th Congress.
2. Code of Federal Regulations. – https://www.ecfr.gov/ (01.04.2025).
3. Economic Espionage Act of 1996. Public Law 104–294, 104th Congress (11.10.1996). – https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf (15.11.2024).
4. Executive Order 12333. – https://www.dni.gov/files/documents/OGC/IC-Legal-Reference-Book-2024.pdf (11.02.2025).
5. Executive Order 13637. – https://www.govinfo.gov/content/pkg/DCPD-201300143/pdf/DCPD-201300143.pdf (01.04.2025).
6. Gesetz zum Schutz von Geschäftsgeheimnissen. – https://www.gesetze-im-internet.de/englisch_geschgehg/englisch_geschgehg.html (10.02.2025).
7. National Security Act 2023. (11.07.2023). – https://www.legislation.gov.uk/ukpga/2023/32/section/2 (15.11.2024).
8. National Security Act. Executive Yuan. (08.06.2022). – https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030028 (05.03.2025).
9. Strafgesetzbuch (StGB). BGBl. 2024 I Nr. 109.
10. Strafprozeßordnung (Deutschland). BGBl. 2024 I Nr. 109.
11. United States Code. – https://uscode.house.gov/ (01.04.2025).

Kasutatud eelnõude seletuskirjad


1. 113 SE I. Riigihangete seaduse muutmise seaduse eelnõu seletuskiri. Vastu võetud 25.01.2012. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/5498ac05-bc6e-7882-13a3-328366ee31f2/riigihangete-seaduse-muutmise-seadus/ (09.04.2025).
2. 417 SE. Riigikaitseseaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri. Vastu võetud 16.02.2022. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/44178720-02b2-4d30-8707-d7dcf606dcee/riigikaitseseaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/ (09.04.2025).
3. 468 SE. Relvaseaduse muutmise ja sellega seonduvalt teist seaduste muutmise seaduse eelnõu seletuskiri. Vastu võetud 20.11.2024. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/6af5a052-2757-4a32-8048-7cc285580339/relvaseaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/ (09.04.2025).
4. 642 SE. Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (terrorismivastase võitluse direktiivi ülevõtmine) eelnõu seletuskiri. Vastu võetud 19.12.2018. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/af992ccb-58f7-4a6e-bef5-d8f82772b3b7/karistusseadustiku-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus-terrorismivastase-voitluse-direktiivi-ulevotmine/ (09.04.2025).
5. 678 SE. Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seaduse eelnõu seletuskiri. Vastu võetud 21.11.2018. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/9b6f21b8-db1c-436d-a045-326913d80d22/ebaausa-konkurentsi-takistamise-ja-arisaladuse-kaitse-seadus/ (09.04.2025).
6. Riigisaladuse ja salastatud välisteabe seaduse, riigihangete seaduse ning riigilõivuseaduse muutmise seaduse (tööstusjulgeolek) eelnõu seletuskiri. Eelnõude infosüsteem (18.09.2024). – https://eelnoud.valitsus.ee/main/mount/docList/7771037e-ded1-492e-928e-01a464e17d27#yDoVThpg (09.04.2025).


Kasutatud Eesti ja Euroopa kohtu kohtupraktika


1. EKo C-337/05, Euroopa Ühenduste Komisjon *versus* Itaalia Vabariik.
2. Harju Maakohus 1-17-4067.

3. Harju Maakohus 1-18-1220.
4. Harju Maakohus 1-19-6496.
5. Harju Maakohus 1-19-6812.
6. Harju Maakohus 1-19-991.
7. Harju Maakohus 1-21-1256.
8. Harju Maakohus 1-24-2429/9.
9. Harju Maakohus 1-24-2627/6.
10. Harju Maakohus 1-24-2791.
11. Harju Maakohus 1-24-2828/10.
12. RKKKo 1-16-10888/62.
13. RKKKm 1-17-9149/626.
14. RKKKo 1-21-1421.
15. RKKKo 1-22-3155.
16. RKKKo 3-1-1-23-17.
17. RKTKo 2-20-13897.
18. RKÜKo 3-4-1-2-13.

Kasutatud välisriikide ja rahvusvaheliste kohtute kohtupraktika


1. Case Concerning The Military and Paramilitary Activities in and against Nicaragua (*Nicaragua vs. United States of America*). ICJ Reports 1986, 14.
2. *United States v. Haitao Xiang* 67 F.4th 895 (8th Cir. 2023).
3. *United States v. Mo Hailong*, No. 4:13-CR-147 (S.D. Iowa October 10, 2016).
4. *United States v. Su Bin*, No. 8:14-cr-00131-CAS (S.D. Cal. July 13, 2016).
5. *United States v. Li Xiaoyu, Dong Jiazhi*, No. 4:20-CR-6019-SMJ (E.D. Wash. July 7, 2020).
6. *United States v. Xiaoqing Zheng*, 114 F.4th 280 (2nd Cir. 2024).
7. *United States v. Yanjun Xu*, 110 F.4th 841 (6th Cir. 2024).
8. U.S. Supreme Court. *Pinkerton v. United States*, 328 U.S. 640 (1946).


Kasutatud kirjandus


1. Anderson, R. J., Petitcolas, F. A. P. On the Limits of Steganography. – IEEE Journal of Selected Areas in Communications 1998/16 (4).

2. Anton, S. Eesti kultuuri ja rahvuse mõiste põhiseaduse preambulis. – Riigiõiguse aastaraamat 2020.
3. Applebaum, A. Autocracy, Inc. The Dictators Who Want to Run the World. Doubleday 2024.
4. Austin, J. The Province of Jurisprudence Determined. Cambridge University Press 1995.
5. Banks, W. Cyber Attribution and State Responsibility. – International Law Studies 2021/97.
6. Bergman, R. Rise and Kill First. The Secret History of Israel's Targeted Assassinations. John Murray 2018.
7. Button, M., Knickmeier, S. Economic and Industrial Espionage: Characteristics, Techniques and Response. – The Handbook of Security (ed. M. Gill) Springer 2022.
8. Carl, S., Kilchling, M., Knickmeier, S., Wallwaey, E. (2017). Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa. Schriftenreihe Forschung aktuell des Max-Planck-Instituts für ausländisches und internationales Strafrecht Band 49. (Viidatud: Button, M., Knickmeier, S. Economic and Industrial Espionage: Characteristics, Techniques and Response. – The Handbook of Security (ed. M. Gill) Springer 2022).
9. Carril, R., Duggan, M. The Impact of Industry Consolidation on Government Procurement: Evidence from Department of Defense Contracting. – National Bureau of Economic Research, October 2018.
10. Drezner, D. W. How Everything Became National Security. – Foreign Affairs. September/October 2024.
11. Eftimiades, N. A Series on Chinese Espionage Vol. I Operations and Tactics. Vitruvian Press 2020.
12. Fialka, J. J. War by Other Means: Economic Espionage in America. W W Norton & Co 1997. (Viidatud: Lotrionte, C. Countering State-Sponsored Cyber Economic Espionage Under International Law. – North Carolina Journal of International Law 2017/40, No 2).
13. Fox, C. L. Hybrid Warfare. The Russian Approach to Strategic Competition and Conventional Military Conflict. Four Minute Men Books 2023.
14. Friedman, R. S. Open source intelligence: A review essay. – Parameters 1998/28, No 2. (Viidatud: Zegart, A. Spies, Lies, and Algorithms. The History of American Intelligence. Princeton University Press 2022).

15. Grauberg, T., Nääs, O. Paneeldiskussioon teemal „Teabehange ja jälitus kriminaalmenetluses“. – Juridica 2024/9-10, lk 671-682
16. Gustafson, K. jt. Intelligence warning in the Ukraine war, Autumn 2021-Summer 2022. – Intelligence and National Security 2024/39 (3).
17. Heldna, E. Julgeolekuasutuste kogutud informatsiooni kasutamine kriminaalmenetluses ja jagamine uurimisasutustega. – Juridica 2016/10.
18. Heuninckx, B. EU Public Procurement Law: An Introduction. (ed. Arrowsmith, S.) University of Nottingham 2010.
19. Hvistendahl, M. The Scientist and the Spy. Riverhead Books 2020.
20. Javers, E. Broker. Trader. Lawyer. Spy. The Secret World of Corporate Espionage. New York: Harper 2010.
21. Johnson, L. K. The Third Option: Covert Action and American Foreign Policy. Oxford University Press 2022.
22. Joske, A. Spies and Lies. How China’s Greatest Covert Operations Fooled the World. Hardie Grant Books 2022.
23. Jäätma, J. Julgeoleku mõiste. – Juridica 2020/2.
24. Kaska, K., Aasmann, L. Julgeolekuasutuste roll küberjulgeoleku tagamisel ja seda mõjutavad suundumused rahvusvahelises õiguses. – Juridica 2020/2.
25. Kergandberg, E. Julgeolek *versus* ehe jälitustegevus, „kah-jälitustegevus“ ja teabehankeks maskeerunud eriti varjatud jälitustegevus Eesti õiguses. – Juridica 2024/9-10, lk 657-670.
26. Kergandberg, E. Luurates „Teeme ära!“ meeskonnaga kevadisel jälitusmaastikul. – Juridica 2020/3.
27. Kross, J. Rahvusvahelise lepingu mõistest. Riigiõiguse aastaraamat 2020. Eesti Teaduste Akadeemia riigiõiguse sihtkapital.
28. Kirsipuu, K. Ärisaladuse mõiste KarS § 377 lg 1 sätestatud kuriteokoosseisu tunnusena. Magistritöö. Tartu Ülikool 2020.
29. Knickmeier, S. Spies without borders? The phenomena of economic and industrial espionage and the deterrence strategies of Germany and other selected European countries. – Security Journal 2020/33.
30. Koort, E. Riigisaladus ja tööstusjulgeolek. Tallinna Tehnikaülikool 2004.
31. Kroenig, M. The Return of Great Power Rivalry: Democracy versus Autocracy from the Ancient World to the U.S. and China. Oxford University Press 2020.

32. Lin, H. Attribution of Malicious Cyber Incidents. – Columbia Journal of International Affairs 2016/70, No 1.
33. Lotrionte, C. Countering State-Sponsored Cyber Economic Espionage Under International Law. – North Carolina Journal of International Law 2017/40, No 2.
34. Lowenthal, M. Intelligence. From Secrets to Policy (8th Edition). CQ Press 2020.
35. Lucas, E. The New Cold War: Putin's Russia and the threat to the West. Palgrave Macmillan 2008.
36. Madise, Ü. (peatoimetaja) jt. Eesti Vabariigi põhiseadus. Komm vlj. 5. vlj. Tartu: Sihtasutus Iuridicum, 2020.
37. Madureira, L. jt. Competitive intelligence: A unified view and modular definition. – Technological Forecasting and Social Change 2021/173.
38. Marshall, T. The Future of Geography: How Power and Politics in Space Will Change Our World. Elliott & Thompson 2023.
39. McFaul, M. Autocrats vs. Democrats: China, Russia, and the New Global Order. Mariner Books 2025.
40. Michel, P. R. Big Tech Has a Patent Violation Problem. Harvard Business Review 05.08.2022. – https://hbr.org/2022/08/big-tech-has-a-patent-violation-problem (14.11.2024).
41. Miller, C. Chip War: The Fight for the World's Most Critical Technology. Simon & Schuster 2022.
42. Mobley, B. W., Wege, C. A. Counterintelligence Vetting Techniques Compared across Multiple Domains. – International Journal of Intelligence and Counterintelligence 2021/34 (4).
43. Mägi, M. Ärisaladuse kaitse karistusõigusliku regulatsiooni efektiivsus kehtivas õiguses. Magistritöö. Tartu Ülikool 2017.
44. Nasheri, H. Economic Espionage and Industrial Spying. Cambridge University Press 2005. (viidatud: Reid, M. A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat? – University of Miami Law Review 2016/70, No 3., lk 798)
45. Parind, M., Simovart, M. A. (koost). Riigihangete seadus. Komm vlj. Tallinn: Juura 2019.
46. Perlroth, N. This is How They Tell Me the World Ends: The Cyberweapons Arms Race. Bloomsbury 2021.

47. Polmar, N., Allen, T. B. Spy Book: The Encyclopedia of Espionage. 2. Ed. New York: Random House Reference 2004. (Viidatud: Purre, M. Riigireetmine ja riigireetur. – Juridica 2020/2, lk 79–89).
48. Priest, D., Arkin, W. M. Top Secret America: The Rise of the New American Security State. Little, Brown and Company 2011.
49. Purre, M. Riigireetmine ja riigireetur. – Juridica 2020/2.
50. Purre, M. Riigireetmise ja salakuulamise regulatsioon Eesti karistusõiguses. Magistritöö. Tallinna Tehnikaülikool 2014.
51. Reid, M. A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat? – University of Miami Law Review 2016/70, No 3.
52. Richterova, D. jt. Russian Sabotage in the Gig-Economy Era. – The RUSI Journal 2024/169 (5).
53. Risklakki, J. Luure ja spionaaž. Doktriinid, operatsioonid, agendid. 2023.
54. Rustmann Jr., F.W. CIA, Inc.: Economic Espionage and the Craft of Business Intelligence. Potomac Books 2002.
55. Saarts, T. Kaitsedemokraatia militaarses infooaasis – Eesti lähitulevik? – Vikerkaar 2024/6.
56. Sage-Passant, L. Beyond States and Spies: The Security Intelligence Services of the Private Sector. Edinburgh University Press 2024.
57. Schindler, S., DiCarlo, J., Paudel, D. The new cold war and the rise of the 21st-century infrastructure state. – Transactions of the Institute of British Geographers 2022/47 (2).
58. Schweitzer, P. Friendly spies: How America's Allies are Using Economic Espionage to Steal Our Secrets. Atlantic Monthly Press 1993.
59. Shah, R. M., Kirchhoff, C. Unit X: How the Pentagon and Silicon Valley Are Transforming the Future of War. Scribner 2024.
60. Shulipa, Y. How Putin Kills Abroad. Vilnius: International Center for Civic Initiatives „Our Home", 2021. (Viidatud: Riehle, K. P. The Russian FSB. A Concise History of the Federal Security Service. Georgetown University Press 2024, lk 90).
61. Sinisalu, A. Mõjutustegevuse piirid rahvusvahelises õiguses. Doktoritöö. Tartu: Tartu Ülikooli Kirjastus 2012.
62. Sinisalu, A., Maiberg, H. Linn tuleb hävitada Jehoova auks ehk religioosse äärmusluse oht riigile. – Juridica 2024/8.
63. Sootak, J. Karistusõigus. Üldosa. Tallinn: Juura 2018.

64. Sootak, J. Seadusainsus. Kui isiku tegu vastab mitmele süüteokoosseisule, siis mitme järgi ja kuidas ta tegelikult vastutab? – Juridica 2010/1.
65. Sootak, J., Pikamäe, P. (koost). Karistusseadustik. Komm vlj. 5. vlj. Tallinn: Juura 2021.
66. StGB-MK: Münchener Kommentar zum StGB. 4. Auflage. München: Beck 2021.
67. Thiel, P., Masters, B. Zero to One: Notes on Startups, or How to Build the Future. New York: Crown Business 2014.
68. Tikk-Ringas, E. Küberjulgeoleku õiguslik raamistik. – Juridica 2012/3.
69. Tran, D. The Law of Attribution: Rules for Attributing the Source of a Cyber Attack. – Yale Journal of Law & Technology 2018/20.
70. Warner, W. T. Economic Espionage: A Bad Idea. – National Law Journal, 12 April 1993. (viidatud: Lotrionte, C. Countering State-Sponsored Cyber Economic Espionage Under International Law. – North Carolina Journal of International Law 2017/40, No 2, lk 469)
71. Wice, S. When to Refer to the U.S. Code Versus the Underlying Statute. – Yale Journal on Regulation. Notice & Comment. Yale Journal on Regulation (July 25, 2018). – https://www.yalejreg.com/nc/when-to-refer-to-the-u-s-code-versus-the-underlying-statute/ (26.04.2025).
72. Vogelstein, F. Dogfight: How Apple and Google Went to War and Started a Revolution. Sarah Crichton Books 2013.
73. Võsaste, S. Kuriteo matkimise kasutamine riigivastaste süütegude ennetamisel. Magistritöö. Tartu Ülikool 2024.
74. Värk, R. Julgeolekunõukogu tõlgendused terrorismi olemusele. – Juridica 2010/2.
75. Zegart, A. Spies, Lies, and Algorithms. The History of American Intelligence. Princeton University Press 2022.

Kasutatud intervjuud

1. Priit Pruksi intervjuu Lauri Almanniga, 27.01.2025.
2. Priit Pruksi intervjuu Erik Kannikega, 31.01.2025.
3. Priit Pruksi intervjuu Erik Kannikega, 10.04.2025.
4. Priit Pruksi intervjuu Kalev Koidumäega, 01.04.2025.
5. Priit Pruksi intervjuu Silver Lättiga, 28.01.2025.
6. Priit Pruksi intervjuu Viido Naruskbergi ja julgeolekueksperdiga, 10.04.2025.
7. Priit Pruksi intervjuu Ingvar Pärnamäega, 15.04.2025.

8. Priit Pruksi intervjuu Arnold Sinisaluga, 07.08.2024.
9. Priit Pruksi intervjuu Arnold Sinisaluga, 26.09.2024.
10. Priit Pruksi intervjuu Oliver Väärtnõuga, 09.04.2025.
11. Priit Pruksi intervjuu endise luureametnikuga.
12. Priit Pruksi intervjuu kaitsetööstuse eksperdiga.

Muud allikad

1. Andmekaitseinspektsiooni aastaraamat 2024.
2. Anduril. – https://www.anduril.com/ (27.04.2025).
3. Allen, G.; Berenson, D. Why is the U.S. Defense Industrial Base So Isolated from the U.S. Economy. CSIS (August 20, 2024). – https://www.csis.org/analysis/why-us-defense-industrial-base-so-isolated-us-economy (22.04.2025).
4. Antonov, D., Osborn, A. Russia says hypersonic missile strike on Ukraine was a warning to 'reckless' West. Reuters 22.11.2025. – https://www.reuters.com/world/europe/kremlin-says-hypersonic-missile-strike-ukraine-was-warning-west-2024-11-22/ (04.02.2025).
5. Anvelt, K. Täismahus: Tunnistajast tapjaks: Piusa õppetunnid. – Eesti Ekspress 14.02.2012.
6. AS Milrem 2023. aasta majandusaasta aruanne.
7. Associated Press. Russia has used its hypersonic Oreshnik missile for the first time. What are its capabilities? (09.12.2024). – https://apnews.com/article/russia-oreshnik-hypersonic-missile-putin-ukraine-war-345588a399158b9eb0b56990b8149bd9 (04.02.2025).
8. AS Threod Systems 2023. aasta majandusaasta aruanne.
9. Bajarunas, E. Using NATO's Article 5 Against Hybrid Attacks. CEPA 11.02.2025. – https://cepa.org/article/using-natos-article-5-against-hybrid-attacks/ (04.03.2025).
10. Baldwin, H. Critical Dual-Use Technologies: Commercial, Regulatory, Societal and National Security Challenges. General Report. NATO Parliamentary Assembly 26.08.2024. – https://www.nato-pa.int/download-file?filename=/sites/default/files/2024-12/051%20ESC%2024%20E%20rev.2%20fin%20-%20CRITICAL%20DUAL-USE%20TECHNOLOGIES%20-%20BALDWIN%20REPORT.pdf (10.02.2025).
11. Bellingcat. How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine. (26.04.2021). – https://www.bellingcat.com/news/uk-

and-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/ (11.02.2025).
12. Black Cube. – https://www.blackcube.com/ (09.04.2025).
13. Bond, S. China's influence operations against the U.S. are bigger than TikTok. NPR 25.04.2024. – https://www.npr.org/2024/04/26/1247347363/china-tiktok-national-security (14.11.2024).
14. Boot, M. Our enemies aren't drinking lattes. Los Angeles Times 07.07.2006. – https://www.latimes.com/archives/la-xpm-2006-jul-05-oe-boot5-story.html (24.01.2025).
15. Brennan, M. Transcript: CIA director William Burns on „Face the Nation", Feb. 26, 2023. CBS News. – https://www.cbsnews.com/news/william-burns-cia-director-face-the-nation-transcript-02-26-2023/ (06.03.2025).
16. Cambridge Dictionary. Reconnaissance. – https://dictionary.cambridge.org/dictionary/english/reconnaissance (19.04.2025).
17. Center for Strategic & International Studies. Survey of Chinese Espionage in the United States Since 2000. March 2023. – https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000 (02.03.2025).
18. Central Intelligence Agency. Careers. Jobs. Case Officer. – https://www.cia.gov/careers/jobs/case-officer/ (11.02.2025).
19. Cokelaere, H. Dutch government plans to screen scientists for national security risks. Politico 07.04.2025. – https://www.politico.eu/article/dutch-government-scientists-tech-national-security-espionage/ (09.04.2025).
20. Congressional Research Service. – https://crsreports.congress.gov/ (15.01.2025).
21. Control Risks. – https://www.controlrisks.com/ (09.04.2025).
22. CSIS. Public Report 2019. The Intelligence Cycle. – https://www.canada.ca/en/security-intelligence-service/corporate/publications/2019-public-report/the-intelligence-cycle.html (13.04.2025).
23. CSIS. Thousand Talents Plan. (07.08.2020) – https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20201201/020/index-en.aspx (02.03.2025).
24. Cybernetica. – https://cyber.ee/company/our-story (04.03.2025).
25. CybExer Technologies. – https://cybexer.com/ (08.02.2025).
26. CybExer Technologies OÜ. Majandusaasta aruanne 2023.

27. Daalder, I. H., Lindsay, J. M. The New Cold War. Brookings 30.09.2001. – https://www.brookings.edu/articles/the-new-cold-war/ (25.10.2024).
28. Dahl, R. Charlie ja šokolaadivabrik. Tallinn: Draakon ja Kuu, 2017.
29. Defence Estonia. EKTL member Rantelon is a creator, developer and manufacturer of innovative electronic systems. (24.11.2023). – https://defence.ee/news/ektl-member-rantelon-is-a-creator-developer-and-manufacturer-of-innovative-electronic-systems/ (03.04.2025).
30. Defense Innovation Unit. – https://www.diu.mil/ (10.02.2025).
31. DefSecIntel Solutions OÜ 2023. aasta majandusaasta aruanne.
32. Deutsche Welle. Chinese cyberattacks hit nearly half of German firms, study. (28.08.2024). – https://www.dw.com/en/chinese-cyberattacks-hit-nearly-half-of-german-firms-study/a-70070417 (10.02.2025).
33. Detsch, J. Ukraine's Cheap Drones Are Decimating Russia's Tanks. Report. Foreign Policy 09.04.2024. – https://foreignpolicy.com/2024/04/09/drones-russia-tanks-ukraine-war-fpv-artillery/.
34. Dobrokhotov, R., Grozev, C., Weiss, M. Afgantsy Redux: How Russian military intelligence used the Taliban to bleed U.S. forces at the end of America's longest war. The Insider 08.01.2025. – https://theins.ru/en/politics/277723 (11.02.2025).
35. eAgronom. – https://www.eagronom.com/ (02.03.2025).
36. „Eesti julgeolekupoliitika alused" heakskiitmine. – RT III, 28.02.2023, 1. LISA „Eesti julgeolekupoliitika alused" (22.02.2023).
37. Eesti Kaitse- ja Kosmosetööstuse Liit. Majandusaasta aruanne 2023.
38. Eesti kaitsetööstusturid pakkusid välja droonimüüri idee Euroopa Liidu idapiiri tugevdamiseks. – Postimees 27.02.2025.
39. Eesti Kaitsevägi. Julgeolek. – https://mil.ee/uksused/luurekeskus/julgeolek/ (11.02.2025).
40. Eesti Kaitsevägi. Julgeoleku tagamine luure abil. – Ajakiri Sõdur 2025/1.
41. Eesti Kaitsevägi. Kaitseväe juhataja: Ukraina võitlus on meie võitlus. (06.04.2015). – https://mil.ee/uudised/kaitsevae-juhataja-ukraina-voitlus-on-meie-voitlus/ (04.03.2025).
42. Eesti Kaitsevägi. Luurekeskus. Luureliigid. – https://mil.ee/uksused/luurekeskus/luureliigid/ (02.03.2025).
43. Eesti Kaitsevägi. Luurepataljon. – https://mil.ee/uksused/maavagi/diviis/luurepataljon/ (11.02.2025).

44. Eesti Kaitsevägi. Mida võiks teada kaitseväeluurest? – Ajakiri Sõdur 2025/1.
45. Eesti Kaitsevägi. NATO õppus CWIX oli kaitseväelastele edukas. (21.06.2024). – https://mil.ee/uudised/nato-oppus-cwix-oli-kaitsevaelastele-edukas/ (06.03.2025).
46. Eesti Keele Instituut. Reke. – https://sonaveeb.ee/search/unif/dlall/dsall/reke/1/est (11.02.2025).
47. Eesti Keele Instituut. Spionaaž. – https://sonaveeb.ee/search/unif/dlall/dsall/spionaa%C5%BE/1/est (11.02.2025).
48. Eesti Põllumajandus-Kaubanduskoda. Toidujulgeolek. (12.11.2022). – https://epkk.ee/toidujulgeolek/ (04.03.2025).
49. Eesti Välisministeerium. Eesti omistas esimest korda riigivastased küberrünnakud kuriteo toimepanijatele, kelleks on Venemaa sõjaväeluure. (05.09.2024). – https://vm.ee/uudised/eesti-omistas-esimest-korda-riigivastased-kuberrunnakud-kuriteo-toimepanijatele-kelleks (02.03.2025).
50. Einmaa, I.-M. Eesti loob võimaliku ränderünde ohjeldamiseks 1000-liikmelise kriisirühma. ERR 04.03.2025. – https://www.err.ee/1609497214/eesti-loob-voimaliku-randerunde-ohjeldamiseks-1000-liikmelise-kriisiruhma (04.03.2025).
51. Einmann, A. GRU andis Eesti monumentide rüvetamiseks väga täpsed juhised. – Postimees 03.01.2025.
52. Einmann, A. GRU kasuks luuranud elektrik näitas, et eriteenistuste huvi pälvimiseks ei pea valdama riigisaladust. – Postimees 14.04.2020.
53. Epner, E., Moora, E. „Ta on meie aja kangelane.“ Rahva ees säravale Pevkurile heidetakse ette suure plaani puudumist. – Eesti Ekspress 03.02.2025.
54. ERR. Harri Tiido: luuramisest ja spioneerimisest. (24.09.2024). – https://www.err.ee/1609468270/harri-tiido-luuramisest-ja-spioneerimisest (11.02.2025).
55. ERR. Ilves: üritan lugemise asemel panna lõpuks kirja seda, mida olen tahtnud öelda. (28.01.2025). – https://kultuur.err.ee/1609588466/ilves-uritan-lugemise-asemel-panna-lopuks-kirja-seda-mida-olen-tahtnud-oelda (09.04.2025).
56. ERR. Läti kinnitas spionaažis kahtlustatavate Eesti ja Ukraina kodaniku vahistamist. (11.03.2025). – https://www.err.ee/1609629428/lati-kinnitas-spionaazis-kahtlustatavate-eesti-ja-ukraina-kodaniku-vahistamist (07.04.2025).
57. ERR. Läänemets: riigikaitseobjektide nimekiri täieneb. (15.01.2025). – https://www.err.ee/1609577170/laanemets-riigikaitseobjektide-nimekiri-taieneb (29.01.2025).

58. ERR. Politsei hinnangul pole lubatud nende hooneid pildistada ega filmida. (25.03.2025). – https://www.err.ee/1609638304/politsei-hinnangul-pole-lubatud-nende-hooneid-pildistada-ega-filmida (07.04.2025).
59. ERR. Riigikontroll: vaid üks elektritaristu objekt on selgelt kaitstud. (15.01.2025). – https://www.err.ee/1609576618/riigikontroll-vaid-uks-elektritaristu-objekt-on-selgelt-kaitstud (29.01.2025).
60. ERR. Riik asutab põlevkivist lõhkeaine tootmiseks ettevõtte Hexest (24.04.2025). – https://www.err.ee/1609673597/riik-asutab-polevkivist-lohkeaine-tootmiseks-ettevotte-hexest (24.04.2025).
61. ERR. Rohelised: tuumaenergeetika on tõsine oht julgeolekule. (19.04.2022). – https://www.err.ee/1608569242/rohelised-tuumaenergeetika-on-tosine-oht-julgeolekule (04.03.2025).
62. ERR. SDE ja Reformierakond ei toeta sõjaväelist piirivalvet. (09.10.2018). – https://www.err.ee/867743/sde-ja-reformierakond-ei-toeta-sojavaelist-piirivalvet (04.03.2025).
63. ERR. Siseministri ja ajakirjaniku auto lõhkumises korraldas venemeelne aktivist. (05.12.2024). – https://www.err.ee/1609542391/siseministri-ja-ajakirjaniku-auto-lohkumise-korraldas-venemeelne-aktivist (11.02.2025).
64. ERR. Tsahkna kritiseeris Bideni valitsuse otsust piirata kiibieksporti Eestisse. (16.01.2025). – https://www.err.ee/1609577518/tsahkna-kritiseeris-bideni-valitsuse-otsust-piirata-kiibieksporti-eestisse (05.03.2025).
65. ERR. Tammet: USA kiibipiirang Eestit ei mõjuta. (20.01.2025). – https://www.err.ee/1609581007/tammet-usa-kiibipiirang-eestit-ei-mojuta (18.04.2025).
66. ERR. Venemaa pani välja auhinna Milremi sõiduki kättesaamiseks Ukrainast. (05.09.2022). – https://www.err.ee/1608705520/venemaa-pani-valja-auhinna-milremi-soiduki-kattesaamiseks-ukrainast (03.04.2025).
67. Estdev. Estonia launches cyber range training exercises in Ukraine under the Tallinn Mechanism framework. (11.12.2024). – https://estdev.ee/en/articles/estonia-launches-cyber-range-training-exercises-ukraine-under-tallinn-mechanism-framework (13.04.2025).
68. Euroopa Komisjon. Liidu välisasjade ja julgeolekupoliitika kõrge esindaja. Uus kaitsetööstuse strateegia: EL-i valmisoleku saavutamine reageerimisvõimelise ja keskse Euroopa kaitsetööstuse abil. (05.03.2025).

69. Euroopa Komisjon. Ühisteatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele. Uus Euroopa kaitsetööstuse strateegia: EL-i valmisoleku saavutamine reageerimisvõimelise ja keskse Euroopa kaitsetööstuse abil. Brüssel 05.03.2024.
70. European Commission. On options for enhancing support for research and development involving technologies with dual-use potential. White Paper. (24.01.2024). – https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec_rtd_white-paper-dual-use-potential.pdf (10.02.2025).
71. European Commission. Press statement by President von der Leyen on the defence package. (04.03.2025) – https://ec.europa.eu/commission/presscorner/detail/sv/statement_25_673 (05.04.2025).
72. European Council on Foreign Relations. Mapping Palestinian Politics. Security Forces. Internal Security Force (ISF) – Hamas. – https://ecfr.eu/special/mapping_palestinian_politics/internal_security_force/ (11.02.2025).
73. European Defence Agency. A strategy for the European Defence Technological and Industrial Base. (14.05.2007). – https://eda.europa.eu/docs/documents/strategy_for_the_european_defence_technological_and_industrial_base.pdf (16.01.2025).
74. European Parliament. Directorate-General for External Policies. The development of a European Defence Technological and Industrial Base (EDTIB). 2013 juuni. – https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/433838/EXPO-SEDE_ET%282013%29433838_EN.pdf (16.01.2025).
75. FBI. Atom Spy Case/Rosenbergs. – https://www.fbi.gov/history/famous-cases/atom-spy-caserosenbergs (06.03.2025).
76. FBI. Counterintelligence. – https://www.fbi.gov/investigate/counterintelligence.
77. FBI. Counterintelligence. Transnational Repression. – https://www.fbi.gov/investigate/counterintelligence/transnational-repression (19.04.2025).
78. FBI. Counterintelligence Strategic Partnership Intelligence Note. 2015 september. – https://info.publicintelligence.net/FBI-ChineseTalentPrograms.pdf.
79. FBI. Economic Espionage. FBI Launches Nationwide Awareness Campaign. (23.07.2015). – https://www.fbi.gov/news/stories/economic-espionage (04.02.2025).

80. FBI. FAQ. What is the FBI's foreign counterintelligence responsibility? – https://www.fbi.gov/about/faqs/what-is-the-fbis-foreign-counterintelligence-responsibility (09.04.2025).
81. FBI. FAQ. Where is the FBI's authority written down? – https://www.fbi.gov/about/faqs/where-is-the-fbis-authority-written-down (11.02.2025).
82. FBI. What is „economic espionage"? – https://www.fbi.gov/about/faqs/what-is-economic-espionage (12.02.2025).
83. Feickert, A. The Army's M-1E3 Abrams Tanks Modernization Program. Congressional Research Service, 21.01.2025. – https://www.congress.gov/crs-product/IF12495 (09.04.2025).
84. Ferguson, N., Rice, C. Niall Ferguson and Condolezza Rice on the new cold war. The Economist 13.11.2023. – https://www.economist.com/the-world-ahead/2023/11/13/niall-ferguson-and-condoleezza-rice-on-the-new-cold-war (25.10.2024).
85. Ferragamo, M. What is the BRICS Group and Why is it Expanding? Council on Foreign Relations 18.10.2024. – https://www.cfr.org/backgrounder/what-brics-group-and-why-it-expanding (14.11.2024).
86. Finnish Customs. Finnish Customs suspects the operaator of a nuclear power plant construction project of a regulation offence. 17.04.2025. – https://tulli.fi/en/-/finnish-customs-suspects-the-operator-of-a-nuclear-power-plant-construction-project-of-a-regulation-offence (17.04.2025).
87. Fox News. Trump reveals 'one very big power' the US has over China. – https://www.youtube.com/watch?v=RN0nR8Rx0KI (04.02.2025).
88. Framework for Artifical Intelligence Diffusion. A Rule by the Industry and Security Bureau on 01/15/2025.
89. France 24. France is top industrial espionage offender. (04.01.2011). – https://www.france24.com/en/20110104-france-industrial-espionage-economy-germany-russia-china-business (02.04.2025).
90. Freedman, L. Putin Keeps Threatening to Use Nuclear Weapons. The New York Times 03.10.2024. – https://www.nytimes.com/2024/10/03/opinion/putin-russia-nuclear-weapons.html (14.11.2024).
91. Freedom House. Case Studies: China. (2021) – https://freedomhouse.org/sites/default/files/2021-

02/FH_TransnationalRepressionReport2021_rev020221_CaseStudy_China.pdf (19.04.2025).

92. Frenkel, S., Bergman, R., Saad, H. How Israel Built a Modern-Day Trojan Horse: Exploding Pagers. The New York Times 20.09.2024. – https://www.nytimes.com/2024/09/18/world/middleeast/israel-exploding-pagers-hezbollah.html (18.11.2024).
93. Friedman, T. L. Foreign Affairs; Now a Word From X. The New York Times 02.05.1998. – https://www.nytimes.com/1998/05/02/opinion/foreign-affairs-now-a-word-from-x.html (25.10.2024).
94. FY2025 NDAA: Summary of Funding Authorizations. Congressional Research Service 07.01.2025. – https://crsreports.congress.gov/product/pdf/IN/IN12404 (14.01.2025).
95. Galeotti, M. Spetsnaz: Operational Intelligence, Political Warfare, and Battlefield Role. Marshall Center Security Insight, no. 46, 2020 veebruar. – https://www.marshallcenter.org/en/publications/security-insights/spetsnaz-operational-intelligence-political-warfare-and-battlefield-role-0 (12.02.2025).
96. Gera, V. Western officials suspect Russia was behind a plot to put incendiary packages on cargo planes. Associated Press 05.11.2024. – https://apnews.com/article/russia-poland-germany-sabotage-cargo-planes-b7f559805d7a996dd6aabe8e69041607 (14.11.2024).
97. *Gesetz gegen den unlauteren Wettbewerb – UWG.* – https://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html (10.02.2025).
98. GCHQ. A Brief History of the UKUSA agreement. – https://www.gchq.gov.uk/information/brief-history-of-ukusa (15.01.2025).
99. Gioe, D.V. How America's Allies Boost U.S. Intelligence. And Why Trump Threatens That Cooperation. Foreign Affairs 13.02.2025. – https://www.foreignaffairs.com/united-states/how-americas-allies-boost-us-intelligence (05.03.2025).
100. Goldstein, J. A. Russia's Global Information Operations Have Grown Up. Foreign Policy 04.10.2024. – https://foreignpolicy.com/2024/10/04/russia-propaganda-social-media-platforms-information-warfare/ (14.11.2024).
101. GovInfo. United States Code. – https://www.govinfo.gov/app/collection/uscode (26.04.2025)

102. Grey Dynamics. Senior CIA Ops Officer John Atwell on Culture Change, Working with Five Eyes and Career Advice – Episode 48. 9:10 – The shift towards paramilitarism at CIA after 9/11. – https://podcasts.apple.com/ee/podcast/grey-dynamics/id1637438384?i=1000650118299 (09.04.2025).
103. Hakluyt. – https://hakluytandco.com/ (09.04.2025).
104. Hartley, K. Europe's Defence Industry: An Economic Outlook. Fondation pour la Recherche Strategique 2013. – https://www.frstrategie.org/sites/default/files/documents/publications/notes/2013/201323.pdf (04.03.2025).
105. Heitshusen, V., McGarry, B. W. Congressional Research Service. Defense Primer: The NDAA Process. Uuendatud 06.01.2025. – https://crsreports.congress.gov/product/pdf/IF/IF10515 (15.01.2025).
106. Hindre, M. Kuusk kaitseministeeriumist: sisekontrolli pole ja julgeolek on alamehitatud. ERR 04.02.2025. – https://www.err.ee/1609595108/kuusk-kaitseministeeriumist-sisekontrolli-pole-ja-julgeolek-on-alamehitatud (04.03.2025).
107. International Criminal Court. The States Parties to the Rome Statute. – https://asp.icc-cpi.int/states-parties (09.04.2025).
108. Javers, E. Spies and Co. The New York Times 24.10.2012. – https://www.nytimes.com/2012/10/25/opinion/corporate-espionage-american-style.html (13.02.2025).
109. Jordan, D. China and Philippines trade blame as ships collide. BBC 13.08.2024. – https://www.bbc.com/news/articles/cx2erwedxz5o (14.11.2024).
110. Juurvee, I., Mattiisen, A.-M. The Bronze Soldier Crisis of 2007. Revisiting an Early Case of Hybrid Conflict. ICDS (21.08.2020). – https://icds.ee/en/the-bronze-soldier-crisis-of-2007/ (20.04.2025).
111. Kaitseministeerium. Eesti kaitsetööstuspoliitika „Koostöös loodud kaitsevõime". 2021.
112. Kaitseministeerium. Kaitseministeerium saab kaitsetööstuse asekantsleri. (03.02.2025). – https://kaitseministeerium.ee/et/uudised/kaitseministeerium-saab-kaitsetoostuse-asekantsleri (04.02.2025).
113. Kaitseministeerium. Kaitsetööstuspoliitika. – https://www.kaitseministeerium.ee/et/eesmargid-tegevused/kaitsetoostuspoliitika (05.03.2025).

114. Kaitsepolitseiameti aastaraamatu esitlus 2025. – https://www.youtube.com/watch?v=dNq3KR8XyCU (21.04.2025).
115. Kaitsepolitseiameti aastaraamat 2007.
116. Kaitsepolitseiamet. GRU jaoks luuranud mees mõisteti süüdi Eesti Vabariigi vastases kuriteos. (08.05.2024). – https://kapo.ee/et/content/gru-jaoks-luuranud-mees-m%C3%B5isteti-s%C3%BC%C3%BCdi-eesti-vabariigi-vastases-kuriteos/ (02.03.2025).
117. Kaitsepolitseiamet. Luure ja vastuluure. – https://kapo.ee/et/content/luure-ja-vastuluure/ (11.02.2025).
118. Kaitsepolitseiamet. Majandusjulgeolek. – https://kapo.ee/et/content/majandusjulgeolek/ (04.03.2025).
119. Kaitsepolitseiamet. Majandusjulgeolek. (09.09.2011). – https://web.archive.org/web/20110909120145/http:/www.kapo.ee/est/toovaldkonnad/majandusjulgeolek.
120. Kaitsepolitseiamet. Majandusjulgeolek. (21.10.2020). – https://web.archive.org/web/20201021122615/https:/www.kapo.ee/et/content/majandusjulgeolek.html.
121. Kaitsepolitseiamet. Majandusjulgeolek. (10.04.2021). – https://web.archive.org/web/20210410221810/https:/kapo.ee/et/content/majandusjulgeolek.html.
122. Kaitsepolitseiamet. Mida peaks teadma tööstusspionaažist? (09.09.2011). – https://web.archive.org/web/20110909092048/http:/www.kapo.ee/est/hea-teada/toostusspionaaz.
123. Kaitsepolitseiamet. Mida peaks teadma tööstusspionaažist? (03.11.2019). – https://web.archive.org/web/20191103141731/https:/www.kapo.ee/et/content/mida-peaks-teadma-t%c3%b6%c3%b6stusspionaa%c5%beist.html (08.02.2025).
124. Kaitsepolitseiamet. Tule tööle. – https://kapo.ee/et/kandideeri/ (06.03.2025).
125. Kaitsepolitseiamet. Valik kohtulahendeid. Riigivastased kuriteod. – https://kapo.ee/et/content/riigivastased-kuriteod/ (24.04.2025).
126. Kalev, M., Pere, B. Kuidas vabastati Eston Kohver. Suure avaliku lärmi varjus punus KAPO salaja teist plaani. – Eesti Ekspress 04.09.2024.
127. Kaplan, R. D. A New Cold War Has Begun. Foreign Policy 07.01.2019. – https://foreignpolicy.com/2019/01/07/a-new-cold-war-has-begun/ (25.10.2024).

128. Karnau, A. DefSecInteli uus projekt on mehitamata valvepaat. – Postimees 28.02.2025.
129. Kauranen, A. Finland's secret service says frequency of cable incidents is 'exceptional'. Reuters 04.03.2025. – https://www.reuters.com/world/europe/finlands-secret-service-says-frequency-cable-incidents-is-exceptional-2025-03-04/ (04.03.2025).
130. Kidwell, D. Cyber espionage for the Chinese government. U.S. Air Force Office of Special Investigations 17.09.2020. – https://www.osi.af.mil/News/Features/Display/Article/2350807/cyber-espionage-for-the-chinese-government/ (02.03.2025).
131. Klemm, J. (koost). Kaitsepolitseiameti aastaraamat 2020–2021.
132. Klemm, J. (koost). Kaitsepolitseiameti aastaraamat 2021–2022.
133. Klemm, J. (koost). Kaitsepolitseiameti aastaraamat 2022–2023.
134. Kristensen, H. jt. Status of World Nuclear Forces. Federation of American Scientists 29.03.2024. – https://fas.org/initiative/status-world-nuclear-forces/ (14.11.2024).
135. Kroll Inc. – https://www.kroll.com/en (09.04.2025).
136. Kube, C., Gains, M. China has increased military flights near Taiwan by 300%, U.S. general says. NBC News 08.11.2024. – https://www.nbcnews.com/politics/national-security/china-increased-military-flights-taiwan-300-us-general-says-rcna179184 (14.11.2024).
137. Käsper, R. Eriväelase jutud. Intervjuu Kaupo Rosinaga. (14.03.2025). – https://tasku.delfi.ee/podcast/ff0c1df9-082d-414f-b06d-f48decd50f45/ (04.03.2025).
138. Külauudised. Julgeolekuoht Narva-Jõesuus vajab kiiret kõrvaldamist. (27.03.2022). – https://kylauudis.ee/2022/03/27/julgeolekuoht-narva-joesuus-vajab-kiiret-korvaldamist/ (04.03.2025).
139. Laur, S. Me vajame sõjaväelise piirivalve taastamist. – Postimees 04.03.2025.
140. Lauri, V. Asjatundjad: Eesti võiks koostöös lähiriikidega toota tiibrakette. ERR (26.04.2025). – https://www.err.ee/1609676501/asjatundjad-eesti-voiks-koostoos-lahiriikidega-toota-tiibrakette (26.04.2025).
141. Lauri, V. Riik tellib Eesti kaitsetööstuselt 100 miljoni eest toodangut Ukrainale. ERR 24.03.2025. – https://www.err.ee/1609642670/riik-tellib-eesti-kaitsetoostuselt-100-miljoni-eest-toodangut-ukrainale (06.04.2025).

142. Lawless, J. MI5 spy chief says Russia and Iran are behind a ‘staggering’ rise in deadly plots. Associated Press 09.10.2024. – https://apnews.com/article/uk-intelligence-mi5-threats-russia-iran-936d7c24d303ffea41f6b1cef7c7b814 (14.11.2024).
143. Leicester, J., Burrows, E. At least 11 Baltic cables have been damaged in 15 months, prompting NATO to up its guard. Associated Press 28.01.2025. – https://apnews.com/article/nato-france-russia-baltic-cables-ships-damage-764964a275530915c2cc5af1125ec125 (04.03.2025).
144. Lieber, D. Israel Missed Signs in Plain Sight Hamas Was About to Attack, First Oct. 7 Probe Finds. The Wall Street Journal 27.02.2025. – https://www.wsj.com/world/middle-east/israel-oct-7-inquiry-report-41ea7efa (04.03.2025).
145. LinkedIn. SensusQ. – https://www.linkedin.com/posts/sensusq_sensusq-estonia-police-activity-7257367591931760640-y9Z9 (06.03.2025).
146. Loizos, C. Hone Capital, a Silicon Valley firm, is being probed by the FBI. Tech Crunch 24.09.2024. – https://www.ft.com/content/d94a5467-ebf9-4992-af13-3e71061707a4 (09.04.2025).
147. Mackinnon, A. jt. How US allies may try to safeguard their intel ops from Trump. Politico 21.02.2025. – https://www.politico.com/news/2025/02/21/us-allies-intel-sharing-trump-00205204 (05.03.2025).
148. Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2024–2030 „Läbivalt IT-vaatlikum Eesti“. – https://www.mkm.ee/sites/default/files/documents/2024-07/Kyberturvalisuse%20strateegia%202024-2030_labivalt_IT_vaatlik_Eesti.pdf (04.03.2025).
149. Mao, L., Yu, D., Tien, D. Taiwan. Trends and Developments. Heavier Punishments for Theft of Taiwanese Core Technologies. (16.01.2025). – https://practiceguides.chambers.com/practice-guides/investing-in-2025/taiwan/trends-and-developments (05.03.2025).
150. Marines. Third Force Reconnaissance Company. – https://www.marforres.marines.mil/Units/4th-Marine-Division/3rd-Force-Reconnaissance-Company-/ (11.02.2025).

151. Martin, A. Estonian spy chief: 'Hybrid schmybrid, what's happening is attacks'. The Record 17.02.2025. – https://therecord.media/estonian-spy-chief-russia-hybrid-attacks-are-real-attacks (05.03.2025).
152. Martin, M. Luure Keskagentuuri endine ohvitser: paljudele tuleb Venemaalt lähtuvat ohtu meelde tuletada. – Postimees 25.01.2025.
153. Martinson, A., Tammai, K., Mikheim, V. The Reality and Challenges of Building Defense Technologies. Startup Day, Tartu, 30.01.2025.
154. Maulny, J.-P. The impact of the war in Ukraine on the European defence market. IRIS, 2023 september. – https://www.iris-france.org/wp-content/uploads/2023/09/19_ProgEuropeIndusDef_JPMaulny.pdf (14.01.2025).
155. Melkozerova, V. Ukrainian spies accuse Kyiv's anti-terror chief of being a Russian mole. Politico 12.02.2025. – https://www.politico.eu/article/ukrainian-spies-russia-federal-security-service-fsb-security-service-of-ukraine-sbu-vasyl-malyuk/ (04.03.2025).
156. „Memorandum Respecting Section 202 (Central Intelligence Agency) of the Bill to Provide for a National Defense Establishment, Submitted by Allen W. Dulles, April 25, 1947," reprinted in National Defense Establishment (Unification of the Armed Services), 80th Cong., 1st sess., U.S. Senate Armed Services Committee Hearings Part 3, 525.
157. MI5. Security Service. Five Eyes launch drive to secure innovation. (17.10.2024). – https://www.mi5.gov.uk/news/five-eyes-launch-drive-to-secure-innovation (15.11.2024).
158. Moody, O. Nato's crystal ball? The programm that claims to predict war. The Times 28.01.2025. – https://www.thetimes.com/world/europe/article/natos-crystal-ball-the-program-that-claims-to-predict-war-qx3c70v8g (04.03.2025).
159. Nagel, H. Hannes Nagel: kõrghariduse alarahastatus on julgeolekuoht. – Postimees 31.03.2022.
160. National Counterintelligence and Security Center. Secure Innovation. Scenarios and Mitigations. – https://www.dni.gov/files/NCSC/documents/SecureInnovation/10252024_Final_Scenarios.pdf (09.04.2025).
161. National Protective Security Authority. – https://www.npsa.gov.uk/secure-innovation (15.11.2024).
162. National Reconnaissance Office. – https://www.nro.gov/ (11.02.2025).

163. NATO. Brussels Summit Communique, 14.07.2021. – https://www.nato.int/cps/en/natohq/news_185000.htm (04.03.2025).
164. NATO. Deterrence and defence, 13.12.2024. – https://www.nato.int/cps/iw/natohq/topics_133127.htm#maintain (14.01.2025).
165. NATO DIANA. – https://www.diana.nato.int/ (10.02.2025).
166. NATO. Emerging and disruptive technologies, 08.08.2024. – https://www.nato.int/cps/fr/natohq/topics_184303.htm?selectedLocale=en (10.02.2025).
167. NATO. Wales Summit Declaration, 05.09.2014. – https://www.nato.int/cps/cn/natohq/official_texts_112964.htm (04.03.2025).
168. Neenan, A. G. Defense Primer: Department of Defense Contractors. Congressional Research Service, 06.06.2024. – https://www.congress.gov/crs-product/IF10600 (09.04.2025).
169. Nicastro, L. A. Defense Primer: The National Technology and Industrial Base. Congressional Research Service. Uuendatud 30.03.2023. – https://crsreports.congress.gov/product/pdf/IF/IF11311/12 (15.01.2025).
170. Nicastro, L. A. The U.S. Defense Industrial Base: Background and Issues for Congress. Congressional Research Service. Summary. Uuendatud 23.09.2024. – https://crsreports.congress.gov/product/pdf/R/R47751 (15.01.2025).
171. Nikolajev, J. Venemaa eemaldatud poide tõttu on Narva jõel piiririkkumiste arv kasvanud. ERR 25.09.2024. – https://www.err.ee/1609471057/venemaa-eemaldatud-poide-tottu-on-narva-joel-piiririkkumiste-arv-kasvanud (04.03.2025).
172. Nisametdinov, I. Keskerakond tahab taastada sõjaväestatud piirivalve ajateenijad piirile saates. ERR 09.10.2018. – https://www.err.ee/867689/keskerakond-tahab-taastada-sojavaestatud-piirivalve-ajateenijad-piirile-saates (04.03.2025).
173. Office of the Director of National Intelligence. Office of the General Counsel. Intelligence Community Legal Reference Book. Digital Edition, 2024. – https://www.dni.gov/files/documents/OGC/IC-Legal-Reference-Book-2024.pdf (11.02.2025).
174. Oidsalu, M., Pulk, M. Postimehe eksperiment paljastas avaliku teabe jagamise „musta turu“. (04.01.2022). – https://arvamus.postimees.ee/7597438/voim-ja-julgeolek-meelis-oidsalu-meinhard-pulk-postimehe-eksperiment-paljastas-avaliku-teabe-jagamise-musta-turu (21.04.2025).

175. Ottis, R. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Cooperative Cyber Defence Centre of Excellence (2008). – https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (02.03.2025).
176. Palts, T. Tõnis Palts: suurim julgeolekuoht on vaenulikus inforuumis elavad venekeelsed. Saage aru, vasturelv on eestikeelne haridus. Eesti Päevaleht 23.02.2022. – https://epl.delfi.ee/artikkel/95992383/tonis-palts-suurim-julgeolekuoht-on-vaenulikus-inforuumis-elavad-venekeelsed-saage-aru-vasturelv-on-eestikeelne-haridus (04.03.2025).
177. Paron, R. Raino Paron: majanduspopulism on oht julgeolekule. Finance Estonia 23.03.2022. – https://financeestonia.eu/raino-paron-majanduspopulism-on-oht-julgeolekule/ (04.03.2025).
178. Pihl, K. „Pealtnägija“: miks ja milliseid riigijuhtide saladusi kaitsepolitsei kogub? ERR 13.03.2019. – https://www.err.ee/919467/pealtnagija-miks-ja-milliseid-riigijuhtide-saladusi-kaitsepolitsei-kogub (06.05.2025).
179. Pinkerton. – https://pinkerton.com/ (09.04.2025).
180. President Donald. J. Trump. Regulating Imports with a Reciprocal Tariff to Rectify Trade Practices that Contribute to Large and Persistent Annual United States Goods Trade Deficits. Executive Orders. The White House 02.04.2025. – https://www.whitehouse.gov/presidential-actions/2025/04/regulating-imports-with-a-reciprocal-tariff-to-rectify-trade-practices-that-contribute-to-large-and-persistent-annual-united-states-goods-trade-deficits/ (03.04.2025).
181. Priest, D.; Arkin, W. M. A hidden world, growing beyond control. The Washington Post (July 19, 2010) – https://www.pulitzer.org/cms/sites/default/files/content/washpost_tsa_item1.pdf (03.01.2024).
182. Prokuratuuri aastaraamat 2017. Inna Ombler: on spioone, kes kinnipidamisest kergendust tunnevad. – https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2017/inna-ombler-spioone-kes-kinnipidamisest-kergendust-tunnevad (04.03.2025).
183. Pulk, M. Siseminister Läänemets „poolsõjaväestab“ piirivalve. – Postimees 20.07.2024.
184. Puusepp, H. (koost). Kaitsepolitseiameti aastaraamat 2018.
185. Puusepp, H. (koost). Kaitsepolitseiameti aastaraamat 2019–2020.

186. Pärt, K. Suurem osa kõrge riskiga julgeolekuohte on mittesõjalised. ERR. (23.04.2025) – https://www.err.ee/1609672700/kristian-part-suurem-osa-korge-riskiga-julgeolekuohte-on-mittesojalised (23.04.2025).
187. Racz, A. Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist. FIIA Report 43. (16.06.2015) – https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf (23.04.2025)
188. Radio Free Europa/Radio Liberty. Bolton: Russian Accident Shows Kremlin's Nuclear Ambitions. (15.08.2019). – https://www.rferl.org/a/bolton-russian-accident-shows-kremlin-nuclear-ambitions/30111305.html (04.02.2025).
189. RIA Novosti. ЦАСТ удвоил награду за добытую в ходе СВО эстонскую боевую платформу. (14.02.2024). – https://ria.ru/20240214/spetsoperatsiya-1927303799.html (03.04.2025).
190. Riigikantselei. Riigikaitse arengukava 2022–2031. Tallinn 2021.
191. Riigi Teataja. – www.riigiteataja.ee (20.04.2025).
192. Roonemaa, H. Vene spiooni sõnum Viru vanglast: mu kodumaa unustas mind. – Postimees 10.10.2018.
193. Saar, J., Kõuts, T. Jüri Saar ja Tarmo Kõuts: Eesti kohus on taastada sõjaväeline piirivalve. – Postimees 13.04.2017.
194. Sabbagh, D. 20,000 Britons approached by Chinese agents on LinkedIn, says MI5 head. The Guardian 17.08.2023. – https://www.theguardian.com/uk-news/2023/oct/17/up-to-20000-britons-approached-by-chinese-agents-on-linkedin-says-mi5-head (02.04.2025).
195. Saturno, J. V. Authorizations and the Appropriations Process. Congressional Research Service. Uuendatud 16.05.2023. – https://crsreports.congress.gov/product/pdf/R/R46497 (15.01.2025).
196. Sazonov, V. jt Sisejulgeoleku hübriidohtude tutvustamine. Sisekaitseakadeemia 2020.
197. Schilis-Gallego, C., Lakhani, N. 'It's a free-for-all': how hi-tech spyware ends up in the hands of Mexico's cartels. The Guardian 07.12.2020. – https://www.theguardian.com/world/2020/dec/07/mexico-cartels-drugs-spying-corruption (11.02.2025).
198. SensusQ. – https://www.sensusq.com/ (04.03.2025).

199. SensusQ. Development programm for Ukrainian state instutions. (01.05.2024). – https://www.sensusq.com/blog/development-program-for-ukrainian-state-institutions (04.03.2025)
200. Sinikalda, M. EKRE soovib taastada sõjaväestatud piirivalve. – Postimees 04.01.2015.
201. Sipher, J. The Car Chase to Nowhere: Hollywood & Spies. Tomorrow's Affairs 05.02.2025. – https://tomorrowsaffairs.com/the-car-chase-to-nowhere-hollywood-spies (06.03.2025).
202. Sotsiaaldemokraadid. Toimetulek on julgeolek! – https://valimised.sotsid.ee/teemad/toimetulek-on-julgeolek/ (04.03.2025).
203. Space Stats. Orbital launches by year. – https://spacestatsonline.com/launches (09.04.2025).
204. Stahl, L. Former agents from Israel's Mossad detail how they build an sold explosive pagers to Hezbollah terrorists. CBS News 22.12.2024. – https://www.cbsnews.com/news/israel-former-mossad-agents-detail-explosive-pagers-hezbollah-terrorists-plot-60-minutes-transcript/ (11.02.2025).
205. State Bureau of Investigation. Former Head of the Security Service of Ukraine (SBU) in the Autonomous Republic of Crimea Oleh Kulinich will stand trial. (03.07.2023). – https://dbr.gov.ua/en/news/kolishnij-nachalnik-golovnogo-upravlinnya-sbu-v-ar-krim-oleg-kulinich-postane-pered-sudom (04.03.2025).
206. Statement by President of the Russian Federation, 21.11.2024. – http://en.kremlin.ru/events/president/news/75614 (05.02.2025).
207. Stockholm International Peace Research Institute. Global military spending surges amid war, rising tensions and insecurity. (22.04.2024). – https://www.sipri.org/media/press-release/2024/global-military-spending-surges-amid-war-rising-tensions-and-insecurity (14.11.2024).
208. Strategic Consortsium of Intelligence Professionals. Code of Ethics. (30.04.2014). – https://web.archive.org/web/20141013115335/https://www.scip.org/CodeOfEthics.php (12.02.2025).
209. Zweig, D., Kang, S. America Challenges China's National Talent Programs. Center for Strategic & International Studies, 2020. – https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/20505_zweig_AmericaChallenges_v6_FINAL.pdf (02.03.2025).

210. Tamm, J. Jaanus Tamm: Eesti kaitsetööstus on valmis järgmiseks arengufaasiks. ERR 25.02.2025. – https://www.err.ee/1609614869/jaanus-tamm-eesti-kaitsetoostus-on-valmis-jargmiseks-arengufaasiks (05.03.2025).
211. Tartu Ülikooli Televisioon. 38. Eesti õigusteadlaste päevade paneeli „Jälitus ja teabehange kriminaalmenetluses“ videosalvestis (26.09.2024). – https://uttv.ee/naita?id=35990.
212. The Times and Sunday Times. „Canada’s old relationship with the US is over,“ says Carney. (27.03.2025). – https://www.youtube.com/watch?v=dgjybooP-pA (04.03.2025).
213. The White House. Fact Sheet: Implementation of Export Control Reform. (08.03.2013). – https://obamawhitehouse.archives.gov/the-press-office/2013/03/08/fact-sheet-implementation-export-control-reform (16.01.2025).
214. Thomson, I. Ex-ASML, NXP staffer accused of stealing chip secrets, peddling them to Moscow. The Register 04.04.2025. – https://www.theregister.com/2025/04/04/amsl_russian_spy/ (09.04.2025).
215. Trends in World Military Expediture, 2023. SIPRI Fact Sheet, 2024 aprill. – https://www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf (14.01.2025).
216. Tuul, M. (koost). Kaitsepolitseiameti aastaraamat 2023–2024.
217. Tuul, M. (koost). Kaitsepolitseiameti aastaraamat 2024–2025.
218. United States Space Force. History. – https://www.spaceforce.mil/About-Us/About-Space-Force/History/ (09.04.2025).
219. University of Tartu. Digital Archive ADA. – https://dspace.ut.ee/browse/subject?scope=581ec471-a7cb-494a-a576-095050b702a4&bbm.page=1&startsWith=spionaa%C5%BE (10.02.2025).
220. United States Intelligence Community. How the IC Works. The Six Steps in the Intelligence Cycle. – https://www.intelligence.gov/how-the-ic-works (13.04.2025).
221. U.S. Department of Energy. The Manhattan Project. Espionage and the Manhattan Project (1940–1945). – https://www.osti.gov/opennet/manhattan-project-history/Events/1942-1945/espionage.htm (06.03.2025).
222. U.S. Department of Justice. Chinese government intelligence officer sentenced to 20 years in prison for espionage crimes, attempting to steal secrets from Cincinnati

company. (16.11.2022). – https://www.justice.gov/usao-sdoh/pr/chinese-government-intelligence-officer-sentenced-20-years-prison-espionage-crimes (02.03.2025).

223. U.S. Department of Justice. Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information. (23.03.2016). – https://www.justice.gov/archives/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive (02.03.2025).

224. U.S. Department of Justice. Chinese National Sentenced for Economic Espionage Conspiracy. (07.04.2022). – https://www.justice.gov/archives/opa/pr/chinese-national-sentenced-economic-espionage-conspiracy (02.03.2025).

225. U.S. Department of Justice. Chinese National Sentences to Prison for Conspiracy to Steal Trade Secrets. (05.10.2016). – https://www.justice.gov/archives/opa/pr/chinese-national-sentenced-prison-conspiracy-steal-trade-secrets (02.03.2025).

226. U.S. Department of Justice. Chinese National Who Conspired to Hack into U.S. Defense Contractor's Systems Sentenced to 46 Months in Federal Prison. (13.07.2016). – https://www.justice.gov/archives/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months (02.03.2025).

227. U.S. Department of Justice. Criminal Resource Manual. Introduction to the Economic Espionage Act. – https://www.justice.gov/archives/jm/criminal-resource-manual-1122-introduction-economic-espionage-act (20.04.2025).

228. U.S. Department of Justice. Former GE Power Engineer Sentenced for Conspiracy to Commit Economic Espionage. (03.01.2023). – https://www.justice.gov/archives/opa/pr/former-ge-power-engineer-sentenced-conspiracy-commit-economic-espionage (02.03.2025).

229. U.S. Department of Justice. Former Senior Adviser for the Federal Reserve Indicted on Charges of Economic Espionage. (31.01.2025). – https://www.justice.gov/opa/pr/former-senior-adviser-federal-reserve-indicted-charges-economic-espionage (13.02.2025).

230. U.S. Department of Justice. Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research. (21.07.2020). – https://www.justice.gov/archives/opa/pr/two-chinese-

hackers-working-ministry-state-security-charged-global-computer-intrusion (02.03.2025).

231. U.S. Department of State. Foreign Terrorist Organizations. – https://www.state.gov/foreign-terrorist-organizations/ (11.02.2025).

232. U.S. Department of State. Office of the Historian. 269. Policy Planning Staff Memorandum. (Washington, 04.05.1948). – https://history.state.gov/historicaldocuments/frus1945-50Intel/d269 (12.02.2025).

233. U.S. House of Representatives. (U) Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden. (15.09.2016). – https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_declassified.pdf (17.04.2025).

234. Vabariigi Valitsus. 2025. aasta riigieelarve ja 2025–2028 riigi eelarvestrateegia. Peamised sõnumid valitsemisalade kaupa. KaM ja SiM. – https://valitsus.ee/2025-eelarve#kam (06.01.2025).

235. Vabariigi Valitsus. Koalitsioonilepe 2024–2027. – https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2024-2027 (14.11.2024).

236. Vabariigi Valitsus. Lähme üle kliimaneutraalsele energiatootmisele tagades energiajulgeoleku. (19.06.2023). – https://valitsus.ee/lahme-ule-kliimaneutraalsele-energiatootmisele-tagades-energiajulgeoleku (04.03.2025).

237. Valiarenko, Y. Nuclear Blackmail of the Russian Federation. Ukrainian PRISM. Foreign Policy Council, 10.04.2024. – https://prismua.org/en/english-nuclear-blackmail-of-the-russian-federation/ (14.11.2024).

238. van der Klundert, M. jt. AIVD: opgepakte werknemer ASML had contact met Russische geheime dienst. NOS 06.02.2025. – https://nos.nl/nieuwsuur/artikel/2554733-aivd-opgepakte-werknemer-asml-had-contact-met-russische-geheime-dienst (09.04.2025).

239. Vene hävitaja narris Alaska kohal pilooti. Helsingin Sanomat/Postimees 02.10.2024. – https://maailm.postimees.ee/8107175/video-vene-havitaja-narris-alaska-kohal-nato-pilooti (14.11.2024).

240. Virkus, S. Intervjuu, vaatlus ja sisuanalüüs. Intervjuu liigid. Tallinna Ülikool (2016). – https://www.tlu.ee/~sirvir/Intervjuu_vaatlus_ja_sisuanals/intervjuu_liigid.html (03.04.2025).

241. Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2018. – https://valisluureamet.ee/doc/raport/2018-et.pdf (26.04.2025).
242. Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2019. – https://valisluureamet.ee/doc/raport/2019-et.pdf (26.04.2025)
243. Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2022. – https://www.valisluureamet.ee/doc/raport/2022-et.pdf (09.04.2025).
244. Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2023. – https://www.valisluureamet.ee/doc/raport/2023-et.pdf (09.04.2025).
245. Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2024. – https://valisluureamet.ee/doc/raport/2024-et.pdf (28.10.2024).
246. Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2025. – https://www.valisluureamet.ee/doc/raport/2025-et.pdf (09.04.2025).
247. Välisluureamet. Tööle välisluureametisse. Luureinfo spetsialist- – https://valisluureamet.ee/toole.html (12.02.2025).
248. Välisministeerium. Eesti toetus Ukrainale. (10.01.2024). – https://www.vm.ee/uudised/eesti-toetus-ukrainale (04.03.2025).
249. Välisministeerium. NATO. Alliansi strateegiline kontseptsioon. – https://www.vm.ee/suhted-teiste-riikide-ja-organisatsioonidega/nato/alliansi-strateegiline-kontseptsioon (14.01.2025).
250. Watling, J., Reynolds, J. The Plot to Destroy Ukraine. Royal United Services Institute for Defence and Security Studies. Special Report, 15.02.2022. – https://static.rusi.org/special-report-202202-ukraine-web.pdf (04.03.2025).
251. Weiss, M. The Hero Who Betrayed His Country. The Atlantic 26.06.2019. – https://www.theatlantic.com/international/archive/2019/06/estonia-russia-deniss-metsavas-spy/592417/ (02.04.2025).
252. Williams, H. Why Russia Is Changing Its Nuclear Doctrine Now. Center for Strategic & International Studies, 27.09.2024. – https://www.csis.org/analysis/why-russia-changing-its-nuclear-doctrine-now (14.11.2024).
253. Winkler, R., Brown, E. Accused Tech Spy Says Rival CEO Recruited Him With Offer to Be Like James Bond. The Wall Street Journal 02.04.2025. – https://www.wsj.com/tech/accused-tech-spy-says-rival-ceo-recruited-him-with-offer-to-be-like-james-bond-793483e1 (03.04.2025).

254. WIPO. Overview of national and regional trade secret systems. Germany. – https://www.wipo.int/documents/d/trade-secrets/docs-overview-country-sheets-germany-final.pdf (20.04.2025).

255. Wong, E. How China Uses LinkedIn to Recruit Spies Abroad. The New York Times 27.08.2019. – https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html (02.04.2025).

## Kasutatud lühendid

| | |
|---|---|
| art | artikkel |
| CFR | *Code of Federal Regulations* (föderaalregulatsioonide koodeks) |
| CIA | *Central Intelligence Agency* (Luure Keskagentuur) |
| DIB | *Defense Industrial Base* (kaitsetööstusbaas) |
| EAR | *Export Administration Regulations* (ekspordikontrolli raamistik) |
| EDTIB | *European Defence Technological and Industrial Base* (Euroopa kaitsetehnoloogia- ja tööstusbaas) |
| EKTL | Eesti Kaitse- ja Kosmosetööstuse Liit |
| EKTÄKS | Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus |
| GeschGehG | *Gesetz zum Schutz von Geschäftsgeheimnissen* (ärisaladuste kaitse seadus) |
| HSL | Hiina sõjaväeluure |
| ITAR | *International Traffic in Arms Regulations* (rahvusvahelise relvakaubanduse regulatsioonid) |
| JAS | Julgeolekuasutuste seadus |
| KAPO | Kaitsepolitseiamet |
| KKS | Kaitseväe korralduse seadus |
| NDAA | *National Defense Authorization Act* (riigikaitse volitusseadus) |
| NTIB | *National Technological Industrial Base* (rahvuslik tehnoloogiatööstusbaas) |
| PPA | Politsei- ja Piirivalveamet |
| RelvS | Relvaseadus |
| RHS | Riigihangete seadus |
| RIA | Riigi Infosüsteemi Amet |
| RiKS | Riigikaitse seadus |
| RSVS | Riigisaladuse ja salastatud välisteabe seadus |
| SBU | Ukraina julgeolekuasutus |

| | |
|---|---|
| StGB | *Strafgesetzbuch* (Saksamaa karistusseadustik) |
| StrKS | Strateegilise kauba seadus |
| U.S.C | *United States Code* (föderaalkoodeks) |
| USML | *United States Munitions List* (Ameerika Ühendriikide laskemoonanimekiri) |
| UWG | *Gesetz gegen den unlauteren Wettbewerb* (ebaausa konkurentsi vastane seadus) |