Kiberdrošība no stratēģiskā skatpunkta, jeb kādēļ maziem un vidējiem komersantiem būtu jāinvestē kibernoturībā?

Vitālijs Rakstiņš

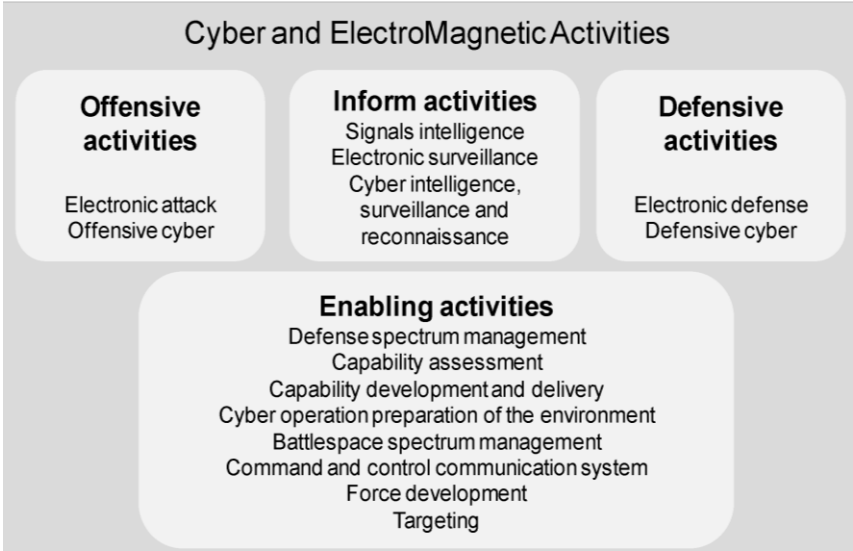
Rīgas Stradiņa universitāte

Kas ir kiberdrošība?

Kiber no tehniskā jēdziena uz visaptverošu un stratēģisko

“**Digitālā drošība**” - tādu ekonomisko un sociālo risku pārvaldība, kuri izriet no informācijas un komunikācijas tehnoloģiju un datu pieejamības, integritātes un konfidencialitātes (OECD)

“**Kiberdrošība**” - ir instrumentu, politikas, drošības konceptu un vadlīniju, risku vadības, rīcības, apmācības, pieredzes un tehnoloģiju kopums, kuru var izmantot elektroniskās vides, tās organizēšanas un lietotāju resursu aizsardzībai (ITU definīcija) Kiberdrošība - asociējās ar tādām koncepcijām kā “kiberkarš”, “kiberaizsardzība” vai “kiberietekme” un netiek lietots ekonomikas aprindās (OECD). “kiberdrošība” ir darbības, kas jāveic, lai aizsargātu tīklu un informācijas sistēmas, to lietotājus un citas personas, kuras skar kiberdraudi (Kiberdrošības akts, Nacionālās kiberdrošības likums)



“**Informācijas drošība**” - tehniskās pārvaldības termins, kas primāri atspoguļo tehniskās kopienas viedokli (piemēram, ISO/IEC 27000). Turklāt termins ir neskaidrs starptautiskajā kontekstā, jo dažas valstis tajā iekļauj arī pret dezinformāciju, ietekmi un informācijas manipulācijām vērstu politiku.

“**tīklu un informācijas sistēmu drošība**” (NIS2, Nacionālās kiberdrošības likums) ir tīklu un informācijas sistēmu spēja noteiktā uzticamības līmenī pretoties jebkurām darbībām, kas apdraud glabājamo vai pārraidāmo, vai apstrādājamo datu pieejamību, autentiskumu, integritāti vai konfidencialitāti vai minēto tīklu un informācijas sistēmu piedāvātos vai ar to starpniecību pieejamos saistītos pakalpojumus.

Kas ir noturība?

- organizācijas spēja ilgtspējīgi uzturēt un nodrošināt plānotos biznesa procesus / rezultātus, neskatoties uz notikumiem digitālajā vidē;

- **spējas** sagatavoties dažādiem satricinājumiem vai katastrofām (**all-hazard approach**), pretoties tiem, reaģēt uz tiem (un arī pielāgoties, transformēties krīzē) un atgūties no tiem;

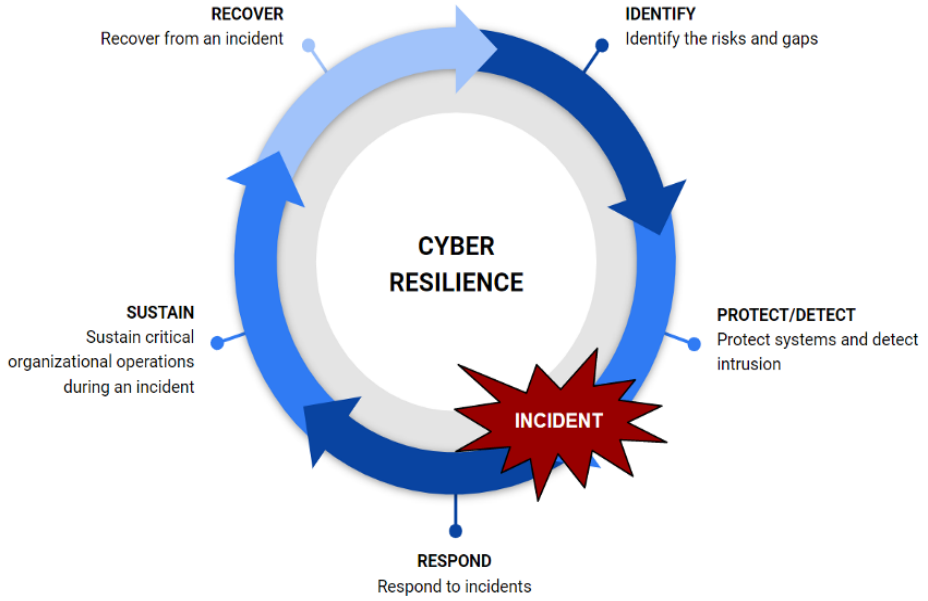
- Nevienu objektu / sistēmu nav iespējams aizsargāt no dažādu veidu apdraudējumiem ilglaicīgi / visu laiku!

- Fokuss uz kritisko pakalpojumu / funkciju nepārtrauktību;

- Noturība ir **aktīvā rīcība** adaptācijai un transformācijai;

- Noturība nav konkrēta riska novēršanas stratēģijā, drīzāk integritātes stiprināšana pret daudziem apdraudējumiem;

- Nepieciešams veidot spējas, kas nav balstītas tikai uz riskiem, bet veidot arī iekšējās spējas/rezerves (scenāriju pieeja), lai spētu funkcionēt jebkādā krīzē



Apdraudējums

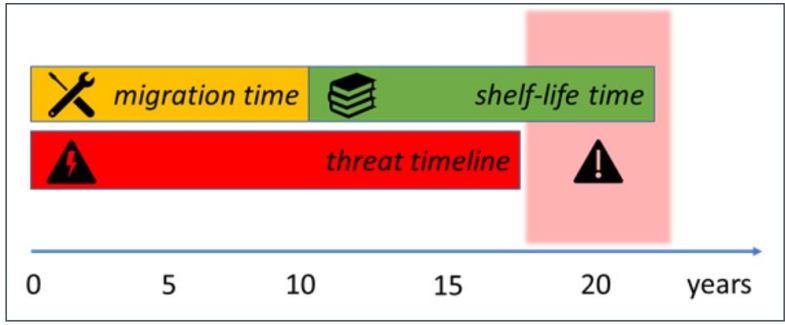
- Ievainojamības (Attack Surfaces) eksponenciāli pieaug;
- graujošo tehnoloģiju (ģeneratīvā mākslīgā intelekta, kvantu tehnoloģiju) nekontrolētā izplatība;
- piegāžu ķēžu drošība / noturība
- Aktoru skaits turpina pieaug, t.sk. kibernoziegumi kā pakalpojums (Cybercrime as a Service)

Globālie riski (2 gadu griezumā)

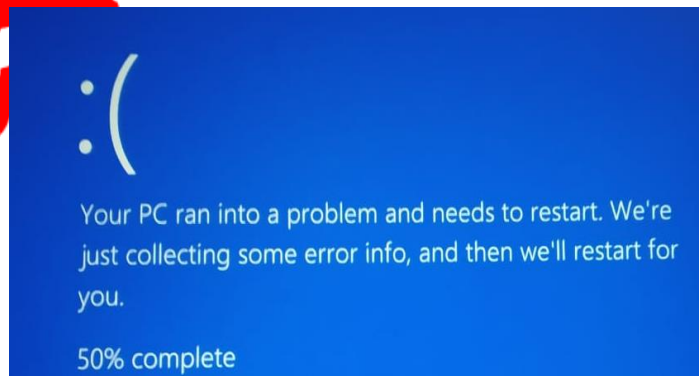
polycrisis

[poli-krai-sis] *noun*

the simultaneous occurrence of several catastrophic events



Kvantu tehnoloģiju ietekme



polycrisis

[poli-krai-sis] *noun*

the simultaneous occurrence of several catastrophic events

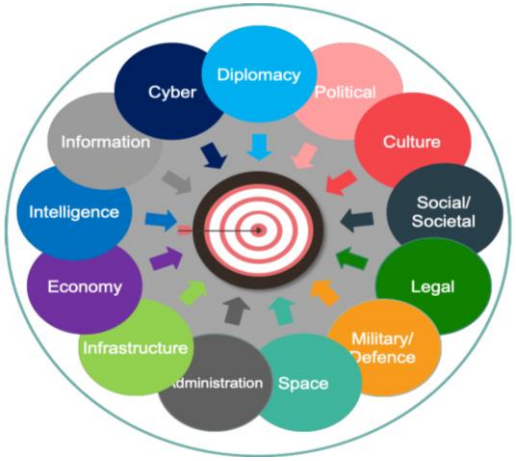
Polikrīzes

Permacrisis

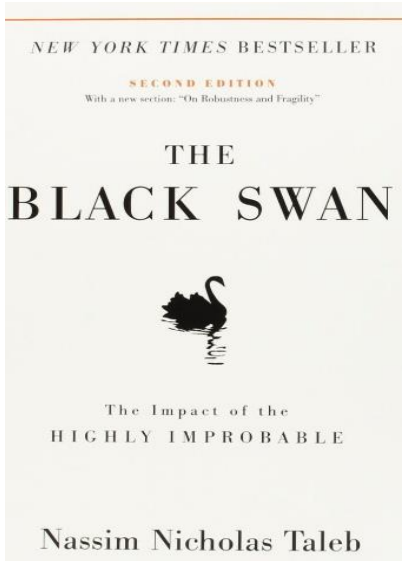
(noun): [ˈpɜːməˌkraɪsɪs]

1. An extended period of instability and insecurity, especially one resulting from a series of catastrophic events.

Pastāvīgā krīze



Augstās intensitātes hibrīda uzbrukumi

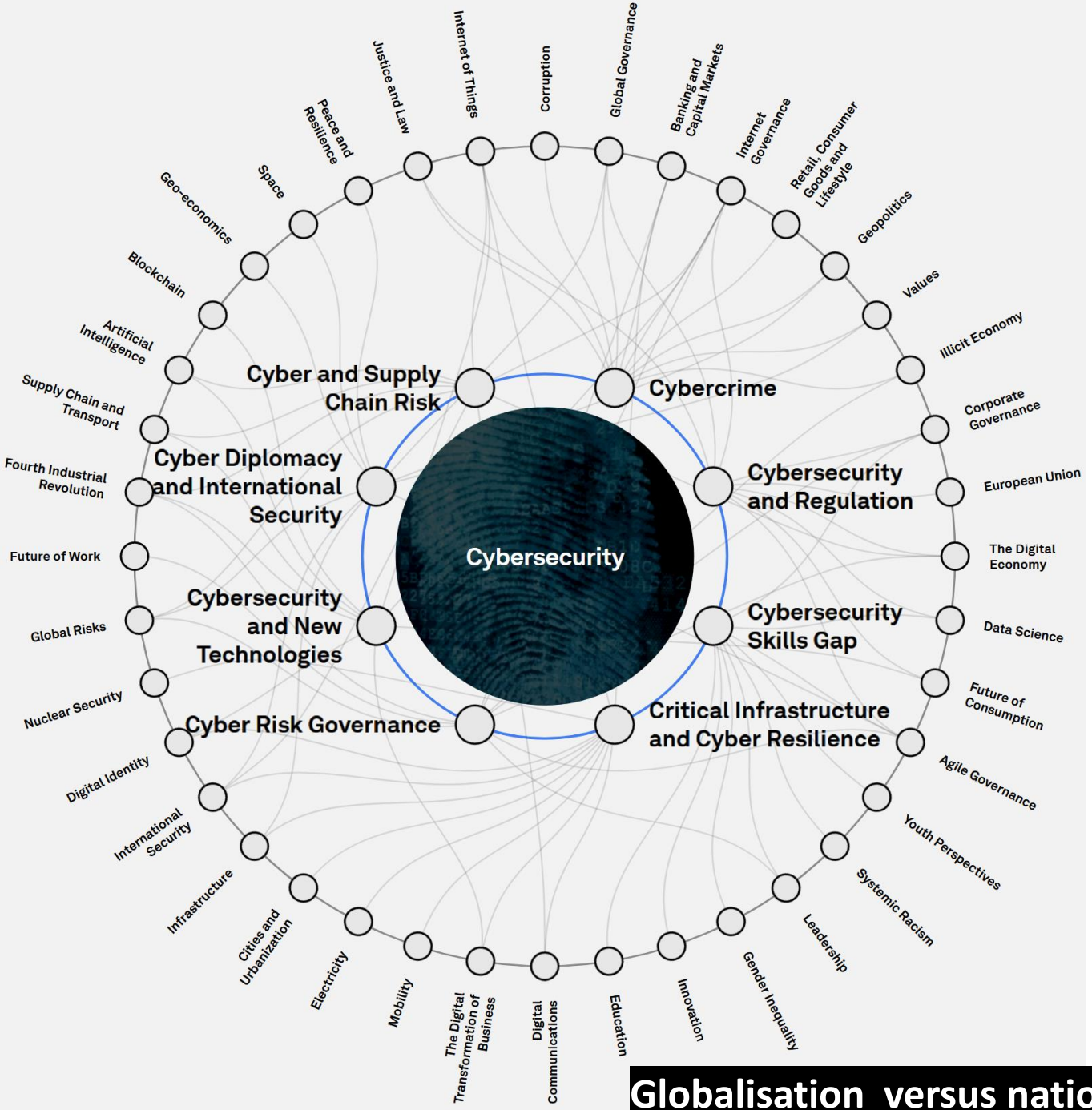


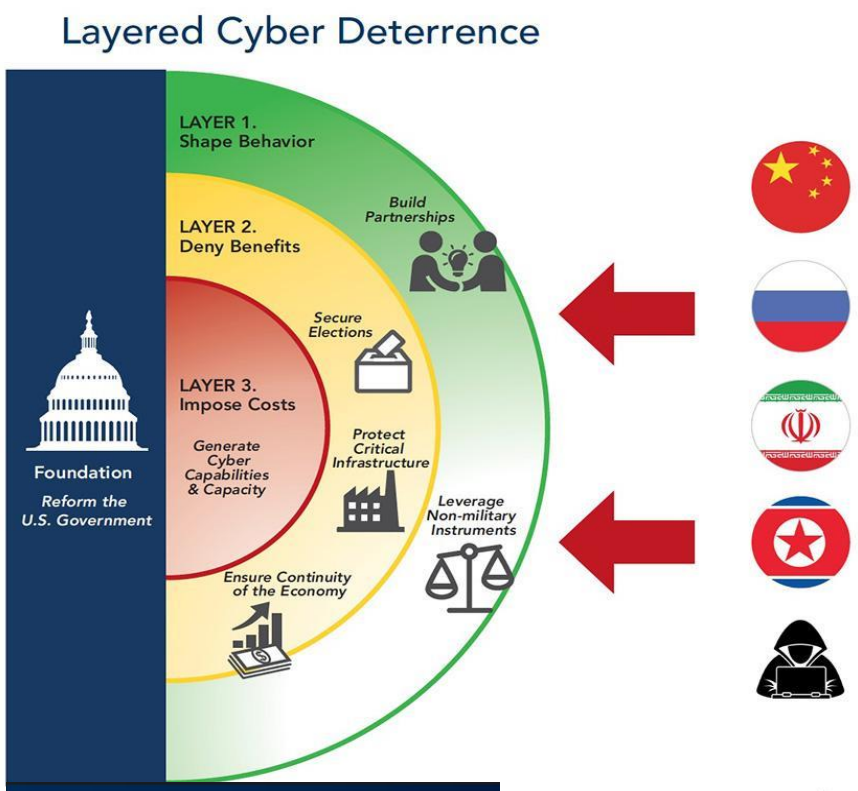
Cilvēktiesības, brīvības, brīvais tirgus ….

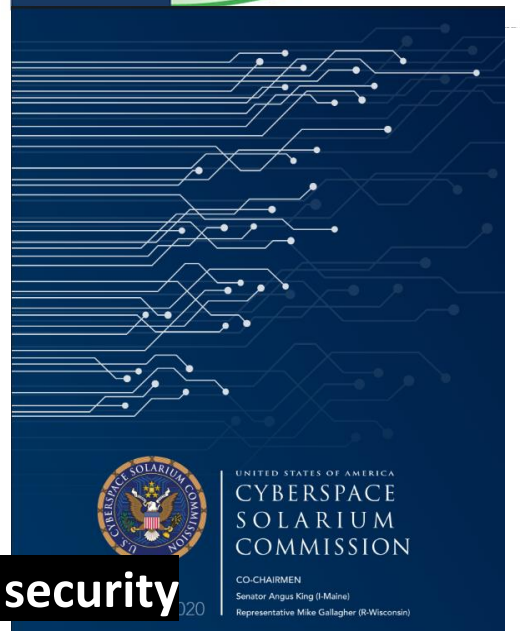
2024.gads

Ierobežojumi un ārkārtas pilnvaras krīžu pārvarēšanai

- **Funkciju deleģēšana** privātajam sektoram
- Lielākā **atbildība** (gan CEO, gan lietotājiem)
- Lielāki **ierobežojumi un pienākumi**
- Like-minded partnerības v. kvantu diplomātija
- Nacionālā drošība v. globalizācija







Globalisation versus national security

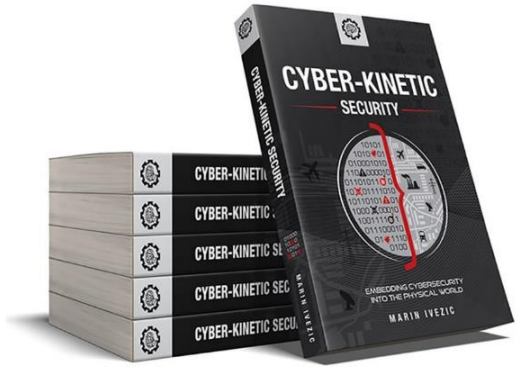
Daudzslāņu kiber **atturēšana**:

[1] ietekmēt uzvedību

[2] liegt labumus (no kiberuzbrukumiem)

[3] palielināt sankcijas / cenu par nodarījumu

Instrumentārijs



[1] Kompleksa risinājumi: kinetiskie + digitālie + DNP

[2] Security by design

[3] Duty of care

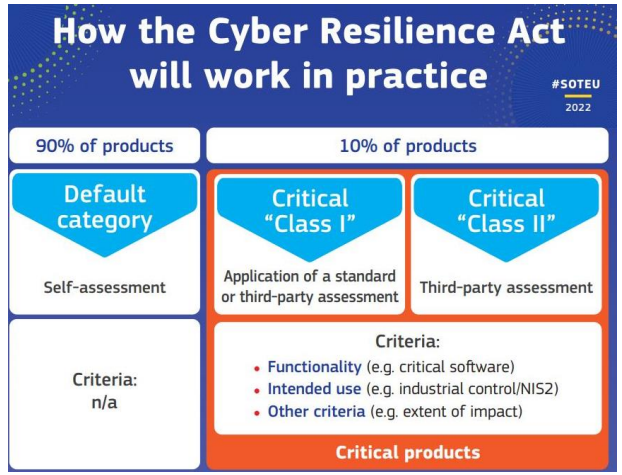
Dzīves cikla nodrošinājums
Pienākums iestrādāt final update

THE Clean NETWORK

Clean CARRIER | Clean APPS | Clean STORE
Clean CLOUD | Clean CABLE | Clean PATH

I. Riska scenāriji, kas saistīti ar nepietiekamiem drošības pasākumiem
II. Ar 5G piegādes ķēdi saistītie riska scenāriji
III. Riska scenāriji, kas saistīti ar galveno apdraudētāju *modus operandi*
IV. Riska scenāriji, kas saistīti ar 5G tīklu un citu kritiski svarīgu sistēmu savstarpējo atkarību
V. Ar galalietotāju iekārtām saistīti riska scenāriji

[4] Piegāžu drošība / stratēģiskās atkarības



[5] Security by Demand

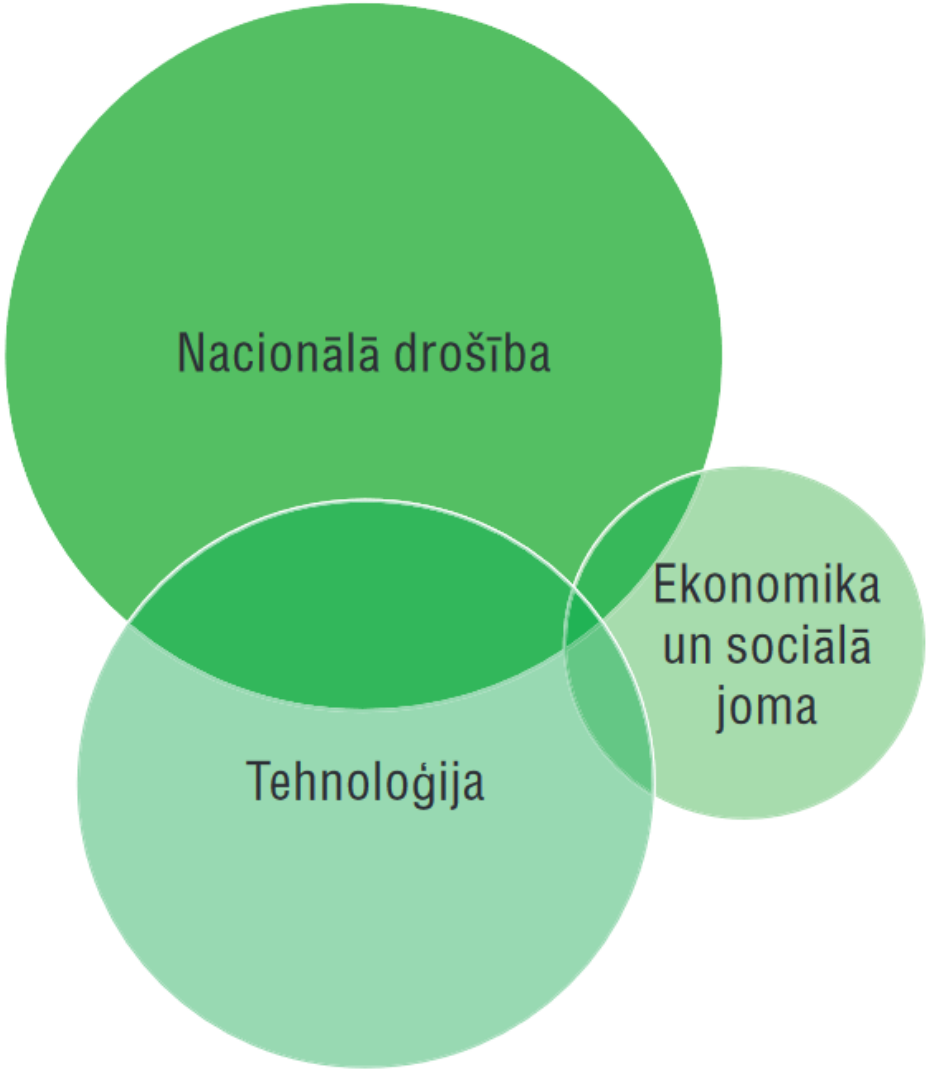
Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību (2017)

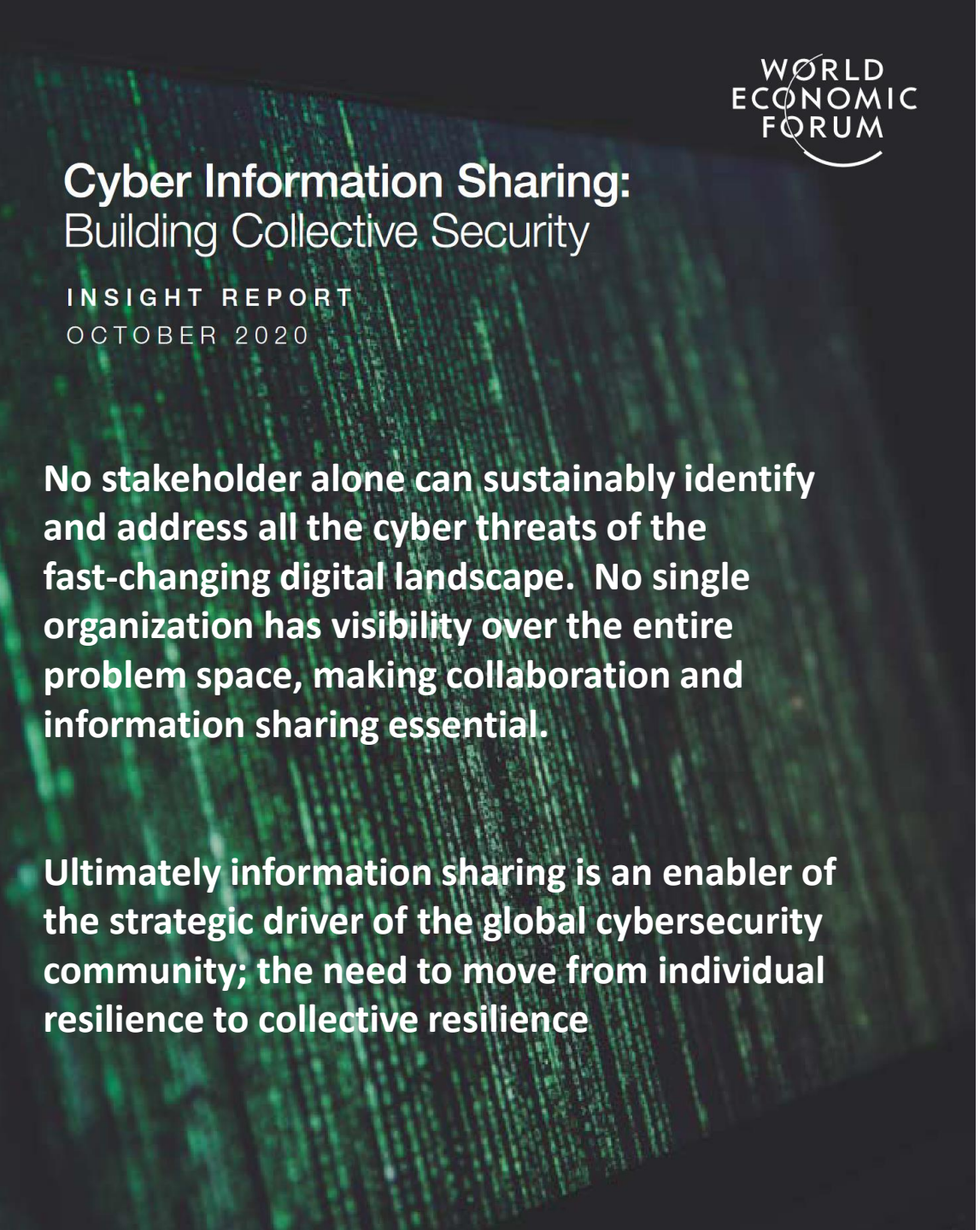
- Stabilākas un efektīvākas struktūras
- **Vienotais kiberdrošības tirgus:**
    - **ES kiberdrošības sertifikācijas satvars:**
        - **drošība kritiskās vai augsta riska līmeņa lietotnēs**
        - **kiberdrošība digitālajos produktos, tīklos, sistēmās un pakalpojumos**
        - **integrētās drošības metožu izmantošana lietu interneta ierīcēm**
    - **Nozaru kiberdrošības prasības (finanšu, enerģētika, transports, veselība…)**
    - atbildība / zaudējumi
    - ārvalstu tiešo investīciju ES pārbaude
- Noturība (ātra ārkārtas reaģēšana, krīzes pārvarēšanas mehānismi)
- Pētniecība un zinātne
- Kiberprasmes
- Kiberhigiēnas un izpratnes veicināšana
- Atturēšana no kibernoziegumiem
- Starptautiskā sadarbība

IZAICINĀJUMS: visu iniciatīvu (starptautisko, ES, nacionālo, industrijas) koordinācija / savietojamība

Latvijas kiberdrošības stratēģija (2023.-2026.) izvirzīti pieci rīcības virzieni:

- Kiberdrošības **pārvaldības** pilnveidošana;
- Kiberdrošības **noturības** stiprināšana (DNP, drošības prasības un standarti, sertifikācija, eID u.tml.);
- Sabiedrības **izpratne, izglītība** un pētniecība;
- Starptautiskā **sadarbība**;
- Kibernoziedzības novēršana un apkarošana.





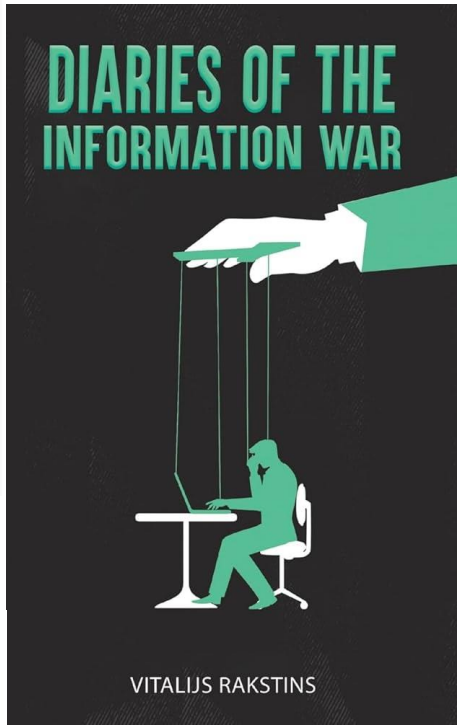
Izaicinājumi

- Graujošo tehnoloģiju nekontrolētā izplatība (neprognozējamie kaskadējošie efekti);
- Laiks (viss attīstās ļoti ātri, regulējums un standarti nevar paspēt);
- Daudz standartu (t.sk. nesavienojamo / outdated);
- Nefiskālās barjeras/ ekonomiskais karš;
- Pārrobežu standartu (sertifikācijas) savstarpējā atzīšana;
- Sertifikācijas standarti ierīcēm un pakalpojumiem;
- Kompleksa risinājumi (kinetiski / digitāli / DNP);
- Globālais kvalificēto speciālistu trūkums (t.sk. kvalifikācijas atzīšana);
- Piegāžu drošība: apakšnieki, trešās puses, u.c.
- Informācija apmaiņa - gan pārrobežu, gan iekšēji (datu standarti / savietojamība un ierobežojumi, clean data);
- Pārrobežu sadarbība;
- PPP drošības jautājumos
- Kvantu diplomātija / iespējas apiet ierobežojumus;
- Sadarbības kultūra!

Kā motivēt MVU investēt kiberdrošībā un noturībā?

- Nepieciešams investēt:
  - lai būtu daļa no starptautiskās ekosistēmas
  - lai kvalificētos publiskiem iepirkumiem;
  - Lai kvalificētos apdrošināšanai u.tml.
- Piegādātājs / apakšnieks «vienmēr būs vainīgs»;
- Daļa no kiberdrošības pasākumiem neprasa lielus resursus;
- Reputācija un sociāla atbildība

Cilvēks joprojām centrā



- Uz cilvēku orientēta pieeja kiberdrošībai (human-centric approach to cyber security);
- Sistēmas darbojās milisekundēs, bet lemj cilvēki;
- Sadarbības kultūra = cilvēku sadarbība;
- Sabiedrības plašāks akcepts kiberdrošības ierobežojumiem;
- Atbildības personificēšana;
- Indivīdiem pašiem jāuzņemas lielāka atbildība par savu kiberdrošību;
- Atturēšanas efekts (visas sabiedrības noturība liedzot sasniegt uzbrucēja mērķus (“kopīga atbildība”).


MANA LATVIJA
MANA ATBILDĪBA