Державна служба спеціального зв'язку та захисту інформації України

CERT-UA

Organizational / Technical Model of State CyberSecurity in Ukraine: Critical Informational Infrastructure CyberProtection & CyberIncidents Response

Mykola Khudyntsev

State Center of CyberDefense
State Service of Special Communication and Information Protection of Ukraine

Odesa – 2019

Regulatory Base

Decree of the President of Ukraine № 96/2016 of 15.03.2016
"On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 " On the Strategy of Cybersecurity of Ukraine "

Decree of the President of Ukraine No. 32/2017 of 02/13/2017 "On the decision of the National Security and Defense Council of Ukraine dated December 29, 2016 " On threats to cybersecurity of the state and urgent measures for their neutralization "

Decree of the President of Ukraine No. 183/2017 dated 11.07.2017
"On the decision of the National Security and Defense Council of Ukraine dated 10 July 2017 " On urgent measures to finance the needs of Ukraine's national security and defense in 2017 "

Decree of the President of Ukraine No. 254/2017 dated August 30, 2017
"On the decision of the National Security and Defense Council of Ukraine dated July 10, 2017" On the state of implementation of the decision of the National Security and Defense Council of Ukraine dated December 29, 2016 "On threats to cybersecurity of the state and urgent measures for their neutralization", introduced by the Decree of the President of Ukraine from February 13, 2017, No. 32 "

Decree of the President of Ukraine No.283 / 2017 dated September 25, 2017
"On the decision of the Council of National Security and Defense of Ukraine of September 13, 2017" On the Concept of Reform and Further Development of the State Management System in Conditions of Emergency and in a Special Period ”

Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine"
No.2163-19 dated 05.10.2017

Next Regulatory Steps (Road-Maps for CI & CII)

- new regulatory documents (laws, decrees, directives)
- normative and technical documentation for steakholders (standards, orders, recommendations)
- typical design and project documentation for customers (typical technical requirements, tasks, design solutions, playbooks)

Next Technical Steps (Infrastructure Projects)

National Telecommunication Network (NTN)

State authority's system for protected access to the Internet (SSAI = Trusted Internet Connection)

Unified basic and reserve secure data-centers for storage of the state electronic information resources data (CCSD)

Systems of protected mobile communication (SPMC) & Public Safety System (PSS)

Cybersecurity system of state information resources and objects of critical information infrastructure (CSS SIR CII)

Organizational / Technical Model (OTM) of Cybersecurity and Cyberprotection

Top Tasks

Digital Infrastructure

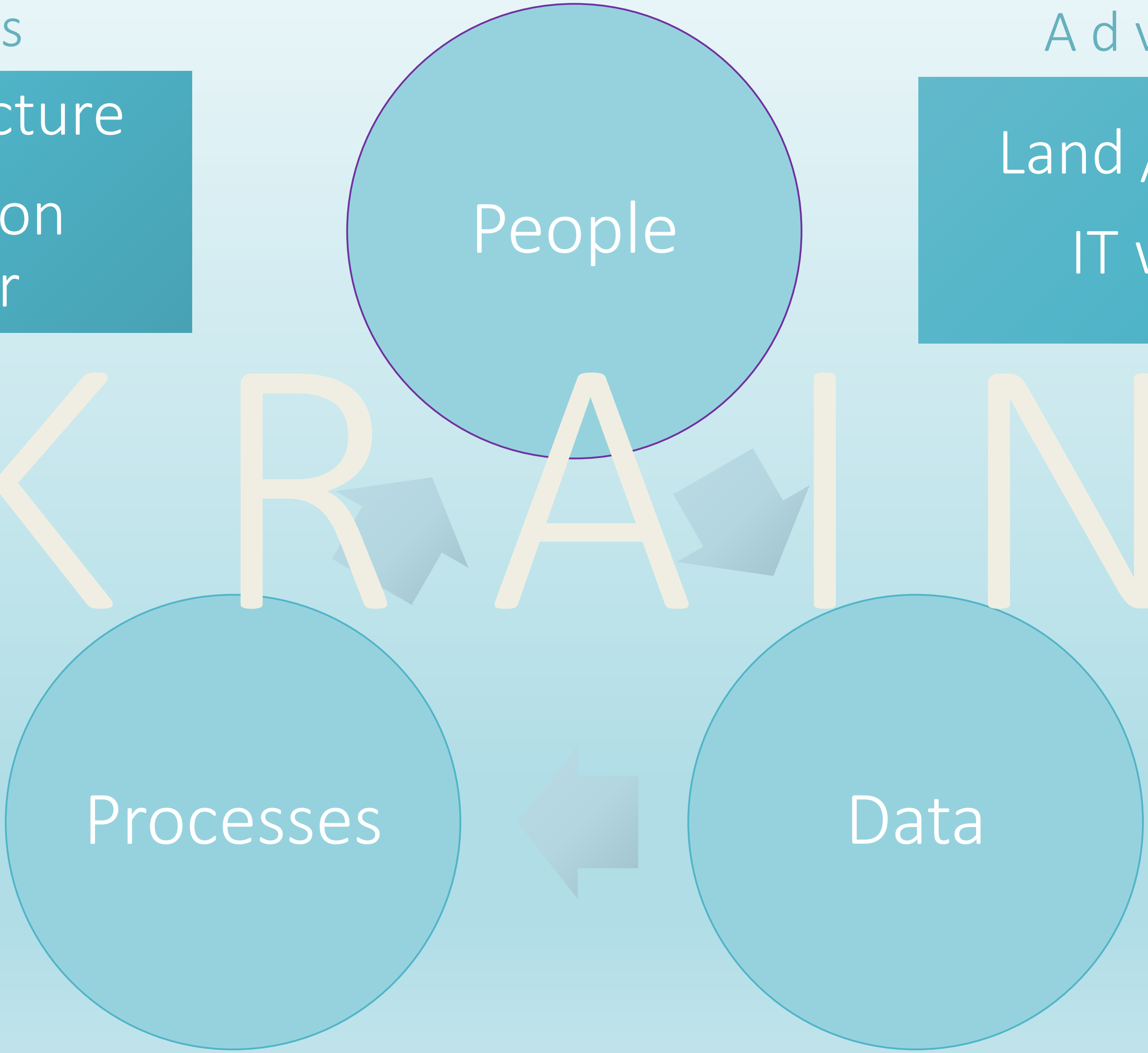
CyberProtection in AgriSector

Advantages

Land / Agriculture

IT workforce

UKRAINE



Organizational / Technical Model (OTM) of State Cybersecurity

OTM's **description levels**:

- regulatory (normative)
- technical regulation
- organizational (structural)
- technical (principle)

OTM's description forms:

- conceptual scheme
- ecosystem
- organizational / technical model
- organizational scheme (HLD)
- principal scheme (LLD)

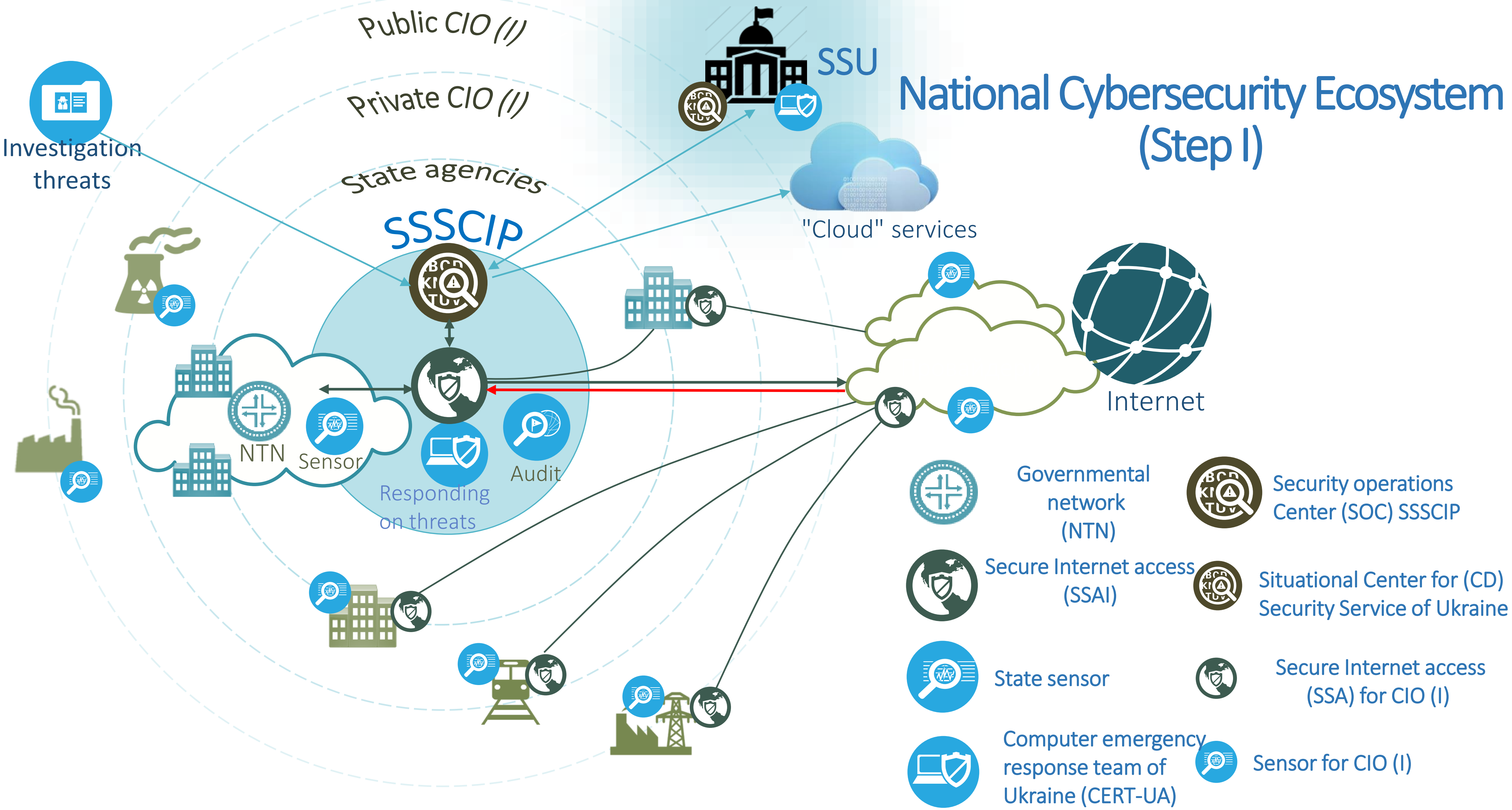
Organizational / Technical Model (OTM) of Cyber (current and *perspective*):

- National security operation centers (SOC)
- Governmental computer emergency response team (CERT)
- National security information and event management (SIEM)
- sources (streams) of telemetric data:
  - external streams (*optimized* and unoptimized)
  - access nodes for external (incl. global) networks
  - sensors (passive and *active*) and *terminal agents*
  - *video telemetry, open (incl. global) network & social telemetry*
- *systems of data processing, aggregation and storage, knowledge warehouse,* technical *and organization interfaces*
- *SCADA-systems & Internet of Things*
- *smart / mesh / grid / metrics / block-chain / DSS systems*

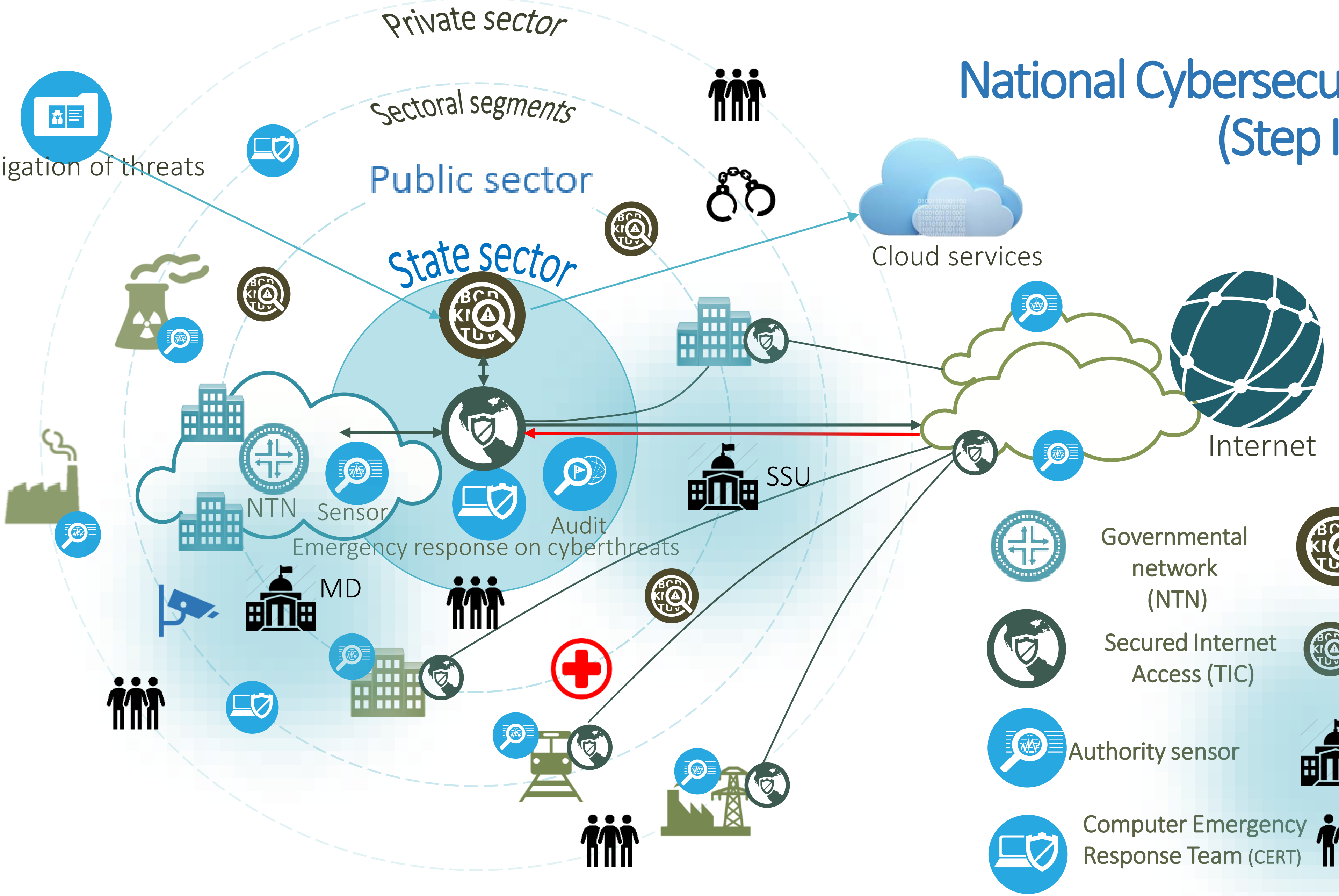
OTM segmentation, structuring and scaling (*current* and perspective):

- *central* and industrial SOC, CERT and SIEM – Automated CyberDefense System (ACDS)
- creating new ACDS and integration with *existing ones*
- streams of telemetric data from *periphery* and cores (of other ACDS)
- *passive* and active monitoring
- threats modeling, intelligence, opposition, like military actions, protection
- authentication and self-authentication of subjects
- smart-SLA-contracts, block-chain technologies
- national private partnership, trusted community, outsourcing
- metrics of cybersecurity systems state changes, metric of trust

National Cybersecurity Ecosystem (Step I)


Public CIO (I)
Private CIO (I)
State agencies
Investigation threats
SSU
"Cloud" services
SSSCIP
NTN
Sensor
Audit
Responding on threats
Internet
Governmental network (NTN)
Security operations Center (SOC) SSSCIP
Secure Internet access (SSAI)
Situational Center for (CD) Security Service of Ukraine
State sensor
Secure Internet access (SSA) for CIO (I)
Computer emergency response team of Ukraine (CERT-UA)
Sensor for CIO (I)

National Cybersecurity Ecosystem (Step II)



✚	Governmental network (NTN)	🔍	Cybersecurity Holder's operations center
🛡	Secured Internet Access (TIC)	🔍	Cybersecurity Holder's situation center
🔍	Authority sensor	🏛	Cybersecurity Holder
🛡	Computer Emergency Response Team (CERT)	👥	New Personnel

National Cybersecurity Ecosystem (Step II) - Challenges & Answers

CYBERWASTE	+++	CYBERHYGIENE	+ –
CYBERINFECTION	+++	CYBERIMMUNITY	– – –
CYBERILLITERACY	++	CYBEREDUCATION	+ – –
CYBERINJURIES	+++	CYBERREABILITATION	– –
CYBERINCIDENT (CI)	+++++	EMERGENCY RESPONSE	+ + – –
CYBERATTACK (CA)	++++	EMERGENCY RESPONSE	+ – – –
CYBERCRIMINALITY	+++	CRIMINAL INTELLIGENCE / CYBERPOLICE	+ – – –
CYBERCRIME	++	CRIMINAL INTELLIGENCE / CYBERPOLICE	+ – – –
ORGANIZED CYBERCRIME	+	SECURITY SERVICE (SSU)	– –
STATE CYBERCRIME	+	SPECIAL EVENTS SSU	– –
CYBERTERRORISM	++	SPECIAL EVENTS SSU	+ – – –
CYBERSPYING	+++	CYBER (COUNTER) INTELLIGENCE	– – –
CYBER/HIBRID WAR	+++++	CYBERDEFENSE AND HACKTIVISM	– – – – –

Cooperation & Initiatives

Topics & Initiatives

- SOC & CERT consultations & cooperation
- Common technical interface
- Hard&Soft ware Solution CyberElection
- Methodical help in regulations (standards, recommendations, SLA, playbooks)
- Telemetry cyberdata exchange
- Development of Global Cybersecurity System for Agricultural Sector (Global AgriCyberData Exchange)
- Workforces events (trainings, conferences, workshops)
- Donor projects & grants in humanitarian field of cyber
- Metrics of Trust in CyberData Exchange Systems

Cooperation (International)

- ITU-T SG17 Security
- Food and Agriculture Organization (FAO)
- EU Programs (Horizon 2020)
- Ukraine-NATO Trust Fond / MITRE
- International Foundation for Electoral Systems (IFES)
- USA Embassy in Ukraine
- National SOCs & CERTs (Netherlands, Israel, USA)
- FIRST / Delta Holland / Thales / TNO
- Global Forum of Cyber Expertise (GFCE)

Cooperation (Local)

- National Coordinated CyberSecurity Center
- National Administration of State Service & SOC & CERT
- E-Government Agency
- CyberSecurity stakeholders (45 memorandums)
- Kyiv National Politechnical University
- National University of Environment & Bioresources

THANK YOU FOR YOUR ATTENTION!

cert.gov.ua
dckz@dsszzi.gov.ua
dckz_hmm@dsszzi.gov.ua