Concept of Organizational / Technical Model of State CyberProtection in Ukraine

Mykola Khudyntsev

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

Kyiv – 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 steak-holders (standards, orders, recommendations)
- typical design and project documentation for customers (typical technical requirements, tasks, design solutions, playbooks)

Current & 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)

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

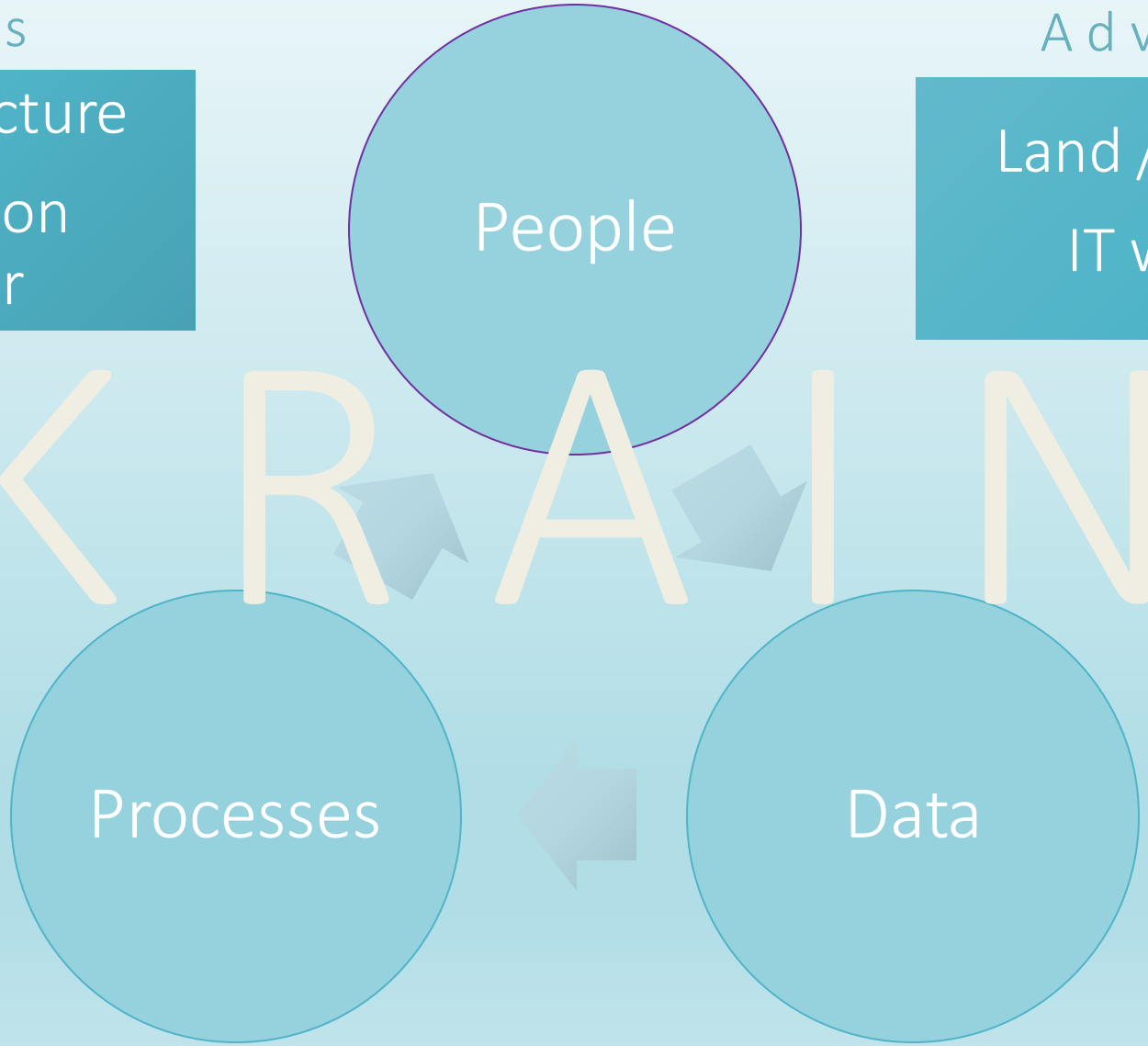
Digital Infrastructure

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)

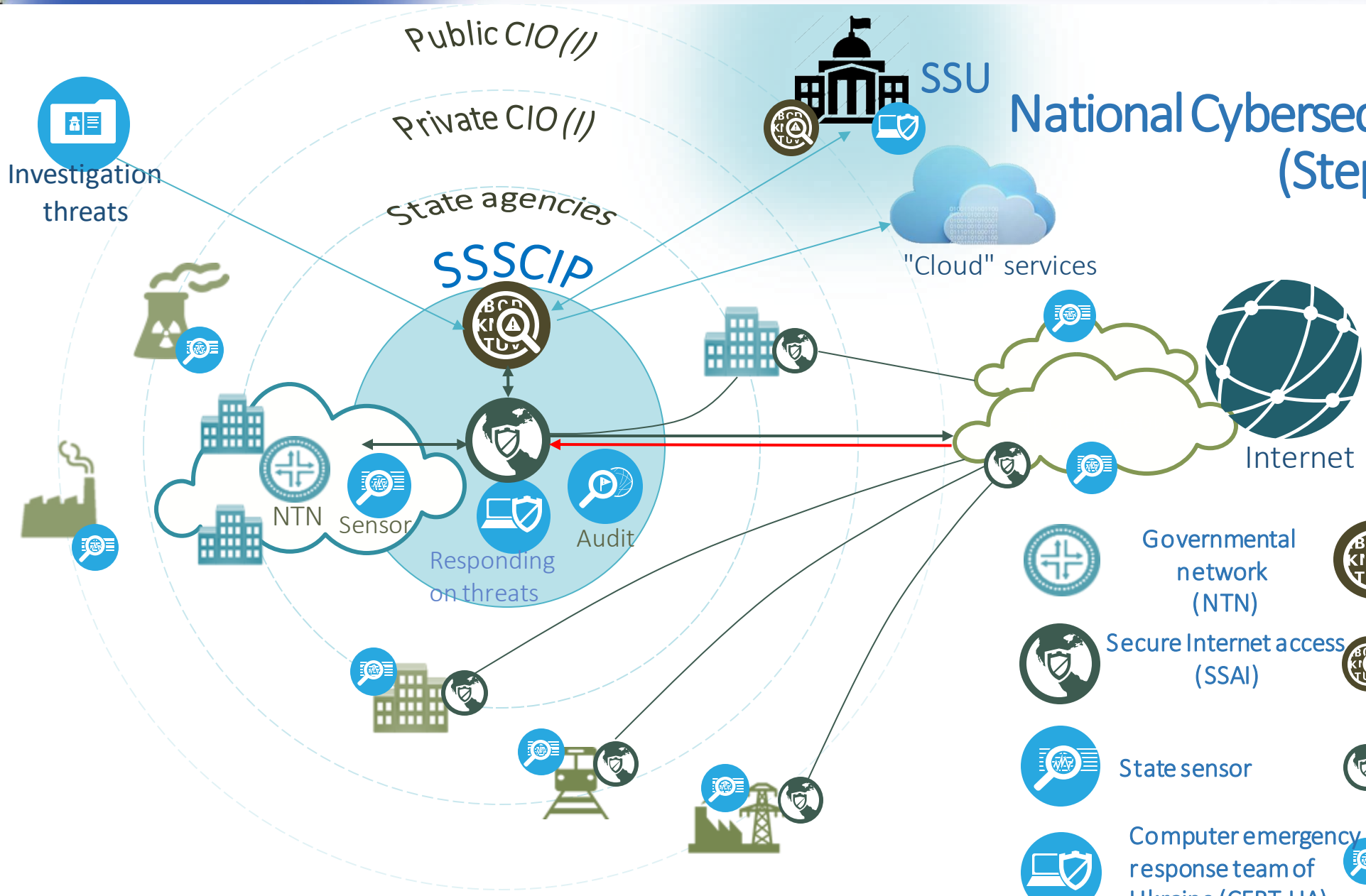
Organizational / Technical Model (OTM) of Cyber (current and *perspective*):

- 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*

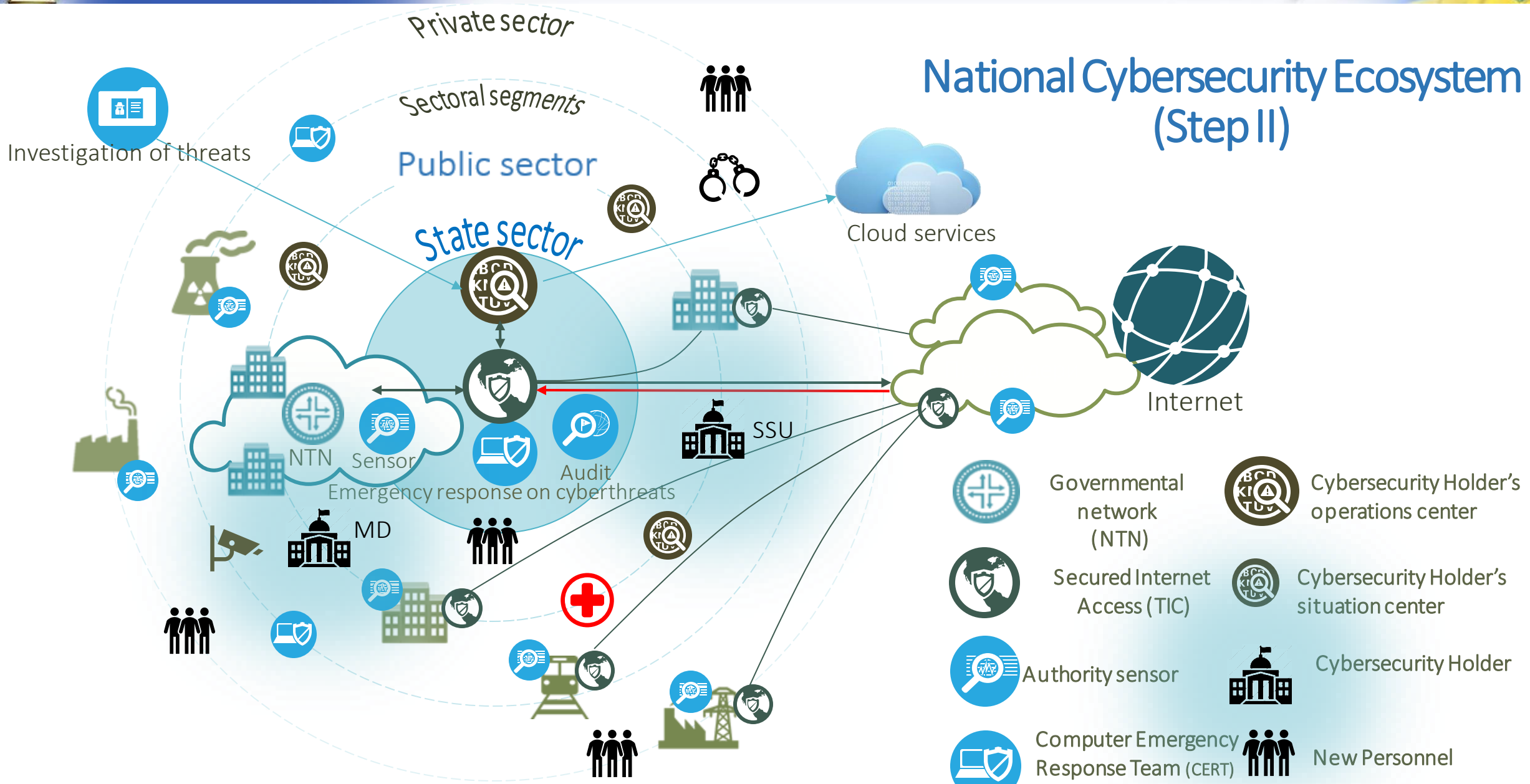
OTM segmentation, structuring and scaling (*current* and perspective):

- *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)



National Cybersecurity Ecosystem (Step II)



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	–––––

Event name	<2018	2018	2019	>2019
Regulatory:				
Doctrine of Cybersecurity of Ukraine (DCU)		no	necessary	
Cybersecurity Strategy of Ukraine (CSU)	yes			
Cybersecurity Strategy of Ukraine (version Next)		no	necessary	
Government plan for CSU implementation	yes	no	necessary	necessary
Plans for Cybersecurity Entities (SCO) for the implementation of CSU	part	part	necessary	
Protocol of interaction of the SCO	no	necessary	necessary	
The procedure for the interaction of the SCO	no	necessary	necessary	
Plans of subjects of subjects of cyber defense SEIR and OKII (CS) concerning the CS	no	necessary	necessary	
Protocol of interaction between the subjects of cyber defense SEIR and OCII (CS)	no	necessary	necessary	
The order of interaction of the CS	no	necessary	necessary	
The Law "On the Basic Principles of Cybersecurity"	yes			
The Law "On Critical Infrastructure and its Protection"		development	expected	
Development of draft legal documents		necessary	necessary	necessary
Development of draft normative and technical documents		necessary	necessary	necessary

Event name	<2018	2018	2019	>2019
Normative and organizational and technical:				
Organizational-technical model (national system) of cyber security		concept	ND	
Organizational and technical model (national system) of cyber defense		concept	ND	
Security Operations Center for Cyber Security (SOC) / Cybercrime Response Center (OCRC)		ND		
Government Emergency Response Team (CERT-UA)		ND		
Sectoral (departmental) centers and teams (groups) of response (SOCs & CERTs)		typical ND		
Organizational and technical requirements (OTR) for a secured Internet access node		ND		
OTR to the cyber defense system of the state information resource and / or object of the critical information infrastructure		ND		
OTR to backup copies of the state information resource and / or object of critical information infrastructure		ND		
Procedures for the functioning of information and telecommunication systems in the field of cybersecurity and cyber defense			NLD / NAD	

Event name	<2018	2018	2019	>2019
Technical:				
Security Operations Center / Operational Center for Cybercrime Response	creation	creation		
The organizational and technical complex of response teams to computer emergency events (CERT-UA)	creation	creation		
Detection and response subsystem at end-point attacks	I step	II step	OSP state budget OCII) own funds	
Subsystem of telemetry collection of information and telecommunication systems (active sensors)	I step	II step	OSP state budget OCII own funds	
Subsystem of collecting telemetry of streams of IP-video data (IP-sensors)			pilot project	expedient
Subsystem of Telemetry Collection of Social Resources Data (SD-Sensors)				pilot project
Subsystem of telemetry collection of SCADA-systems (SS-sensors)			pilot project	expedient
Subsystem of telemetry collection of data on the Internet (IOT-sensors)			pilot project	expedient
Subsystems for telemetry collection smart-, mesh-, grid-, metrics-, dss- AS				pilot project

Event name	<2018	2018	2019	>2019
OSP secure access system to the Internet (SSAI)		SSAI SCCC	other SSAI	other SSAI
Secure Internet access node OSP SCCC Secure	deployment	State SSAI (TIC)	connection of ITS OSP (II step)	connection of ITS OSP (III step)
Sectoral (departmental) centers and teams (groups) of response (SOC & CERT)		I step	II step	III step
State register of cyber incidents (the only interactive cyber incident database)		purchase of equipment	system creation	
Technical interface for interaction with the SCO and the CS		pilot project	implementation	
OSP ITS Register (Register)		reanimation	deployment	
Center for Anti-Virus Protection of National Information Resources (CAPI)	working		modernization	
The only state repository of software and its updates (TSR SU)		necessary	expedient	
The system of indicators for the state of the national cyber security system (SIS NCSS) / the single (universal) system of indicators of cyber threats			expedient	

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)
- 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
- State University of Telecommunication
- National University of Environment & Bioresources

THANK YOU FOR YOUR ATTENTION!

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