State Service of Special Communications and Information Protection of Ukraine

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Case study: major attack on critical infrastructure

Olexandr BAKALYNSKYI, PhD
Deputy Director Department of Cyber Defense
Administration of State Service of Special Communication and Information Protection of Ukraine

Historical background

A list of large-scale cyberattacks at critical infrastructure

May 2014 - a cyber attack on the central election commission website during the President election

October 2015 - large-scale cyber attack on a number of Ukrainian television channels

December 23, 2015 - cyber attack on the energy sector (Kyivoblenergo, Chernivtsioblenergo, Prikarpatyeoblenergo)

February 2016 - cyber attack on the Borispol airport

December 6, 2016 - a cyber attack on the internal telecommunication networks of the Ministry of Finance, the State Treasury, the Pension Fund

December 15, 2016 - DDOS attack on the Ukrzaliznytsia website

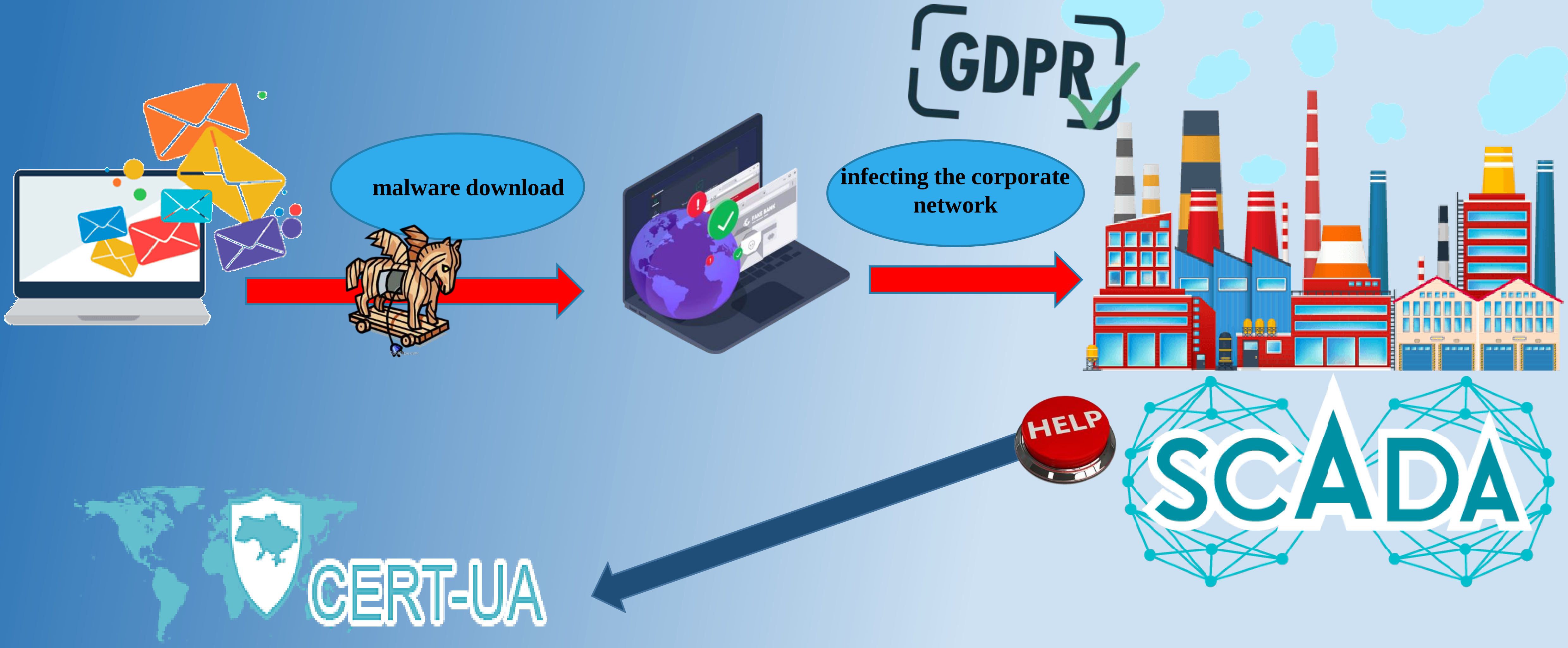
RUSSIAN ARMY IN THE WAR IN DONBAS
"I can tell you outright and unequivocally that there are no Russian troops in Ukraine."
Vladimir Putin, April 16, 2015
LUHANSK OBLAST
DONETSK OBLAST
Luhansk
Donetsk
Mariupol
FINLAND
RUSSIA
KAZAKHSTAN
Moscow
Saint Petersburg
Full version of the map with details and explanations: https://en.informnapalm.org/RussianPresence
Full incident database: bit.ly/RussianPresenceEN
InformNapalm

December 17, 2016 - cyber attack on the substation "Severnaya" of the company "Ukrenergo"

June 27, 2017 - hacker attack using the Petya.A virus program

CONSIDERATION OF A CYBER ATTACK ON THE ENERGY SYSTEM.

System penetration

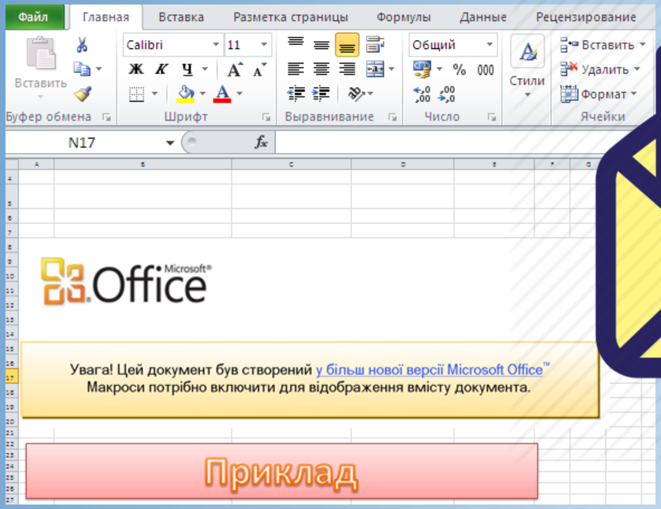


malware download

infecting the corporate network

CONSIDERATION OF A CYBER ATTACK ON THE ENERGY SYSTEM

Example of a letter



Увага! Цей документ був створений у більш нової версії Microsoft Office™
Макроси потрібно включити для відображення вмісту документа.

Приклад

Gcat

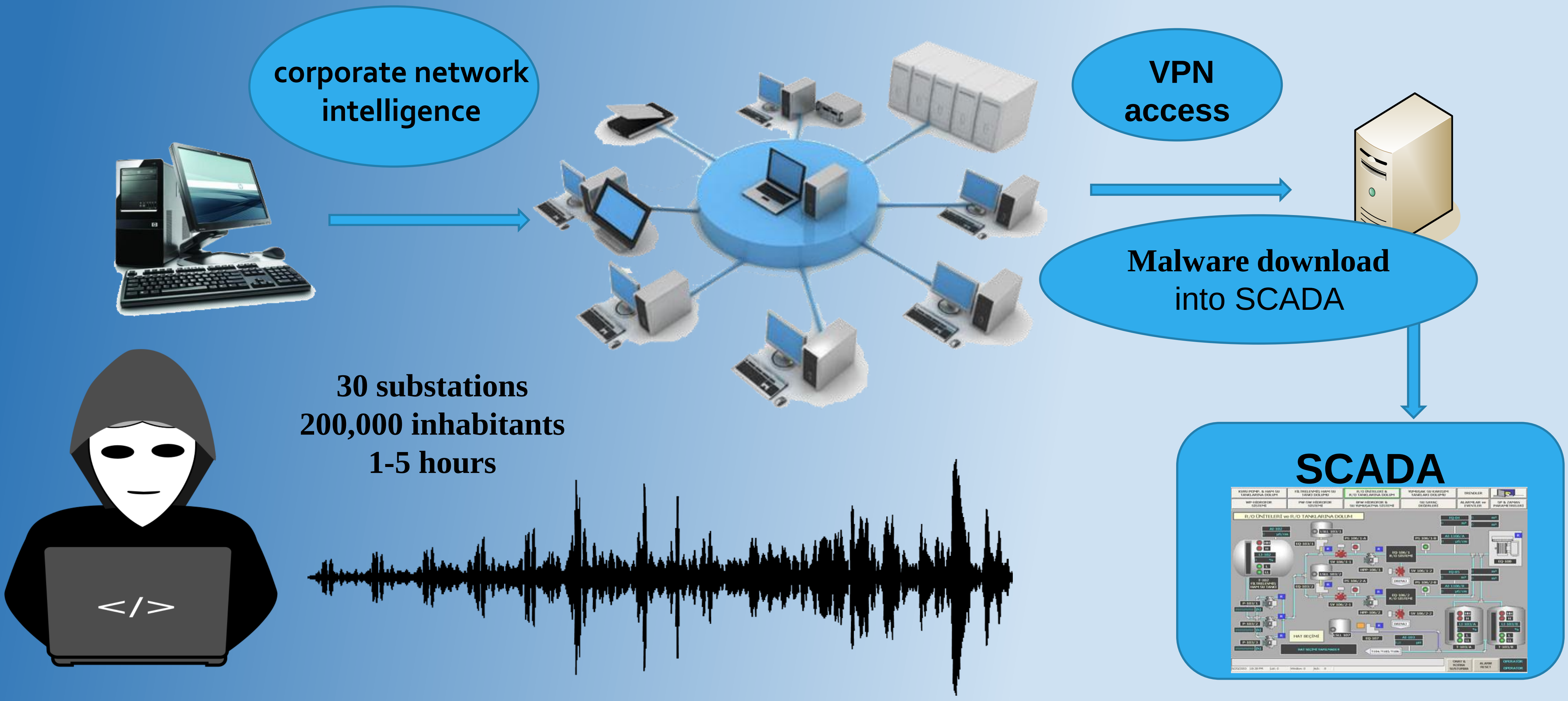
«root.cert»

CyS Centrum

CERT-UA

CONSIDERATION OF A CYBER ATTACK ON THE ENERGY SYSTEM.

Destructive activity of intruders



corporate network intelligence

VPN access

Malware download into SCADA

SCADA

30 substations
200,000 inhabitants
1-5 hours

CERT-UA

ROLE of CERT-UA

December 26, 2015 CERT-UA received information about attempts of unauthorized access to the systems of Prikarpatyeoblenergo OJSC.

<u>Indications of compromise have been found :</u>

hxxps://5.9.32.230/Microsoft/Update/KS1945777.php

hxxps://31.210.111.154/Microsoft/Update/KS081274.php

……………………………………………………………………………………

hxxp://41.77.136.250/Microsoft/Update/KS081274.php

Win32/Rootkit.BlackEnergy.AM
Win32/Kryptik.DFJC
RootKit.Kryptik.AAl

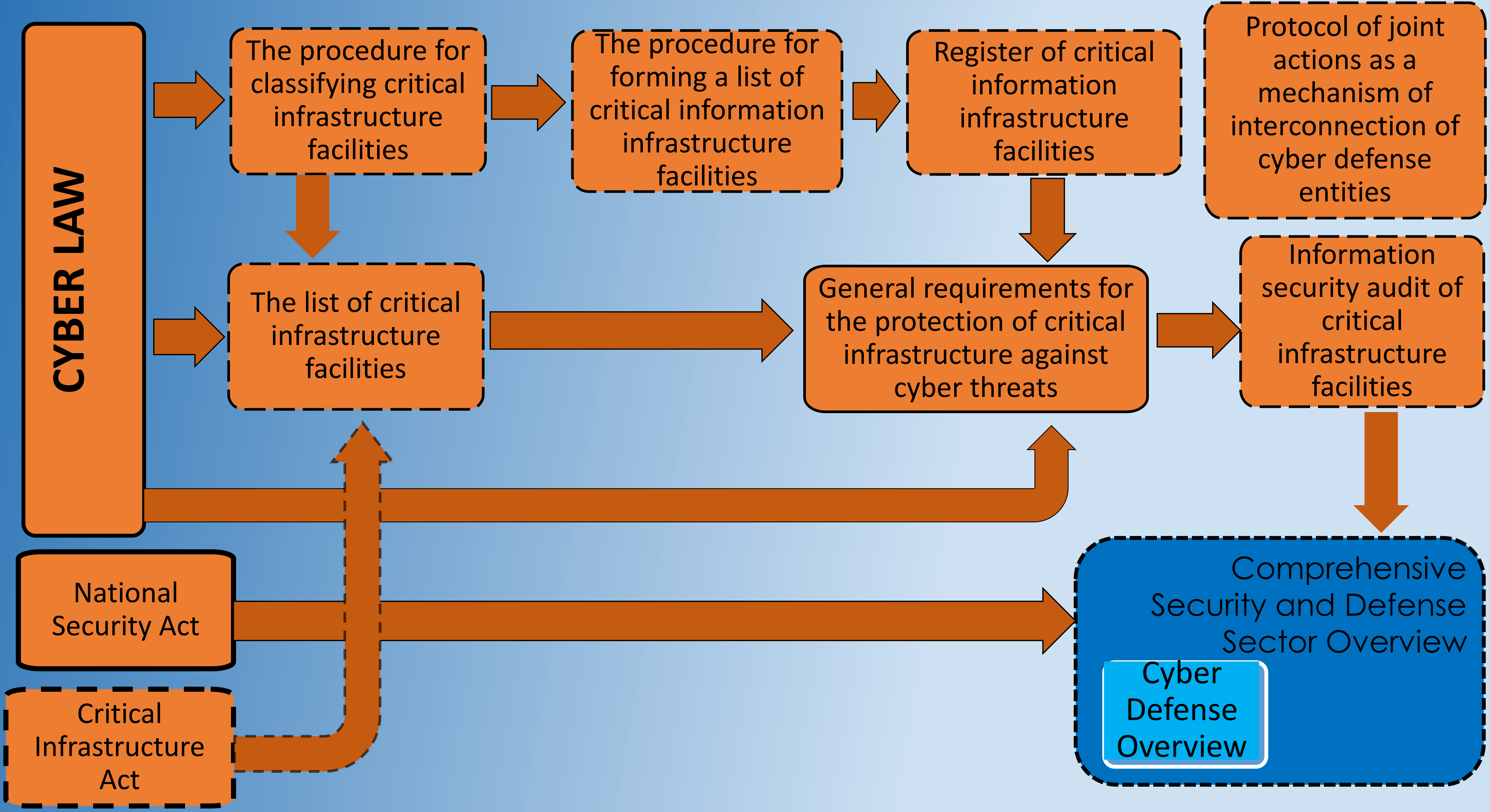
The cyber attack on the flight control systems of the Borispol International Airport has been successfully identified and neutralized. Using the already known indicators of compromise, the specialists of the Boryspil International Airport, with the support of CERT-UA employees, discovered the BlackEnergy Trojan on the network.

АКЦІОНЕРНЕ ТОВАРИСТВО
ЧЕРНІВЦІОБЛЕНЕРГО

BORYSPIL
INTERNATIONAL AIRPORT

УКРЕНЕРГО

LEGAL REGULATION



CYBER LAW

The procedure for classifying critical infrastructure facilities

The procedure for forming a list of critical information infrastructure facilities

Register of critical information infrastructure facilities

Protocol of joint actions as a mechanism of interconnection of cyber defense entities

The list of critical infrastructure facilities

General requirements for the protection of critical infrastructure against cyber threats

Information security audit of critical infrastructure facilities

National Security Act

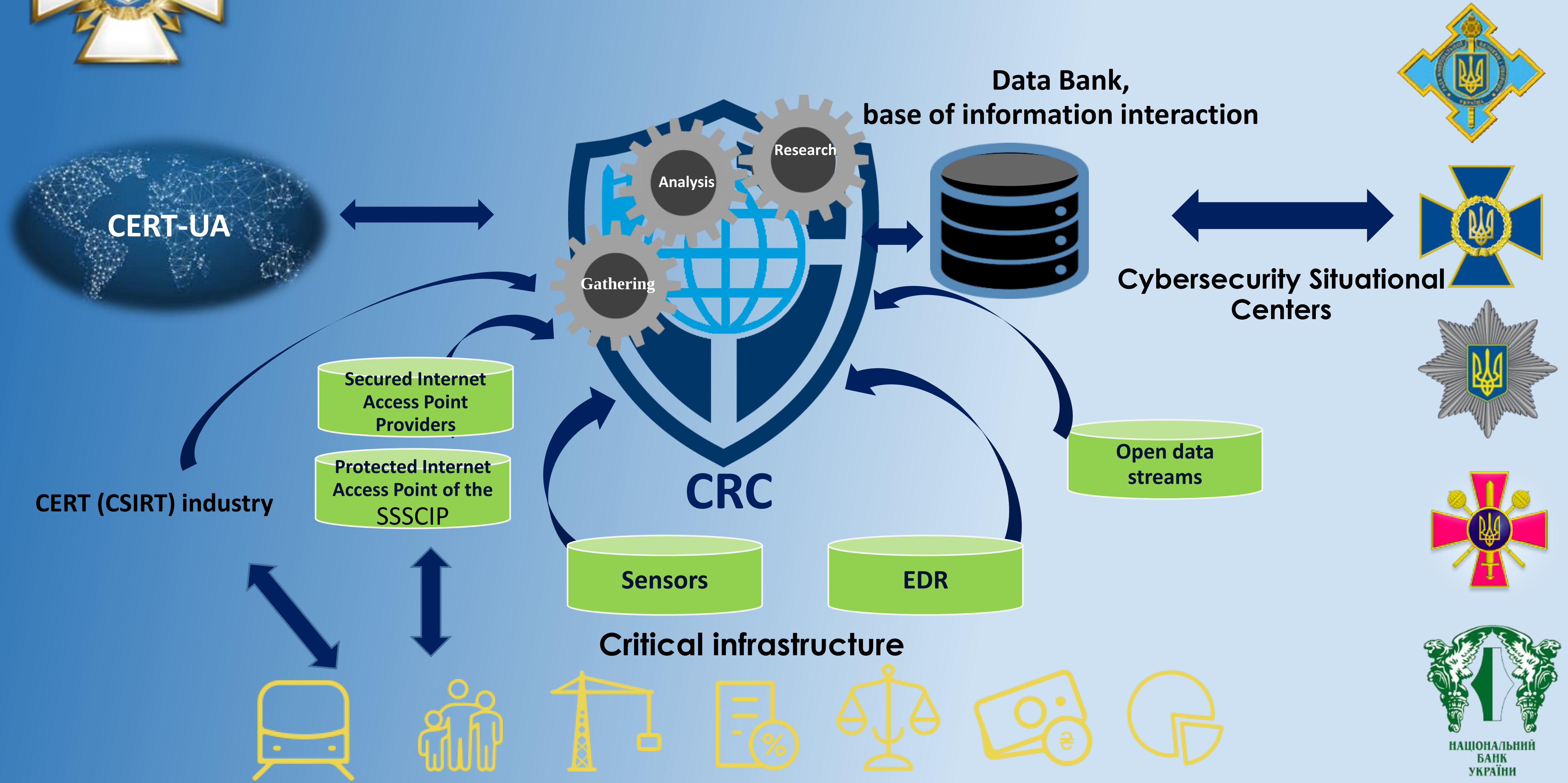
Critical Infrastructure Act

Comprehensive Security and Defense Sector Overview

Cyber Defense Overview

CYBERINCIDENT RESPONSE CENTER

Cybersecurity Situational Centers



CERT-UA

Research

Analysis

Gathering

Data Bank,
base of information interaction

Cybersecurity Situational Centers

Secured Internet Access Point Providers

Protected Internet Access Point of the SSSCIP

CERT (CSIRT) industry

CRC

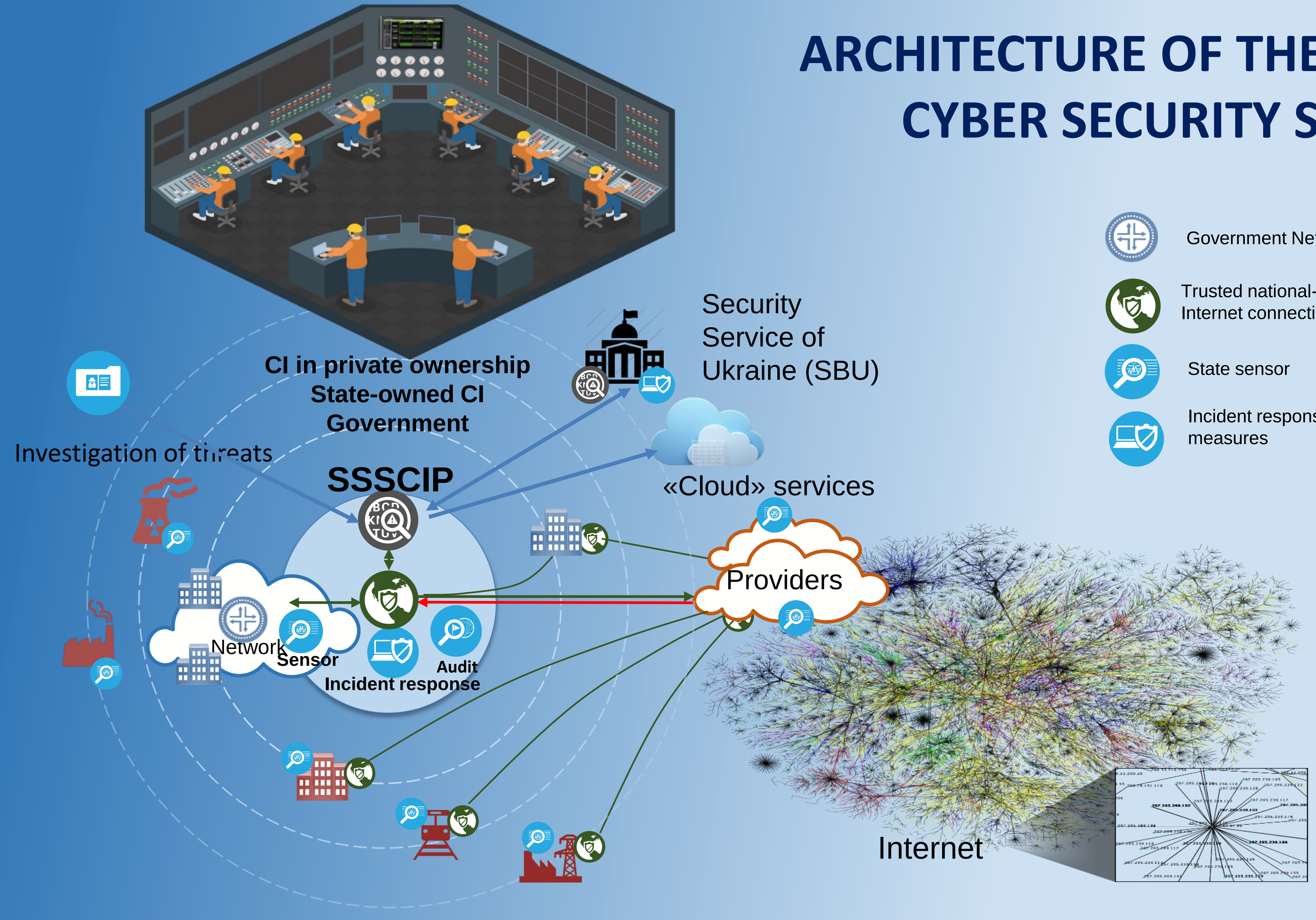
Open data streams

Sensors

EDR

Critical infrastructure

ARCHITECTURE OF THE NATIONAL CYBER SECURITY SYSTEM



Security Service of Ukraine (SBU)

CI in private ownership
State-owned CI
Government

Investigation of threats

SSSCIP

«Cloud» services

Providers

Network

Sensor

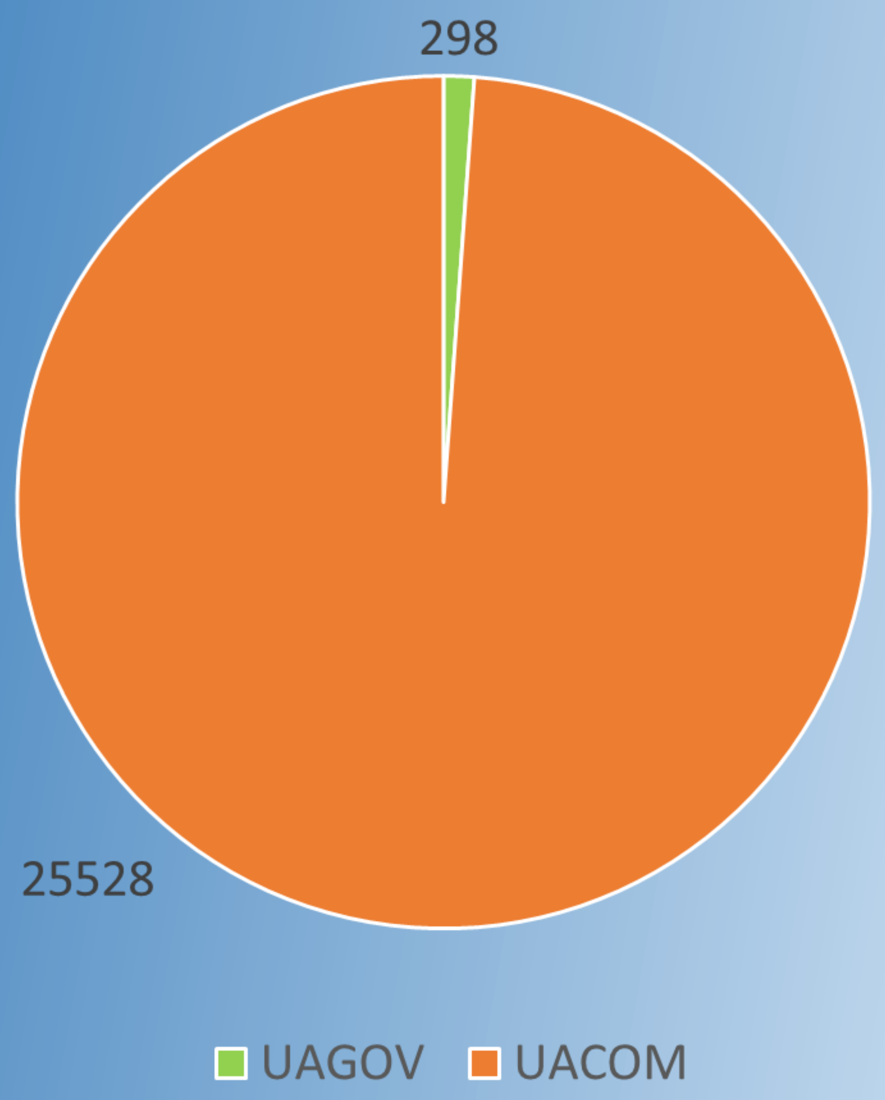
Audit

Incident response

Internet

- Government Network
- Trusted national-level Internet connection
- State sensor
- Incident response measures
- Operational Center for Security of the SSSCIP
- Operational Center for Security of the SBU
- Trusted internet connection for critical infrastructure
- Sensor or critical infrastructure

CERT-UA statistics since the beginning of 2019



25826 incidents have been reported for the year
Of them:

- attempt to gain unauthorized access – 186;
- phishing – 851;
- DDoS – 25;
- system vulnerability– 32;
- malware software – 24888.

ТОРГОВО-ПРОМИСЛОВА
ПАЛАТА УКРАЇНИ

CYBERGYGIENE

«Simple security rules in cyberspace»

Operators (providers) of the Internet Association of Ukraine

Kyivstar
Lifefell
Vodafone
Ukraine
ThreeMob

КИЇВСТАР

3Mob

lifecell

Recommendations for government agencies

Internet

Reacting

CERT-UA

Mail

Site

EUROPEAN
CYBER
SECURITY
MONTH

- **Using email**
- **Web site hosting**
- **Secure Internet connection**
- **Procedure for detection**

• STUDY ACADEMY •

CYBER SIMULATOR

(training and advanced training)

In order to train qualified specialists in the field of cybersecurity, as well as to improve their skills, develop practical and theoretical skills, a cyber simulator has been created in the base of the CERT-UA team for responding to computer incidents in Ukraine.

It is a classroom with a technology platform where you can build the appropriate networks and cyber attack scenarios in a virtual environment. The main goal is to develop practical skills in investigating incidents that are created by modeling the corresponding actions of attackers.

There is also the possibility of creating so-called competitions like Red & Blue.

UCA #FRD ACTIVITY

Ukrainian Cyber Alliance

At the end of 2017, the Ukrainian Cyber Alliance, along with other IT specialists, conducted an action for almost two months in order to assess the level of security of state resources.

Activists did not break anything, they only showed vulnerable resources, found typical vulnerabilities and shortcomings, namely:

- Not updated software;
- Use of default passwords;
- Lack of network segmentation;
- Imperfect security policy settings.

Their activities attracted attention to the existing problems in cybersecurity of individual enterprises and departments of Ukraine and allowed the implementation of measures to eliminate them. However, the information was published on social networks, which caused a public outcry and also became known to the Russian Federation.

RESULTS, CONCLUSIONS, PLANS FOR THE FUTURE

Recognizing the importance of cyber defense of critical infrastructure facilities and ensuring the functioning of the national information infrastructure, the following should be included in the key tasks:

- ❑ **formation of a regulatory framework in the field of cybersecurity aimed at achieving compatibility with the EU and NATO countries,**

- ❑ **resolving the issue of public-private partnership in the field of cybersecurity;**

- ❑ **further scaling of the organizational and technical model of cyber defense in all regions of Ukraine:**
  - *inclusion in the system of cyber monitoring and early detection of cyber threats of IT-systems of critical infrastructure (primarily energy, healthcare, financial and transport sectors);*
  - *the establishment of industry cybersecurity centers;*
  - *development of a network of computer emergency response teams)*

- ❑ **development of international cooperation with EU and NATO member countries.**

THANK YOU!