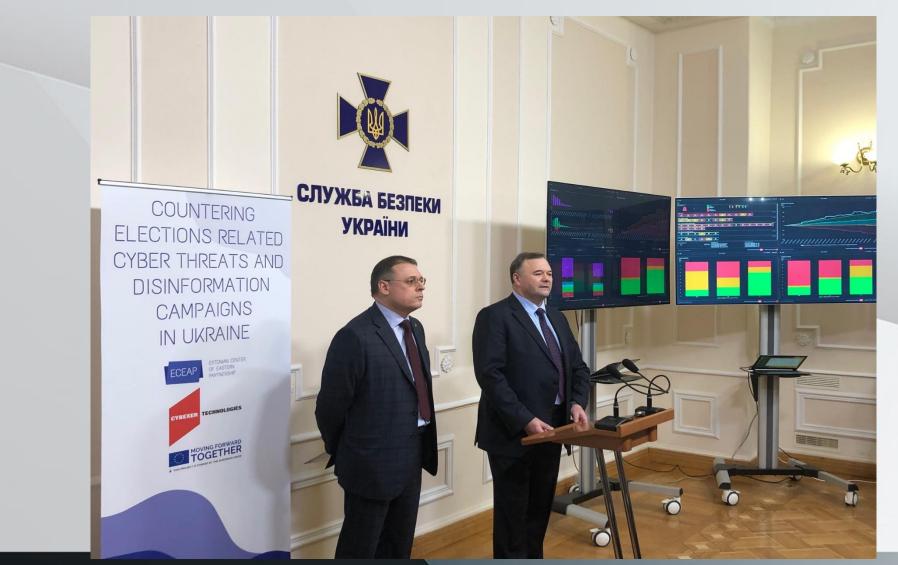
#### Election Interference: Lessons Learned from Ukraine Merle Maigre, Executive Vice President for Government Relations 04 June, 2020

CYBEXER TECHNOLOGIES

## **Briefly**

- Why care about elections in Ukraine?
- EU Countering Election-related Cyber Threats in Ukraine (2019)
- Technical and strategic exercises
- Cyber hygiene workshop for parties
- Post-election assessment of cybersecurity
- Recommendations and mitigations

#### **Technical cyber security exercises in Kyiv, March 2019**



www.cybexer.com

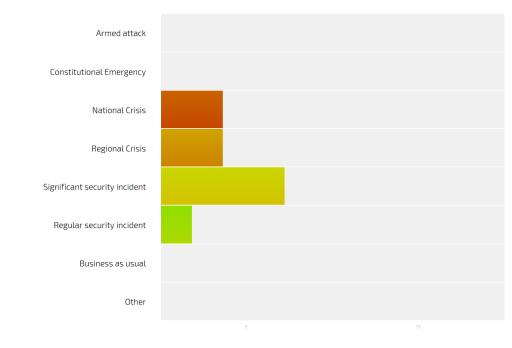
### Strategic-Level Crisis Simulation Exercise on Election Cyber security in Kyiv, July 2019

DIFFICULTIES IN ENSURING ELECTION SECURITY On the scale of 1 - 10, where 1 is least significant and 10 is most significant, please identify what are the main difficulties in election security: Disinformation, including "fake news" and social media operations Use of legacy systems Election system in constant change Malicious outside influence Inadequate level of cyber hygiene Level of decentralization of the electoral system Insider threat and corruption Lack of resources including talent and funding Lack of adequate laws and regulations Lack of interagency cooperation and coordination Lack of cooperation among political parties Lack of cooperation/trust with private sector Minimum Average Maximum

0 0 0 0 0 0 0 0 11 12 13 14 15 16 22 22 23 31 22 24 24 24 24 31 31 312 33 4 4 2 45 46 47 48 40 40 41 51 54 55 57 58 62 63 64 65 56 71 72 73 74 77 78 70 70 70 70 70

#### DEFINE THE SEVERITY OF THE SITUATION

Based on the information available to you at this time, define the severity of the situation:



01 02 03 04 05 11 12 13 14 15 16 21 22 13 142 13 14 15 16 21 22 12 13 132 134 36 38 30 31 31 312 134 142 42 45 46 47 48 49 40 47 48 49 40 41 51 54 56 57 58 62 2 3 64 65 66 71 72 73 74 77 78 79 70 70 71 72

## Cyber Hygiene E-Learning workshop, Kyiv July 2019





### **Post-election report, October 2019**

TOGETHER

- main f

POST-ELECTION ASSESSMENT OF THE CYBERSECURITY INFRASTRUCTURE AND INTERAGENCY COOPERATION IN UKRAINE WITH RELATED RECOMMENDATIONS



ESTONIAN CENTER

# **Top 3 risks & recommendations for IT infrastructure**

- 1. IT systems of the CEC not listed as critical infrastructure
- 2. Outdated security measures
- 3. Outdated physical security measures Deciding the course of action, defining the level of the crisis, adopting guidelines to communication, etc.

- Include the CEC IT systems Vybory and SVR in the official list of critical infrastructure
- 2. Regular conduct of risk analysis and risk assessment.
- 3. Assess physical risks to infrastructure including workstations

# Top 3 risks & recommendations for interagency cooperation

- 1. Unclear responsibilities for the protection of electoral systems
- 2. Unclear criteria for the selection of experts to the Election Protection Task Force
- 3. Cooperation with all third parties involved

- 1. Document and formalize the best practice of 2019 elections *ad hoc* cooperation measures
- 2. Guidelines about specific functions and roles of experts that are needed to support the CEC
- 3. Comprehensive approach and agreements with ie system developers, hosts, support service providers etc.

### **CybExer Technologies**

#### **CYBEXER** TECHNOLOGIES