Statement on Outcomes of IFES' Cybersecurity Week and Assessment

Kyiv, Ukraine

June 27, 2018

Russia's occupation of Crimea and the conflict in Eastern Ukraine has clear characteristics of hybrid warfare – a combination of conventional, informational (in the form of disinformation campaigning) and cyber warfare. With Ukraine's 2019 presidential and parliamentary elections approaching, the prospects of cyberattacks that could potentially undermine critical systems is a real and present danger, and could have severe ramifications for Ukraine and beyond. The importance of safeguarding the cybersecurity of Ukraine's electoral process cannot be overstated.

From 4-8 June 2018, the International Foundation for Electoral Systems (IFES), through the support of the United States Agency for International Development (USAID) and UK aid of the United Kingdom government, deployed a team of international and national experts to assess the cybersecurity of Ukraine's electoral process and infrastructure. The team met with a variety of stakeholders including Ukraine's Central Election Commission (CEC), government security agencies and civil society organizations. On 7 June, IFES organized a roundtable discussion on "Cyber Threats for the Electoral Process in Ukraine" with the participation of senior experts and high-level representatives from state bodies, government, electoral administration, civil society and the private sector, to take stock of the current situation.

Key findings of IFES' Cybersecurity Week include:

1. In recent years, Ukraine has experienced a series of high-level destructive cyberattacks, including on the power grid, airport and financial systems. Just three days before the 2014 presidential elections, the CEC experienced a comprehensive and sophisticated cyberattack. The attackers disabled the CEC network nodes and wiped numerous components of the election system, using advanced malware. This demonstrates very clearly the amount of damage that a sophisticated cyberattack can do in an electoral environment. Ukrainian key stakeholders are aware of these threats, eager to counter them, but in need of additional resources;
2. Some significant improvements have been introduced to the CEC IT systems in recent years, including isolation of critical networks, limiting remote access and implementation of a network flow monitoring solution and intrusion prevention systems. A new disaster recovery data center has also been established;
3. Ukraine is a signatory to the Council of Europe's 2006 Budapest Cybercrime Convention and has adopted a new Law on Cybersecurity that came into effect in May 2018. The law provides a high-level overview of cybersecurity and cyberdefense, and introduces new rules on protecting institutions and facilities designated as Critical Infrastructure (CI). IFES believes that the CEC should be part of this framework, but with appropriate provision to protect the institution's independence. The Cabinet of Ministers has until early August to pass a series of by-laws to regulate the level of protection that the state will provide to CI objects and institutions, including through network monitoring and logging, resilience against DDoS attacks, auditing of systems including through intrusion tests (penetration tests) and certification. These are to be conducted under the responsibility of the State Service of Special Communication and Information Protection (SSSCIP);

4. The official election campaign for the March 2019 Presidential Elections will start in December 2018. Elections are imminent and time is limited for the CEC and other agencies to implement any new projects, including those related to cybersecurity;
5. The mandates of 13 of 15 CEC members have long expired. This reduces the effectiveness of the CEC's mandate and affects the ability to pursue solutions and reach decision on future projects;
6. The CEC has requested 36 million *hryvna* from the 2018 budget, but this has not been allocated with the argument that the elections will happen in 2019. Thus, the CEC lacks the financial resources to upgrade its cybersecurity infrastructure. At present, there is a significant level of support on cybersecurity from various inter-governmental institutions and international assistance projects, with which the CEC is working on improving its cybersecurity systems.

Following this Cybersecurity Week and Assessment, IFES is preparing a comprehensive report with key partners. This report will offer a range of recommendations including:

1. **The CEC's IT personnel capacity should be increased** through additional resources and **targeted training**;
2. **Cybersecurity awareness** of the CEC staff should be increased, and **cyberhygiene training** should be provided to all participants of the electoral process;
3. An explicit **communication strategy dealing with cybersecurity and elections** should be developed by the CEC well ahead of the next elections to maintain public confidence in the electoral process;
4. **Collaboration** between the CEC, state security agencies and other electoral stakeholders **should be intensified and better coordinated** to increase operational resilience;
5. The CEC should elaborate **a comprehensive cybersecurity strategy** on how to respond during a cybersecurity crisis, in collaboration with state security agencies that will be involved in the process during elections. Readiness should be enhanced through crisis simulations involving key stakeholders well in advance of the elections;
6. The CEC needs new equipment to **replace outdated hardware components** throughout its systems. These "weakest links" could be exploited to gain illegal access to the CEC systems. The needed new components must be **procured sufficiently early** to be properly configured and tested - and staff must receive comprehensive training well in advance, ensuring that staff themselves do not introduce new and possibly undetected cybersecurity vulnerabilities when configuring and operating the new equipment;
7. Consider the introduction of mandatory **post election audits** to build voter confidence; and,
8. The government should immediately **allocate the CEC enough financial resources** for its cybersecurity needs, as the CEC must take action on key issues such as procurement, configuration, testing and training.

IFES has initiated the creation of the informal network "Cybersecurity of Ukrainian Elections" to exchange ideas and serve as a clearinghouse for practitioners. **IFES stands ready to continue its electoral assistance in Ukraine, including key efforts to increase electoral cybersecurity**.

This statement was prepared by the IFES' Cybersecurity Assessment Team of the International Foundation for Electoral Systems (IFES) through the support of the United States Agency for International Development (USAID) and UK aid. The opinions expressed herein are those of the author and do not necessarily reflect the views of USAID, the United States Government, or the UK government.