IFES Electoral Technology and Cyber-Hygiene Programming

IFES supports citizens' right to participate in free and fair elections. Our independent expertise strengthens electoral systems and builds local capacity to promote sustainable democracy.

As societies become increasingly reliant on technology, processes are increasingly digitized. This is also the case with elections, where technology and computers have become indispensable. Today, most election management bodies (EMBs) use some degree of technology with the aim of improving electoral processes. From standard office tools or a basic website to inform the public, to sophisticated biometric databases or fully online internet voting systems, new technologies bring new opportunities to deliver faster, more accurate and potentially more transparent and cost-effective elections.

But with every new technology integrated into the electoral process, new risks emerge: technology that is immature, misunderstood or simply creates new opportunities for malicious actors to interfere with the security and integrity of electoral processes. A new course from the International Foundation for Electoral Systems (IFES) provides participants with a brief introduction to technologies available for each electoral process, looking at the benefits and risks that they introduce and how these risks can be mitigated. An innovative cyber-hygiene awareness training is introduced in the second part of the course, aimed at providing EMB staff with cybersecurity policies, good practices and tools to protect themselves and their organizations when using technology in elections.

This regional course was developed based on the interactive trainings for electoral stakeholders in Ukraine. The pilot course was held in partnership with the Ragnar Nurkse Department of Governance and Innovation at the Tallinn University of Technology (TalTech) in June 2019.

Course Aims

- Introduce and acquire a general background of the main technological solutions used in the electoral context
- Introduce the use of internet technology to communicate with voters
- Understand the challenges and risks inherent to the use of technology in elections.
- Understand basic cybersecurity concepts
- Integrate cyber-hygiene practices and learn about tools that election administrations should use to protect themselves and the electoral process:

- Clear desk and clear screen policy
- Precautions when using USB devices
- Dangers of the "internet of things"
- Social networking hygiene
- Detect and stop phishing and spear-phishing attempts
- Password best practices
- Data backup and protection
- Software and antivirus updates

Ukraine

In Ukraine, IFES introduced a highly interactive training course designed to raise awareness of online security risks. The course helps learners understand what measures can best protect them and their election administration from those who seek to harm the democratic process. IFES' cyber-hygiene course has been designed for electoral stakeholders and election-related civil society organizations, as well as a number of government ministries and agencies in Ukraine, and uses an adult learning methodology. Following course participation, alumni are added to a monthly IFES Newsletter that offers reminders on important cyber-hygiene techniques. This initiative is made possible through the support of the United States Agency for International Development (USAID), UK aid from the UK government and Global Affairs Canada.

Indonesia

As part of the initiative to improve electoral cybersecurity and data integrity for the General Election Commission (KPU), IFES conducted a cyber-hygiene training of trainers for KPU Information and Data Center staff and operators at the provincial level, who then facilitated additional cyber-hygiene trainings. Fifty-four KPU facilitators have trained 1,088 regional commissioners and operators. The curriculum was adopted by the KPU through a co-development workshop and informed their cyber-hygiene handbook. The KPU then initiated a cyber-hygiene awareness campaign, where IFES assisted in the development of campaign materials and a training evaluation methodology. This project is funded by Australia's Department of Foreign Affairs and Trade.

Regional Europe

The "Regional Elections Administration and Political Process Strengthening Program" (REAPPS) supported the development of a regional full-length pilot course. In partnership with the Ragnar Nurkse Department of Governance and Innovation at TalTech, IFES held the 2 1/2-day course in Tallinn, Estonia. The course brought together representatives from 11 Central and Eastern European EMBs to learn more about technology in elections and international practices in cyber hygiene, culminating in a certification by TalTech.

The participants – six men and six women from Bosnia and Herzegovina, Croatia, Estonia, Georgia, Kosovo, Latvia, Lithuania, North Macedonia, Poland, Romania and Serbia – engaged in interactive lessons and guided discussions facilitated by two IFES experts, covering case studies in election technology and building better cyber behavior in their institutions. This course was made possible through the support of USAID.

Future Programming

With the data collected from course trainings in Ukraine and Estonia, IFES will further develop its cyber-hygiene trainings. An official IFES course curriculum and handbook will be available for global use and courses can be deployed regionally and globally, tailored to the needs of country contexts and local institutions.

Course trainings will continue in Ukraine and Central and Eastern Europe, expanding depth and scope to address ongoing challenges in cybersecurity. One such expansion is tailored for computer administrators and "power-users."

Further, IFES will integrate cyber-hygiene practices into its policies and procedures to build a robust, organization-wide strategy to combat cyber threats. This includes the recruitment of a global technology and cybersecurity adviser, who will be available internationally for program implementation.

Courses deployed regionally, and globally, tailored to country-specific contexts

Official IFES course curriculum and accompanying handbook

Follow-up course event in Tallinn, Estonia held again in conjunction with the Tallinn University of Technology

New policies and procedures to improve IFES' organizational cyber hygiene practices

Stay connected through www.facebook.com/IFES1987 and Twitter @IFES1987.