Cybersecurity is a critical issue in Ukraine. For elections, successful cyberattacks can have an irreparably negative impact on electoral integrity, damaging trust in the process and tampering with citizens’ democratic rights. In Ukraine, there have been significant cyberattacks on both public and private institutions using advanced malware and spyware. IFES has worked with a range of security and electoral partners to ensure that electoral cyber infrastructure is updated and protected, that civil society has the tools it needs to protect itself and Ukraine is learning and adapting to increasingly sophisticated attacks by malevolent actors, including the Russian Federation.

Cybersecurity Modernization

In 2018, IFES utilized its innovative Holistic Evaluation and Adaptation Testing (HEAT) methodology to conduct a cybersecurity assessment in Ukraine. Based on needs identified in this assessment, IFES is working with the Central Election Commission (CEC), the State Security Service of Ukraine (SBU) and the State Service for Special Communication and Information Protection to provide critical improvements to cybersecurity infrastructure. The joint effort will update cyber infrastructure and address gaps in security. Before the 2019 presidential election, IFES supported the first round of modernizations, which addressed the most pressing needs to secure critical election information. During the presidential and parliamentary elections, electoral and security participants were able to successfully detect, mitigate and respond to cyber-attacks. The election process was not disrupted despite significant efforts by malignant actors.

IFES is now working on a second round of updates and modernization initiatives. IFES’ targeted interventions contributed directly to fending off cyberattacks ahead of and through Election Day, as acknowledged by the CEC, state security agencies and election observers.

Cyber-hygiene

Recognizing the importance of smart cybersecurity practices among government and community actors, IFES and the CEC have developed a cyber-hygiene awareness training course. The course engages participants on good cyber-hygiene practices, including how to prevent phishing, internet security basics and guiding cybersecurity principles – critical skills to protect election information and sensitive data. IFES provided trainings to all geographical levels of election management, national and international observers and civil society groups who are often the target of attacks due to the communities they work with – LGBTQ organizations, women’s organizations, and disability rights groups.

This curriculum is useful for electoral actors and state agencies. IFES has been active in responding to requests for training, developed more in-depth and technically-focused versions and trained 90 representatives from the Verkhovna Rada Secretariat, the Ministry of Healthcare and Ministry of Energy and Coal Industry’s Secretariats, the Head Office of the SBU and the Ukrainian Association of Women in Law Enforcement Agencies.
International Best Practice

IFES ensures that key security participants in Ukraine are exposed to international best practice and works to help build both inter and intra-agency coordination. Recently, IFES supported Ukrainian cybersecurity counterparts from the SBU, the State Service for Special Communication and Information Protection and the Cyber Police to attend the 31st Annual FIRST Conference in Edinburgh, United Kingdom. The conference focused on facilitating global communication between incident response and security teams to promote prompt and effective resolution to computer security incidents in critical infrastructure as well as overall election cyber protection. IFES experts bolster international best practice both inside and outside of Ukraine, serving as resources on panel discussions on cyber security.

ArcSight SIEM software training programs

On September 16-20, IFES organized ArcSight SIEM software training programs and ArcSight Administrator and Analyst ASP Exams for CEC and SBU cyber security teams. These initiatives fall under the mandate of the CEC and SBU and help to improve the capacity of cybersecurity stakeholders to assist the CEC in preventing, mitigating and investigating cybersecurity attacks. This comprehensive training course is key for CEC and SBU cyber defense teams to be able to effectively utilize ArcSight SIEM software products. The program is focused on monitoring, detecting, managing and responding to advanced persistent threats and security events, which is a vital component in ensuring effective cybersecurity defense by the CEC and SBU.

Looking Forward

- IFES is planning an update of its HEAT assessment to establish the next stage of updates to Ukraine’s electoral cybersecurity infrastructure.
- IFES is currently developing an advanced cybersecurity training course for information technology professionals in Ukraine and beyond. This training builds on IFES’ Cyber Hygiene Module and targets advanced users and local network and IT administrators responsible for infrastructure. The training will be developed in collaboration with academic institutions and national cybersecurity agencies.
- IFES is developing and strengthening collaboration with academic and cybersecurity institutions in Ukraine such as the Educational and Scientific Institute of Information Security in the Academy of Security Service, the Kyiv National Aviation University and the Ministry of Energy.

These initiatives are made possible through the support of the United States Agency for International Development (USAID), Global Affairs Canada and UK aid. The opinions expressed in this document do not necessarily reflect the views of the USAID, the Government of the United States, Global Affairs Canada, the Government of Canada or the UK government.