International Perspectives to Technological Voter Registration Threats

Dr. Beata Martin-Rozumilowicz
IFES Director for Europe and Eurasia

Background

- Cyber threats have become an increasing concern since at least the mid-2000s.
- This has been especially true in the Europe/Eurasia region:
  - Estonia 2007, Georgia 2008, Lithuania 2008, Kyrgyzstan 2009
- Most serious incursions in Ukraine 2014/2015 with attempts to change electoral results and hitting CI.

Ukraine 2014

- 3-pronged wave of cyber-attacks aimed at disrupting Ukraine's presidential vote (attempts to fake computer vote totals) was defeated by government cyber experts;
- Expert: "first time we've seen a cyber-hacktivist organization act in a malicious way on such a grand scale to try to wreck a national election"
- Parliamentary elections in October, hackers attacked Ukraine's CEC website on the eve of elections.

US 2016

- US 2016 Presidential campaign sees advent of serious attacks on voter registration systems
- National intelligence and law enforcement authorities determine Russian-sponsored intrusions in 21 states
- Proof that 7 broken into and at least 1 hade voter registration data tampered with
- Although data salvaged on the basis of back-ups, clear probing with intent through a variety of techniques

Significance

- Clearly an iterative process
- Various actors (both state and non-state), applying tests, learning from experiences, and then applying in later cases
- Attempts used in US 2016 are being adjusted and tested again in recent elections
- Similarly, whatever attacks make take place in those elections will likely be further exploited in other parts of the world

Recent Election - Nigeria

- INEC confirmed there have been unsuccessful attempts on the card reader accreditation back-end server and the piloted results transmission (although there is considerable reluctance to share information)
- They don't wish to indicate number of such attempts or whether successful/unsuccessful
- No explicit mention of the look-up register, but presumption that these would have been subject to attempts. Bit of a closed box

Upcoming Election - Indonesia

- Still to be updated

Upcoming Election - Ukraine

- 25-26 February attacks - large scale intrusion attempt to the CEC infrastructure
- 26 February, SBU uncovered plot: Ukrainian contractor for a telecom organization and resident of Russia. Russian contact was collecting data on networks of strategically important mobile operators, location of telecommunication nodes, periods of time necessary to restore them after damage
- Indications that objective was to disrupt telecommunication nodes used by the State Voter Registry (SVR) for the preparation of the election

Key Lessons Learned

- **Coordination** – need to develop clear lines of communication and protocols between EMBs and other key agencies dealing with cyber (security, defense, interior, etc.), while maintaining independence;
- **Clearance** – explicit discussions well in advance so that those who are aware of exploits are able to communicate them to those in EMBs that can do something about them;
- **Communications** – clear messaging to public to maintain confidence
- **Training** – for all levels of EMB staff, on basic Cyber understanding.

IFES' Work

- Developing programming at the cutting edge of this field:
  - A cyber assessment methodology, while can be globally utilized;
  - A framework document looking at best practice from around the world;
  - Assistance in developing cyber strategies for EMBs well ahead of elections;
  - Training for all levels of EMB on cyber issues and cyber-hygiene;
  - Possible tabletop crisis simulations to learn in real time;
  - Development of communication strategies / techniques so that EMBs can be proactive in the way they approve cyber in order to maintain confidence in electoral processes.

Conclusions

- Increasingly, cybersecurity in voter registration is becoming an issue of global concern, which should be of interest to all parties in terms of sharing information and best practice
- Planning for eventual exploits and attacks needs to happen early in electoral process, to develop proper mitigating measures
- Coordination is key, so that the system as a whole can respond rapidly and effectively
- Transparency in communication is of primacy, so that voters understand what is happening based on fact, rather than hearsay and conspiracy.

Questions?
Happy to Answer at End of Session