Republic of Armenia

Position Presentation

International Criminal Police Organisation
(INTERPOL)
(This is just an example, very brief)

Topic A: Background

- The people of Armenia have demonstrated their desire to safeguard its elections, which is seen as a historical opportunity for democratic development especially since the Velvet Revolution (2018).
- Armenia strongly believes in that **“cybersecurity innovation is the backbone of digital transformation”** (INTERPOL, 2021) - but more importantly, technology-based election systems must come with educational and legal solutions which provide skill-sets to enhance policing capabilities and reduce technology-related fraud by outside forces.

Topic A: What has Armenia done?

The Central Armenia Electoral Commission (CEC) has demonstrated its interest in cyber innovation by partnering with Smartmatic in 2017 to implement VIU-815 voter authentication devices (VADs) with Access-IS OCR310e optical character recognition - authenticating passports and national ID cards while enabling officers to prevent fraud due to voter impersonation and multiple voting in its parliamentary elections (Smartmatic, 2017).

So? Armenia continues to look forward to partnering with countries with the capabilities to provide for personnel training and equipment support, as well as multi-level collaboration and policing to protect the integrity of elections around the world.

Topic A: Short-Term Proposals

Promoting ‘cyberelections’

- Incorporating technology into enhancing the validity of elections
- INTERPOL’s Cyber Innovation Lab and Cyber Fusion Centre (CFC) in Singapore
- Encourage local legislatures to set-up individual task forces to monitor the procurement of technology such that it does not contradict with democratic ideals - including voter secrecy and executive control.

Topic A: Medium-Term Proposals

Regulate and update clear standards for electoral-related tech

- E.g. biometric recognition and ballot identification technology
- Foster a **legal, culturally-competent environment** for cyber-secure elections
- Closing down possible access points to cybersecurity exposure, e.g. human, political and legal exposure

Topic A: Long-Term Proposals

“Detect-Trace-Sanction” Doctrine (Give it a snappy name!)

1. Working with local National Centre Bureaus (NCBs), while requiring a report be produced to allow **monitoring**
2. Providing a specific point of contact for local election authorities to provide a rapid response to identified threats to immediately begin **cybertracing**
3. Working with regional authorities (e.g. EUROPOL, AFRIPOL) and the INTERPOL General Assembly to recommend **sanctioning** of identified targets, possibly via the UNSC-INTERPOL Special Notices

Topic A: References

1. Yadayadayadaya
2. https://www.youtube.com/watch?v=dQw4w9WgXcQ