COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Council of Europe
Conseil de l'Europe

VENICE COMMISSION
COMMISSION DE VENISE

Octopus Conference on Cooperation against Cybercrime

Democracy under attack: e-challenges to democracy

Simona Granata-Menghini
Deputy Secretary
European Commission for Democracy through Law
Venice Commission

Council of Europe
Conseil de l'Europe

Security in elections and the right to free suffrage

- Freedom of voters to form an opinion (electoral democracy)
- Freedom of voters to express their wishes (deliberative democracy)

- No democratic elections without respect for human rights, particularly the freedoms of expression, of the press, of assembly and of association for political purposes.
- Security must not become a hurdle to the free exercise of political freedoms or a pretext to curtail them.

Cyber threats to the democratic process

- The development of institutional activities and infrastructure that make elections possible (organisation of elections, creation and administration of voters' registers, implementation of electronic ballots and internet voting) naturally depends on technology.
- Most social discourse related to the democratic process now occurs online. This includes email, tweets, websites, databases, computer networks, and many other information technologies used by voters, electoral bodies, political parties and politicians, and the media.
- New information technologies make **democratic processes more accessible to all citizens**. The internet and social media might allow many people to exert their vote, express their opinion, organise for political purposes and even survey the performance of public institutions and elected officials at a relatively low cost. But they also **expose to the risk of tampering with the electoral processes, stealing voter information and cyberespionage**.
- The rapid growth of social media along with the decline in longstanding authoritative sources of information makes it easier to use cyber capabilities and other methods to **inject disinformation and propaganda into the media and influence voters**.
- Cyber threats target
  - ✓ elections,
  - ✓ political parties and politicians and
  - ✓ traditional and social media

E-challenges to electoral democracy

- Against **elections**, cyber capabilities are used to: suppress voter turnout preventing citizens from registering and/or from voting, tamper with election results, and steal voter informations
- Against **political parties and politicians,** cyber capabilities are used to: conduct cyberespionage of personal and political information for the purposes of coercion and manipulation (Blackmail, embarrass or discredit a political target), steal or manipulate voter or party database.
- **Hacking**

✓ into voting machines

✓ Hacking into specific sites or email accounts + dissemination of content found there

- These threats are clearly performed **outside the legal boundaries**

E-challenges to deliberative democracy

- Against **traditional and social media**, cybercapabilities are used to spread disinformation and propaganda, and to shape the opinion of voters.
- Computational propaganda:
- ✓ Segmentation and profiling of users, data-driven campaigning on social media
- ✓ Information disorder (*Council of Europe report DGI(2017)09, Information disorder: toward an interdisciplinary framework for research and policy making, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c*)
- Threats to the electoral equity, to level playing field among political contestants, through:
- ✓ Manipulation of behaviour and electoral preferences (Search Engine Manipulation Effect – SEME)
- ✓ Censorship
- ✓ Monitoring of online practices
- These practices apparently occur **within the legal boundaries**

A borderless world

- Cyber capabilities are publicly available, cheap, easy to use
- Cyber tools are embedded in a borderless environment: the internet. All information would be potentially created, stored and constantly moved to any or many servers in the world, even beyond national borders.
- Cybercrime and cyber threats operate beyond the limits of any national jurisdiction.
- Difficulties for criminal investigation and prosecution.

The new actors

- Wide, diverse and rapidly evolving range of players -"**internet intermediaries**" - facilitate interactions on the internet between natural and legal persons, by offering and performing a variety of functions and services, alone or in parallel and in combination:

✓ connect users to the internet, enable the processing of information and data, or host web-based services, including for user-generated content. Aggregate information and enable searches;

✓ give access to, host and index content and services designed and/or operated by third parties.

✓ facilitate the sale of goods and services, including audio-visual services, and enable other commercial transactions, including payments

✓ moderate and rank content, including through automated processing of personal data, and may thereby exert forms of control which influence users' access to information online in ways comparable to media, or they may perform other functions that resemble those of publishers

- *Committee of Ministers Recommendation CM Rec(2018)2 on the role and responsibilities of internet intermediaries (https://rm.coe.int/1680790e14)*

What is at stake

- Right to vote and to be elected
- Right to privacy and protection of personal data
- Right to freedom of expression
- Freedom of commerce

- Electoral equity and equality of opportunities
- Threat to institutional stability, hampering democratic governance
- Loss of public trust in the electoral process may be beyond remedy
- Threats may be as dangerous as actual interferences

Possible solutions

(preliminary Venice Commission conclusions based on EMBs conference and ongoing study on "the role of social media and the internet in democratic development"

- Recognise the transnational nature of the problem
- Criminalisation and prosecution of cyber attacks
- Securing electronic evidence
- Recognise the essential role played by internet service provides, search engine and social media companies to investigate and prosecute cybercrime
- Strengthen the international framework to enhance transational cooperation among states and private actors
- Procure a greater uniformity among national legislations
- Introduce co-responsibility of private and public actors:
  - ✓ Education and information campaigns for internet users
  - ✓ Self-regulation of internet intermediaries in line with international standards
  - ✓ Remedial mechanisms
- Ensure up-to-date standards: Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Elsinore, Denmark, 17-18 May 2018); on-going work on a Protocol to the Budapest Convention
- Train EMBs and provide sufficient resources
- Provide for gradual introduction of new technologies and back up of traditional tools

Conclusion

- The new information technologies have created a novel public sphere for the democratic debate, with new actors and conflicting rights that cannot be correctly addressed with the current understanding of human rights and democracy as an issue only between citizens and governmental institutions and even as an exclusively national problem.
- A different model is necessary, based on principles of co-responsibility and international cooperation to regulate, adjudicate and solve fundamental rights conflicts, to protect simultaneously social and individual freedoms in the era of e-democracy.
- Secure and safe use of digital technologies is a multi-stakeholder responsibility in a multi-national environment: parliaments, governments, political parties, EMBs, the media, prosecutors and the judiciary, other relevant agencies but also civil society, the IT community and experts.