RESOLUTION

Preventing interference of foreign powers in European Elections

Adopted at the YEPP Council Meeting in Vienna, 13.04.2019

Recognizing that:

- European election, which will be held on May 23-26, 2019, will take place in a different political and legal environment compared to the previous vote in 2014;

- According to the EU Barometer survey "Democracy and Elections" conducted in September 2018, 61% of respondents were concerned about European elections being manipulated through cyberattacks, and 59% were concerned about foreign actors and criminal groups influencing elections covertly[1];

- Russia's Internet Research Agency (IRA), government-linked company based in St. Petersburg, is thought to have an annual budget of $12 million, and to employ over a thousand workers to misinform and polarize voters, and disrupt political discourse around the world[2];

- The pattern of Russia's interference has been repeated in the EU: from the influence operations in the run-up to the 2016 referendum in the Netherlands on the EU-Ukraine Association Agreement; continued digital influence to further reduce trust in the wake of the UK EU membership vote; Kremlin-affiliated media promotion of polarising issues during the 2017 German election; and pro-Kremlin bots engaging in a coordinated 'disruption strategy' over Catalonia in 2017, along with Kremlin-backed news platform;

- In 2018, representatives of online platforms, leading social networks, advertisers and advertising industry agreed on a self-regulatory Code of Practice to address the spread of online disinformation and fake news

- On March 30, 2019, Facebook CEO Mark Zuckerberg published a blog "Four Ideas to Regulate the Internet", calling on governments and regulators to take a more active role for updating the rules for the internet in four areas: harmful content, election integrity, privacy and data portability;

- Cyberattacks have increased threefold between 2015 and 2017. The economic impact of cyber crime rose fivefold since 2013. 87% of Europeans see cyber crime as an important challenge for EU's internal security[3] ;

- On 20 February, 2019, Tom Burt, Microsoft's corporate vice president for customer security and trust, informed about spear-phishing attempts connected to the

[1] http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2198

[2] https://www.lawfareblog.com/documents-senate-intelligence-committee-publishes-two-reports-internet-research-agency

[3] https://www.consilium.europa.eu/en/policies/cyber-security/

hacking group Strontium, also known as APT28 and Fancy Bear on think-tanks and NGOs working on topics related to democracy, such as German Council on Foreign Relations, The Aspen Institutes in Europe, The German Marshall Fund etc.

Acknowledging that:

- According to the European Parliament's first official poll, the anti-EU groups will potentially control more than 14 percent of the next European Parliament[4];

- Disinformation campaigns are a powerful instrument used by malign actors to influence social and political situation in western democracies;

- Disinformation is spread via different channels for different audiences. While in Central and Eastern Europe, disinformation is mostly spread through dozens of dedicated outlets in local languages, in Western Europe the campaign shifted towards social media, discussion forums[5];

- Russian government-linked media RT and Sputnik, which are present in 100 countries and provide coverage in 30 languages, spread and promote headlines describing the decomposition of the modern liberal system. The RT, with a budget of approx. $300 million a year, maximizes its impact via spreading viral material on social media platforms (Facebook, Twitter, Youtube);

- Political processes have a long history of misinformation and misperceptions. The proliferation of misinformation has been rapidly increased by social media in recent years"

- In addition to state sponsored manipulation other concerns are social media platforms which are being operated as for-profit enterprises, which are dependent on the accumulation and monetization of personal data

- According to the European Commission, despite the growing threat, awareness and knowledge of cybersecurity is still insufficient: 51% of European citizens feel uninformed on cyber threats, 69% of companies have basic or no understanding of their exposure to cyber risks;

- According to the list of The World Economic Forum Global Risks Report 2019, "cyber-attacks" are one of the five major global risks in terms of likelihood and ranked number seven in terms of impact6;

- In addition to the central unified European Union Action plan to prevent election interference and democracy subversion, each of the Member States has to implement its own strategy to protect electoral process;

[4] http://www.europarl.europa.eu/news/en/press-room/20190218IPR26703/first-seat-projections-for-the-next-european-parliament

[5] https://euvsdisinfo.eu/the-strategy-and-tactics-of-the-pro-kremlin-disinformation-campaign/

[6] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

YEPP calls on:

- The EU Member States to develop and introduce national policies for media literacy as a part of long-term strategy to tackle societal vulnerability to misinformation;

- The EU Commission to increase funding for detection and analysis, including the Strategic Communication Task force;

- The EU Member States to establish counter-influence task forces, to examine financial and political links between foreign actors and domestic business and political groups;

- The EU Member States to amend electoral legislation to require political parties to publicly report their sources of funding.