EUROPEAN PARLIAMENT THINK TANK – TOPICAL DIGEST

April 2019

In today's age of social media, disinformation campaigns and cyber-attacks have become serious threats to our democracy. In this context, with the upcoming elections to the European Parliament and the nomination of the new European Commission, it is no exaggeration to say that the future direction of the European Union is at stake. It is therefore clear that further improvements will need to be made to the EU's cyber-defence policy. This digest presents a selection of parliamentary research publications on cybersecurity and elections.

Foreign influence operations in the EU

Briefing by Naja Bentzen, EPRS, July 2018

Attempting to influence political decision-making beyond one's own political sphere is not a new phenomenon – it is an integral part of the history of geopolitics. Whereas hard power relies on military and economic force, the soft power of a state involves public diplomacy and dialogue on values, cultures and ideas, which should normally correspond with its behaviour abroad. Although the extent is hard to measure, democratic states whose values match the prevailing global norms – pluralism, fundamental rights and freedoms, and the rule of law as a principle within states and in international relations – and exert this influence by contributing to the prevention and resolution of conflicts, traditionally appear more attractive, thus having more soft power leverage. However, influence can also serve purposes of interference and destabilisation.

ENISA and a new cybersecurity act

'EU Legislation in Progress' Briefing by Maria Del Mar Negreiro, EPRS, February 2019

In September 2017, the Commission adopted a cybersecurity package with new initiatives to further improve EU cyber-resilience, deterrence and defence. As part of these, the Commission tabled a legislative proposal to strengthen the EU Agency for Network Information Security (ENISA). Following the adoption of the Network Information Security Directive in 2016, ENISA is expected to play a broader role in the EU's cybersecurity landscape but is constrained by its current mandate and resources.

The new European cybersecurity competence centre and network

'EU Legislation in Progress' Briefing by Maria Del Mar Negreiro, EPRS, February 2019

Building on the 2017 cybersecurity package, which set out a series of initiatives to further improve EU cyber-resilience, deterrence and defence, in September 2018, the Commission presented a proposal for the creation of a European cybersecurity competence centre with a related network of national coordination centres. The initiative aims to improve and strengthen the EU's cybersecurity capacity, by stimulating the European technological and industrial cybersecurity ecosystem as well as coordinating and pooling necessary resources in Europe.

Online disinformation and the EU's response

'At a glance' note by Naja Bentzen, EPRS, February 2019

The visibility of disinformation as a tool to undermine democracies increased in the context of Russia's hybrid war against Ukraine. It gained notoriety as a global challenge during the UK referendum on EU membership as well as the United States presidential election campaign in 2016. The European Union and the European Parliament are stepping up efforts to tackle online disinformation ahead of the May 2019 European elections.

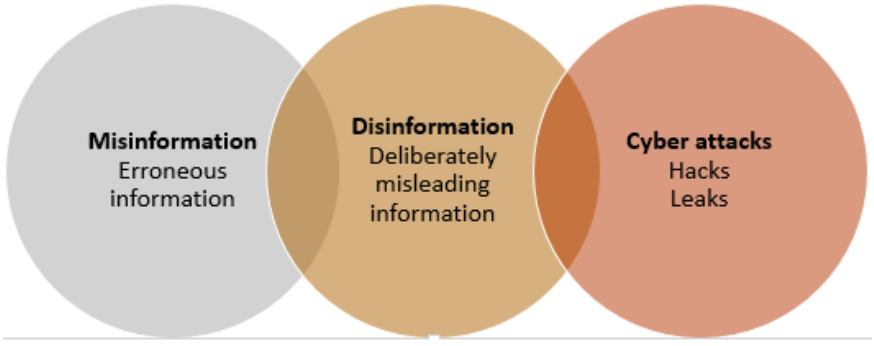
Automated tackling of disinformation – Major challenges ahead
Study by the Scientific Foresight Unit, EPRS, March 2019
This study maps and analyses current and future threats from online misinformation, alongside currently adopted socio-technical and legal approaches. The challenges of evaluating their effectiveness and practical adoption are also discussed. Drawing on and complementing existing literature, the study summarises and analyses the findings of relevant journalist and scientific studies and policy reports in relation to detecting, containing and countering online disinformation and propaganda campaigns.

Regulating disinformation with artificial intelligence
Study by the Scientific Foresight Unit, EPRS, March 2019
In this study, the authors examine the consequences of the increasingly prevalent use of artificial intelligence (AI) disinformation initiatives on freedom of expression, pluralism and the functioning of a democratic polity. The study examines the trade-offs in using automated technology to limit the spread of disinformation online. It presents (self-regulatory to legislative) options to regulate automated content recognition (ACR) technologies in this context.

Further reading:
Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States
Study by European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, February 2019
Societal costs of 'Fake news' in the Digital Single Market
Study by European Parliament Policy Department for Economic, Scientific and Quality of Life Policies, December 2018
Computational propaganda techniques
'At a glance' note by Naja Bentzen, EPRS, October 2018
How to spot when news is fake
'At a glance' note by Naja Bentzen, EPRS, February 2019
From post-truth to post-trust?
'At a glance note' by Naja Bentzen, EPRS, October 2018
Polarisation and the news media in Europe
Study by the Scientific Foresight Unit, EPRS, March 2019

More in the Graphics Warehouse:

Overlapping disruption to information



Source: EPRS, adapted from the Council of Europe, 2017.