EU encryption debate

Reasons for the debate

- encryption is super important to the EU and its market
- terror attacks brought up encryption as something that terrorists use
- Europol and LEA called for counters as they were concerned
- IOCTA report said encryption is a problem
- encryption is important for privacy etc but also provides safe havens for criminals
- slow cooperation between LEAs
- there are very different capabilities in different countries
- LEA fear that they will go dark

The Debate

- members demand a policy solution
- currently no solution in sight
- Germany, France, UK want regulations
- academics, technologists, civil societies, businesses are against it
- VP for Digital Single Market is also against it
- Europol and ENISA agree to not want backdoors – does more harm than good

Issues

- Europol budget is being increased, LEAs are offered training and consulting
- EU does not have a mandate, so members would have to do this themselves – different capabilities
- there needs to be a solution to individual rights vs security interests
- fear of going dark, lacking technical expertise, no cooperation frameworks, not enough money
- there is no concrete plan
- how can one support encryption but at the same time try to get better at breaking it
- laws on encryption breaking/circumventing are not developed yet
- strong foreign encryption is still really difficult to break
- sharing of toolboxes might not work particularly well

Results

- Europol encourages member states to build their own arsenals as well as more cooperation
- resolution of December 2016 meeting of interior ministers: mandate for commission to find technical, legal and political issues and solutions
- consultations with many experts and stakeholders
- October 2017: embedded announcement of ... in anti-terrorism package:
  - support Europol and their decryption abilities
  - create an expert network for LEA
  - toolbox for alternative investigation techniques
  - better cooperation between member states
  - training for national LEA
  - continues assessment
  - states that encryption is vital – should not be weakened
  - does not exclude backdoors
- plans for just breaking encryption straight up
- GDPR talks on encryption as well