CYBER SANCTIONS REGIME

YULIYA MIADZVETSKAYA

LEGAL RESEARCHER AT CENTER FOR IT AND IP LAW, KU LEUVEN

EU CYBER DIPLOMACY TOOLBOX

"This has a whiff of August 1945. Somebody just used a new weapon and this weapon will not be put back in the box."

- From resilience building and early warning mechanism to cyber diplomacy
- Non-paper on 'Developing a joint EU diplomatic response against coercive cyber operations' (2016)
- Urgency to adopt EU cyber sanctions framework before the May 2019 EP elections
- 17 May 2019 cyber sanctions regime approved by the Council

HOW DO CYBER SANCTIONS WORK?

- Performed or attempted cyber-attack
- External: outside the EU
- Threat: critical infrastructure, services necessary for the essential social activities, State functions
- Smart sanctions approach
- No attribution to third countries (why?)

CHALLENGE OF ATTRIBUTING CYBER-ATTACKS

“Electrons don’t wear uniforms.”

- Anonymity on Internet is a barrier to forensic-based technical attribution
- Legal and contextual attribution (StuxNet)
- Attribution is a prerogative of individual states
- Delimitation between targeted measures and attribution of responsibility to a third state

CHALLENGE OF COMMON APPROACH

Divided in diversity?

- The ‘otherness’ of the CFSP
- The prioritisation of good diplomatic relations
- Institutional divide over NotPetya cyber-attack

CHALLENGE OF THE FUNDAMENTAL RIGHTS TEST

- Kadi saga: full review of the lawfulness of all Union acts in the light of the fundamental rights
- Fundamental rights:
  - Asset freeze: violation of the right to property and the freedom to conduct a business (Rosneft, Rotenberg)
  - Personal data protection (reputational damage)
  - The rights of the defence and of the right to effective judicial review

    Clear and distinct criteria tailored to the specifics of each restrictive measure'. It is the task of the EU authorities to present *'sufficiently solid factual basis'*.

CHALLENGE OF PROVIDING EVIDENCE

- Sensitive nature of the information upon which the sanctions listings are based can be compromised by its disclosure
- *'The entitlement to disclosure of evidence as part of the rights of the defence is not an absolute right'*
- CJEU: no evidence should mean no sanction
- Divergences in cyber capacities between Member States
- Limitations to the principles of mutual trust and sincere cooperation

OVERVIEW OF THE US CYBER SANCTIONS

- April 2015 marked the beginning of the US cyber-related sanctions program
- It is implemented by the Office of Foreign Assets Control (OFAC)
- It deals with threats to the national security stemming from cyberspace + interfering with or undermining election processes or institutions
- 3 main elements:
  - presence of an external element
  - likelihood of a threat to national security
  - conduct of all those events in the cyber domain
- Less fragmented decision-making than the EU
- A North Korean programmer was accused of the involvement in several cyberattacks (the WannaCry attack)

CONCLUSION

- Establishing a link between a geographical area and persons behind the attack is a difficult exercise
- Challenge of a collective attribution of cyber-attacks by the EU
- Difficult task of balancing of foreign policy objectives against fundamental rights in order to withstand a potential challenge of targeted sanctions in front of the CJEU
- Challenge of striking a right balance between legitimate interests of preserving confidentiality of evidence and the respect for the right to be heard and the provision of effective judicial protection