





Committee of Ministers adopts Council of Europe Internet Governance Strategy 2012 – 2015 (March 2012):

- ▶ I. Protecting the Internet's universality, integrity and openness
- ► II. Maximising rights and freedoms for Internet users
- ▶ III. Advancing privacy and data protection
- IV. Enhancing the rule of law and effective co-operation against cybercrime (global harmonisation of legislation, Budapest Convention as reference standard, review implementation, expanding technical assistance, transborder access, criminal money, children, safeguards etc.)
- V. Maximising the Internet's potential to promote democracy and cultural diversity

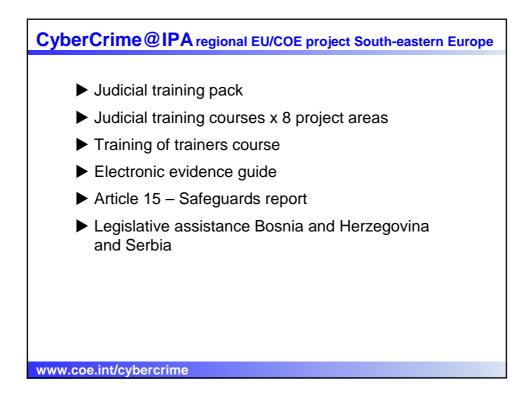


Following Octopus 2009:

- International workshop on financial investigations and criminal money on the Internet (Kyiv, Ukraine, Feb 2012)
- FATF Revised 40 Recommendations (Feb 2012): Encourage ratification and implementation of Budapest Convention
- Typology study on criminal money flows on the Internet adopted by Moneyval (March 2012)

See <u>www.coe.int/cybercrime</u> (reports)

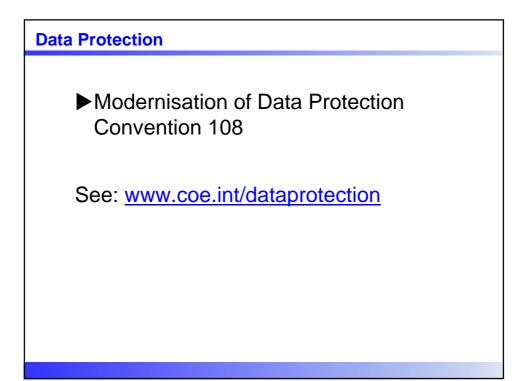
www.coe.int/cybercrime

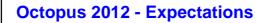


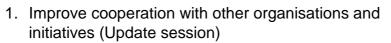




- Phase 2 completed (December 2011)
- Phase 3 launched (January 2012) with funding from United Kingdom, Japan, Estonia and Microsoft
- Workshop on cybercrime and cybersecurity policies and legislation for Central America (in cooperation with the OAS and the Government of Costa Rica) (San Jose, March 2012)
- Dialogue on policies and legislation with Botswana, India, Israel, Korea, Mongolia, Niue, Panama
- Contribution to/participation to activies of APWG, Commonwealth Cybercrime Initiative, CTO, European Union, ICANN, Kaspersky Lab, Microsoft, UNODC
- Child protection study on criminal law benchmarks
- Octopus Cybercrime Community launched
- Octopus 2012 organised







- 2. Legislation: Maintain global process (WS 1)
- 3. Private/public information sharing: towards guidelines? (WS 2)

(?)

- 4. Online child protection: how to implement the legislative engagement strategy (WS 3)
- 5. Transborder access to data: current practices and future options (WS 4)
- 6. Safeguards: promoting human rights, rule of law, data protection requirements (WS 5)
- 7. Inspiration: future cooperation against cybercrime visions and wish lists (Plenary Day 3)

www.coe.int/cybercrime