Harmonizing Cybersecurity Initiatives: A Policy Framework for Strengthening Coordination in Safeguarding Children Online

Iva Kojić
Maša Mihajilović

01

PROBLEM DESCRIPTION

02

POSSIBLE SOLUTIONS

03

RECOMMENDATIONS

04

THE PURPOSE

DESCRIPTION OF OUR PROBLEM

CHILDREN AND YOUNG PEOPLE ON THE INTERNET: WHAT WE KNOW ABOUT THE GROWING UP WITH ONLINE RISKS

SHARE FOUNDATION

50%

of children and adolescents across the surveyed countries are affected by cyberbullying

40%

experiences cyber threats

40%

of adolescents (13-18 years old) experiences unwanted sexual contact

25%

is exposed to violent and sexual content

Current bodies dealing with the issue in Serbia

- **State bodies** including Ministries and a newly introduced National call center for security of children on the Internet, legal aids, social workers
- **Non governmental organizations** such as the Center for a safer Internet
- **Report of the Public Prosecutor's office for Cybercrime** reveals an alarming lack of information on the already small number of reports dealing with child internet threats

ПАМЕТНО БЕЗБЕДНО

Republika Srbija
Ministarstvo trgovine, turizma i telekomunikacija

SRB-CERT

csi.org.rs

Република Србија
ВИШЕ ЈАВНО
ТУЖИЛАШТВО У БЕОГРАДУ
Посебно тужилаштво за
високотехнолошки криминал

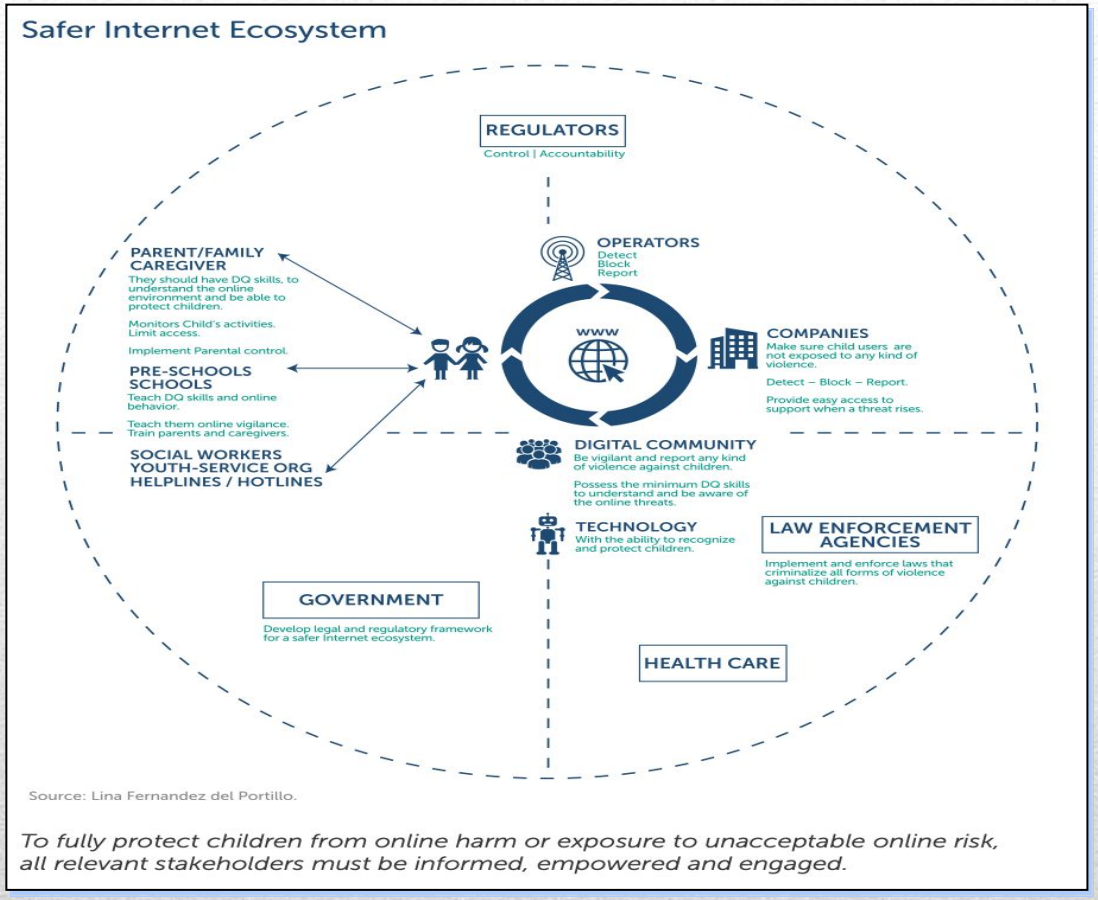
!BODIES PRESENT ON PAPER, BUT VERY FEW ARE ACTING AND PRODUCTIVE!

The question of existing legislation dealing with this issue

Strategy for the development of an information society and information security in the Republic of Serbia for 2021. To 2026.

Ordination for security and protection of children while using information and communication technologies for the period of 2020. To 2024.

POSSIBLE SOLUTIONS



To fully protect children from online harm or exposure to unacceptable online risk, all relevant stakeholders must be informed, empowered and engaged.

Multi-stakeholder engagement is based on the common understanding that the policy of protecting children in the digital environment rests on the commitment and joint responsibility of all interested parties.

MULTI – STAKEHOLDER ENGAGEMENT

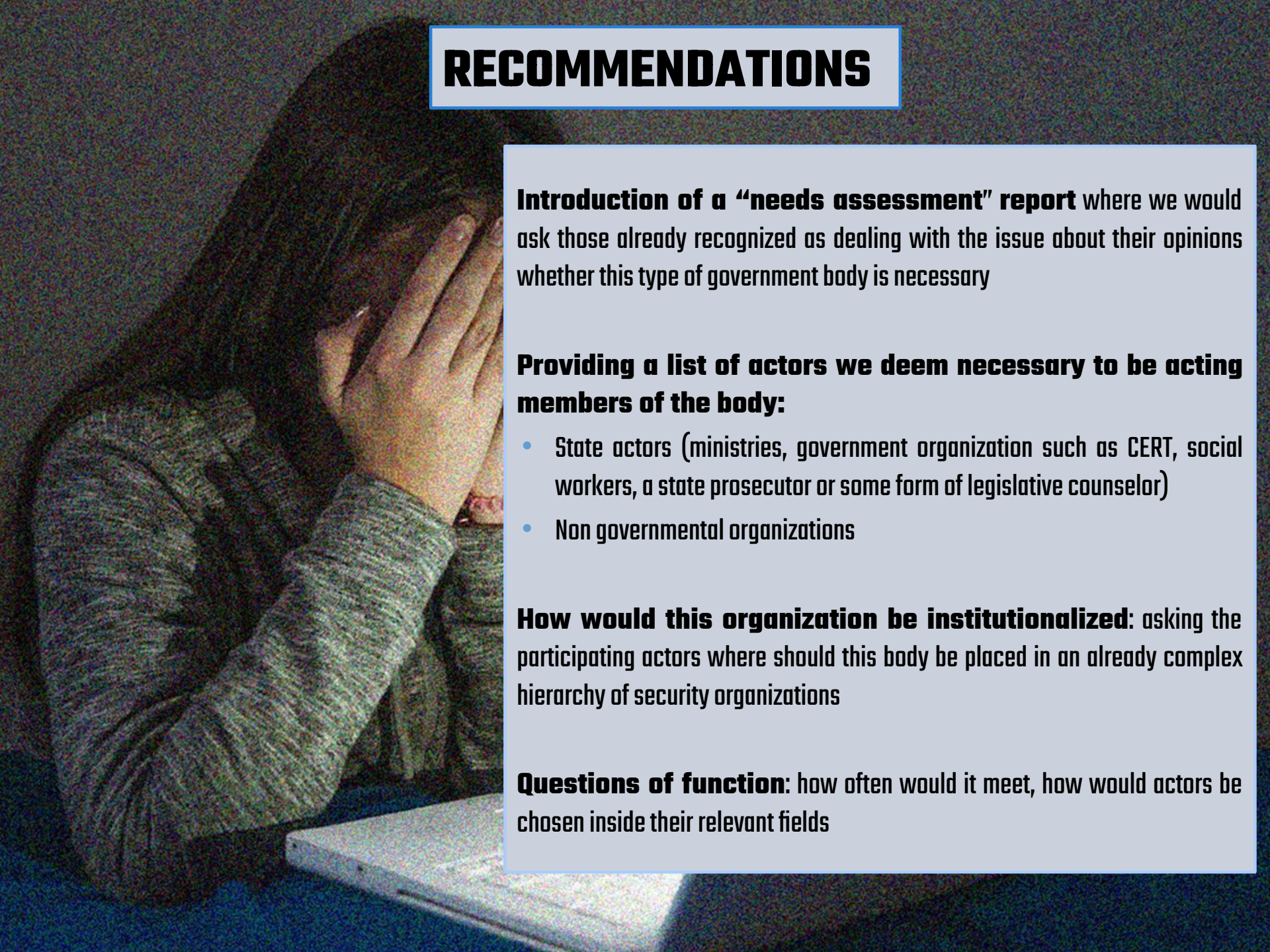
EXAMPLE OF GOOD PRACTICE

- The UK Council for Internet Safety (UKCIS) - a multi-stakeholder forum with an interest in cybersecurity, guided by the government's internet safety strategy, with 200 organizations representing government, regulators, industry, law enforcement, academia and charities.

- Bringing together key actors and working across sectors and disciplines should build a safer internet that can integrate the experiences of a wide range of citizens.

Table 2. Examples of policy mixes and oversight bodies

Country	Policies	Oversight body(ies)
Belgium	*Je decide* – online privacy Digital Champion – promotes digital skills and opportunities Child Focus - combats child sexual exploitation	Data Protection Authority Private Professional, appointed by government mandate Publically funded interagency body
Canada	Canadian Centre for Cyber Security Innovation and Skills Plan, 'Technologies' – identify new technologies and develop skills	Multiple Departments (lead by Public Safety Canada) Innovation, Science and Economic Development Canada
Chile	ENLANCES – Integrates educational resources into the school system Asociación de Telefonia Móvil – Industry body, representing the mobile phone sector	Centre for Education and Technology (within Ministry of Education) Trade association, regulated by the Sub-secretariat of Telecommunications, under the Ministry of Transport and Telecommunications
Colombia	Under the framework of the Law Against Commercial Sexual Exploitation – multiple actions to prevent contact risks National Digital Security Policy ('CONPES No. 3854') – Privacy, digital security Various strategies on personal data, and protection against exploitation	Multiple government entities National Council for Economic and Social Policy Communications Regulatory Commission
France	Digital Education Unit and Policy Community of stakeholders *providing*	Data Protection Authority Educnum - Collective of 70 non-profit organisations and
Hungary	Digital Child Protection Strategy - based on three pillars: awareness raising, digital literacy, and protection and safety.	Whole of government (part of the government's digital success programme)
Mexico	Niñ@s INAI – privacy / protecting personal data @Prende – community awareness and education	National Institute for Transparency, Access to Information and Personal Data Protection Secretariat of Public Education



RECOMMENDATIONS

Introduction of a "needs assessment" report where we would ask those already recognized as dealing with the issue about their opinions whether this type of government body is necessary

Providing a list of actors we deem necessary to be acting members of the body:

- State actors (ministries, government organization such as CERT, social workers, a state prosecutor or some form of legislative counselor)
- Non governmental organizations

How would this organization be institutionalized: asking the participating actors where should this body be placed in an already complex hierarchy of security organizations

Questions of function: how often would it meet, how would actors be chosen inside their relevant fields

THE PURPOSE

This multi-stakeholder cooperation implies not only a collective responsibility towards creating a safe and positive online (and offline) environment, but also our shared, social responsibility towards the well-being of children and youth. It would provide a common focus for decision-making and aim to shape policy, education, parenting and service design.

- Policy paper would be used to foster a shared understanding of digital dangers and risks.
- Policy paper would provide "real life" examples of positive initiatives for digital dangers and challenges, encourage best practice and its implementation.
- It would be used as a reflection tool to assess the likely impact of policy or service design.
- It can be used at any stage in these processes from planning to implementation; monitoring to evaluations.

- https://www.sharefoundation.info/wp-content/uploads/Deca-i-mladi-na-internetu.pdf
- https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2021/86/1/reg
- https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2020/13/4/reg
- https://assets.publishing.service.gov.uk/media/5d7a00c4e5274a27cefd49eb/UKCIS_Digital_Resilience_Working_Group_Policy_Paper.pdf
- https://read-oecd--ilibrary-org.translate.goog/science-and-technology/protecting-children-online_9e0e49a9-en?_x_tr_sl=en&_x_tr_tl=sr&_x_tr_hl=sr&_x_tr_pto=wapp&_x_tr_hist=true