CC-DRIVER

Researching cybercriminality to design new methods to prevent, investigate and mitigate cybercriminal behaviour.

Policy Brief No. 10

April 2023

Who is this for?

Law enforcement authorities, policy makers, private sector organisations, industry, civil society organizations, academia and research institutions, educational institutions, and all interested parties in the fields of cybercrime and cybersecurity.

Highlights

1. Cybersecurity is a shared responsibility.
2. “Nothing about us without us.”

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 883543.

CC-DRIVER

International Summit on Youth and Cybercrime

On 1 March, 2023, the International Summit on Youth and Cybercrime was held in Valencia (Spain), with plenary presentations and multiple panel discussions on the trends of cyber juvenile delinquency, including their human and technical drivers.

The event, hosted by Valencia Local Police, was live-streamed and simultaneously translated into Spanish and English. Over 150 persons from 33 nations attending on-site were joined by 220 viewers online. Participants' backgrounds were law enforcement, academia, education, industry, public administration and policy making, civil society organisations, and media, as well as other areas of expertise in the field of cybercrime and cybersecurity.

Keynote speeches were held by Dr. Nada Milisavljevic from the European Commission and Prof. Julia Davidson from University of East London. The latter presented the latest cutting-edge research on pathways into and out of cybercrime from a young people's perspective, referring to a comprehensive European study with over 8,000 participants. The panel discussions also focused on young cybercriminality, each from a special angle:

- policy makers' perspective
- private sector perspective
- academia and research perspective
- law enforcement perspective
- awareness and education perspective

This policy brief summarizes the most important insights from the five panel discussions.

Policy makers

Cybercrime influences many aspects of life, from individual persons to public safety and security. It's the duty of policy makers to provide a secure environment for citizens. This role includes prevention measures such as education in schools, courses, and trainings, as well as supporting law enforcement agencies in their repressive fight against cybercrime. In doing so, prevention and education should always precede criminal measures.

In order to prepare policy makers to fulfil their duty, it is of utmost importance to understand cybercrime and how the online economy works: Why do people become cybercriminals? Why do people fall victim to cybercrime? This necessitates to make policy with (young) people, not over them, in the very sense of "Nothing about us without us": (Young) People need to be met where they are and be included in the process.

Good cybercrime policy, therefore, is a shared responsibility and can only be developed in a shared effort – policy experts, law enforcement, education and awareness, academia and research, and those who are affected.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

Private sector

Private sector organizations can of course fall victim to cybercrime. In this case, the most successful course of action is to collaborate with law enforcement: to detect as well as to fight. But private sector organisations also can be a valuable stronghold in the fight against cybercriminality.

It's the human factor of cybercrime private sector organisations can influence: On the one hand, people can be a big liability with regards to cybersecurity – and they can also be a great defence. Employees need to be regularly trained and educated on risks. Organisations should become more attractive employers and give (young) people a purpose and path in life which is more (financially) attractive than hacking at home. Youths, however, are not a natural counterpart for the private sector, not least because they usually don't have too much spending money. As a result, developing attractive working alternatives for young people makes it essential to involve them in the process.

Academia and research

Important takeaways from the CC-DRIVER 2021 European Youth Survey are: Cybercrime is gendered and cybercrime is related to age, insofar as some forms of cyber aggression are more pronounced during specific age spans. This shows that to fight cybercrime, we need to know and understand what social and biological developments young people go through in their teenage years in order to implement positive changes, offer help during challenging times, and trigger useful behaviours.

Research (and implementation) so far often focuses on victims and perpetrators. An important topic for future research should be regarding bystanders and the huge difference their behaviour can make: Under what circumstances do people look vs. look away? When do they help and when make it worse?

Research can then be helpful when it is informed from different disciplines and results are accepted and implemented. Therefore, research is an important cog in the wheel of fighting cybercrime: Cybercrime is a shared responsibility.

Law enforcement

Traditional crime is declining while cybercrime is rising. While traditional crime can cause much harm, cybercrime can have easily hundredfold the impact. Along the lines of a counter-terrorism method, law enforcement can implement the 4D approach to prevent and fight cybercrime:

- Prevention
  - Deter – public awareness
  - Divert – positive alternatives
- Fight
  - Degrade – degrade reputation
  - Disrupt – disrupt markets

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

Again, what becomes clear is that collaboration is the best way to fight cybercrime – by sharing knowledge as well as sharing practices (cf. "divert" – developing positive alternatives to a life of cybercrime in the private sector)

With regard to young offenders, an important question is whether they should be treated differently than adults. Yes – because their level of development is different. Youths are more impulsive and more risk seeking than adults. At the same time, they are not yet educated well enough – there's no subject "cybersecurity" at school or online police patrolling. Besides, they have their whole life ahead. But then how should they be treated? In order to answer this question, it is necessary to understand first why they are doing it.

Awareness and education

The main gap in awareness raising and education is to bridge the gap between generations regarding language, digitalness, and generally how to go about things. For adults it is oftentimes not that easy to understand why it is so important for young people to like and comment online, etc. But only by asking young people and listening to their answers can understanding grow and only by understanding, effective countermeasures can be developed (e.g. research, policy making) and implemented (e.g. policy making, law enforcement).

Conclusion

To sum up, the International Summit on Youth and Cybercrime provided different perspectives on the need to address youth cybercriminality by considering cybercrime a shared responsibility that requires the active involvement of policy makers, the private sector, academia, law enforcement , educators, and – very importantly – those involved: youths.

Further Reading

- Information on the International Summit on CC-DRIVER's website
- Stream of the International Summit
- CC-DRIVER Safer Internet Day Material
- CC-DRIVER Policy briefs
- CC-DRIVER Publications
- CC-DRIVER Newsletter
- CC-DRIVER Videos
- CC-DRIVER Blog
- CC-DRIVER / CYBERSPACE Law enforcement agencies' working group

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.