INTERNATIONAL WEBINARS AND LIVE EVENTS

The uses and misuses of technology during the COVID19 crisis*

Geneva Centre for Security Policy – 16 April 2020

*Moderated by **Dr Jean- March Rickli** - Head of Global Risk, GCSP:*

***Dr Clarissa Rios Rojas** – Research associate, Centre for the Study of existential risk, University of Cambridge:*
Existing **technologies** have been **repurposed** to fight COVID19.
Regarding problems such as the **lack of equipment** to treat COVID19 patients, **testing kits** or the production of **vaccines**, several technologies have been **combined** to provide **timely and efficient** responses to the COVID19. It is a great example of **use of technology to respond to the crisis**.

***Mr Ricardo Chavarriaga**- head of Swiss office of CLAIRE initiative on Human-Centred Artificial Intelligence:*
Development and success of technology depends on the way it is applied.
There are many different **applications of Artificial Intelligence (AI)** in the COVID19 response: the first is for the **monitoring of the spread** in news, flight tickets, medical reports, informal testimonies in social media in order to find patterns of the spread. This allowed the community to **identify early warnings**. The second application of AI is for **diagnosis**.
AI can also be used to regulate the **spread of information and mis-information**. Social media use tends to amplify information with a shock value, that can be mis-leading.

***Dr Robert Dewar** - Head of Cyber Security at GCSP*:
One of the side effects of the pandemic: **increase in cybercrime**. One of the most prevalent use of technology right now **is through *phishing emails***: a**rtificial links implanting virus in computers**. Links pretend to talk about COVID19 or from to be issued by government authorities.
Important work to address **people at risk not only of the virus but also from cyber-attacks**.
We're seeing an **increase in criminal activities**. Criminal actors are taking advantage of the **fear of people** regarding the virus. The way hackers and criminal activist operate is **not new**, they **use the environment at their advantage**. The **scale is new**, and is broader.

***Lennig Pedron** – President of ICON, NGO:*
Cyber criminals are the **actors exploiting the most the pandemic**. With people staying at home and being more **vulnerable to attacks**.
We are in a **cyberattacks sprint and a wave of misinformation**. In this pandemic, we face both a **physical and an informational attack, through "infodemic**". Hackers are learning and adapting.
Impacts of COVID19 pandemic: impact on cybercrime ; victims; phishing attacks; sexual material exploitation online; fraud; misinformation.

***Dr Marcello Ienca -** senior researcher at the Health Ethics & Policy Lab:*
It is **ethically challenging** to use **digital data for surveillance purposes**. However, it is also **ethically challenging not to use** digital data if the processing of these data can **save lives**. A certain temporary **sacrifice of rights can be justified** if it can prevent deaths.
However, **if we sacrifice** some degree of information and privacy, we need to be very **clear and transparent** about how do we do it and what it implies.
Digital tech can be used as a new tool of social control but while doing this, it is important for people to keep in mind that **once civil and political rights are removed, they are not always given back**. There is a risk that **digital tracing** can be used for other **surveillance purposes**.