COMMUNITY OF DEMOCRACIES

GLOBAL PRINCIPLES FOR UPHOLDING INFORMATION INTEGRITY ONLINE WORKSHOP

MAY 11, 2023

SUMMARY

Governing Council Members of the Community of Democracies (CoD) attended the second workshop organized by Canada, in its capacity as President of the Governing Council, and the CoD Working Group on Democracy and Technology. The workshop consisted of a panel discussion on "Global Principles for Upholding Information Integrity Online," moderated by Canada's Ambassador to Poland, H.E. Catherine Godin. Following opening remarks from CoD Secretary General Thomas Garrett, the panelists engaged in a thought-provoking discussion on defining information integrity, the need for high-level principles, Canada and the Netherland's joint efforts to develop a Global Declaration on Information Integrity Online, and the multi-fold challenges they face or have identified as researchers, practitioners, government officials, and the tech industry.

Key takeaways for CoD members:

- Not only do we need high-level principles and norms for states, but we also need to agree to a shared set of definitions and terminology on information integrity and mis/disinformation.
- The focus should not solely be on the *content* of information operations. Instead, we need to analyze the tactics, techniques, and actors involved. This includes the role of generative AI in spreading disinformation.
- We should be investing in literacy skills for all. When possible, proactively debunking misleading narratives is crucial.
- Disinformation is borderless and it is important to understand that different countries and regions may be impacted differently by specific narratives (and malign actors).

Panelists:

- **Tara Denham**, Director General, Office of Human Rights, Freedoms and Inclusion, Global Affairs Canada
- **Justin Arenstein**, Chief Executive, Code for Africa
- **Givi Gigitashvili**, Digital Forensic Research Lab, Atlantic Council
- **Sam van der Staak**, Director for Europe, International IDEA
- **Marcin Olender**, Public Policy and Government Relations Manager CEE region, Google

DISCUSSION

The panelists had the opportunity to answer, react to, and discuss four main questions. The experts presented the following key takeaways:

Question 1: What are the biggest gaps in international efforts to protect information integrity online and what steps can we take to address them?

- We have to create common terminology and a structured taxonomy (a system of classification in groups or types) so that we all use the right language and terms when describing phenomena in the information integrity space.
- There is a need for a rules of the road, based on existing international law and human rights frameworks, that would clearly outline norms for countries and expectations for industry.
- The weaponization of content online is not always moral or political, but rather can be profit-driven. We have to follow the money and examine the shadow economy, too.
- Researchers lack access to data from platforms, which would allow them to better understand and track online trends and content moderation policies, amongst others. Instead of offering greater accountability, platforms are not providing adequate access to their data.

Question 2: How can we balance the need for protecting freedom of expression and open access to information with the need to combat disinformation and illegal content online, especially in different regional contexts?

- One approach could be a graduated response model that seeks to understand how “egregious” an online post is and whether it has been mass produced or AI generated to “pump out” revenue and sow discord in society. This would mean moving away from a one-size-fits-all approach.
- In the European Union (EU), there is a Strengthened Code of Practice on Disinformation 2022, which has been helpful in allowing platforms to “follow the money” and cut off the money supply of those “peddling” disinformation.
- We “work in a fog of war and fumble in the dark.” Generative AI has “turbocharged” disinformation campaigns and platforms need to come to the table. All stakeholders need to find constructive ways to work together (including platforms) to have more responsibility and respect freedom of expression.
- The focus shouldn’t be on the content or what is “truth”, but rather on the tactics, manipulated actions, techniques, actors, and problems. This also requires an understanding of regional differences and the public’s trust in government/legislation.

Question 3: What steps can be taken to improve digital literacy and media literacy among citizens, and how can this contribute to increasing resilience to disinformation and illegal content online?

- Literacy skills and training is crucial, and it can follow different models: a centralized model where literacy is taught in schools (the younger the better) or a decentralized model where the entire population (not just those in educational systems) can build up skills/resilience.
- Critics argue literacy is expensive and requires investment, but the cost of not having media literate populations is higher in the long term and in the face of increasing information operations.
- We need to communicate more strategically and in more transparent ways to build trust and actively pre-bunk narratives that are being spread.
- Finland ranks high when it comes to resilience to disinformation because of high trust in democratic institutions, high level of education for all, and a historical understanding of both the regional political situation and cross-border propaganda.

Question 4: What can be done to strengthen international cooperation and collaboration to protect information integrity online, and how can we ensure that any solutions are truly global and inclusive?

- Disinformation is “deliberately borderless to evade detection and control” and we need to change our vantage points to understand its impacts in different regions.
- While the West is focused on Russia and China, in many countries in Africa this isn’t the case because of the historical legacy of the USSR as the “liberator of Africa from Europe” (due to WWII). Instead, the “biggest threat” comes from Saudi Arabia, United Arab Emirates, and Qatar.
- There is a need for regional projects since working in a single country is not enough. There are calls for better capacity building, funding, and empirical research on information integrity.
- Currently, we’re seeing a drive for regulations on big tech and we need to find incentives to bring platforms to the table with solutions. This also includes fostering environments of trust so that data can be shared with researchers.