TTC Ministerial

Foreign information manipulation and interference in third countries

Foreign information manipulation and interference (FIMI) and disinformation is an ever-changing security and foreign policy issue, with a fast-evolving and complex threat situation. Russia's strategic and coordinated use of such activity in the preparation and execution of its war of aggression against Ukraine has increased global attention to the ways in which aggressors manipulate the information environment, amidst global conflict. Intentional manipulation by malign actors of the information environment and public debate threatens the functioning of democracies and the well-being of societies around the world. We are increasingly faced with hostile campaigns manipulating global, regional, and local audiences by spreading chaos and confusion, aiming to undercut trust in well-established/proven facts, global partnerships and alliances, universal values and international human rights, and democratic norms and processes. We also see attempts to corrode the international, rules-based order and fora such as the UN Security Council through manipulative behaviour that undermines democratic institutions and values.

The European Union and the United States are mutually concerned about foreign information manipulation and interference and disinformation; the long-standing cooperation on this issue between us has contributed to a mutual understanding of the threat and close exchanges on effective responses which respect human rights. The Trade and Technology Council proved to be a crucial forum to add another, even more strategic layer to existing and operational cooperation. Against this background, and next to other ongoing work in various different fora, the European Union and the United States have taken a number of actions to increase transatlantic cooperation to proactively address foreign information manipulation and interference and disinformation, while upholding human rights and fundamental freedoms.

Common methodology for identifying, analysing and countering FIMI - The European Union and the United States have built a close partnership around efforts to address such manipulative activity by actors that intentionally seek to undermine the rules-based international order. Operationally, information sharing and discussions of policy and responses have made considerable progress. The TTC provided the opportunity for fundamentally enhancing the existing cooperation on threat intelligence sharing as it pertains to FIMI. **The European Union and the United States have adopted a common standard for exchanging structured threat information on FIMI**, through a more interoperable and machine-readable approach. When fully operational, information will be shared more efficiently, effectively and with a greater level of detail when it comes to understanding the manipulative tactics, techniques and procedures. This standard that the European Union and the United States are now using to analyse FIMI and share information is comprised of the DISARM framework[1], the STIX[2] standard and the OpenCTI platform[3]. This approach will significantly strengthen our collective efforts to identify, analyse and counter FIMI by enhancing our common situational awareness of FIMI threats. At the same time, this standard and its elements are made up of open-source solutions, which is key to ensure an approach that can be used by stakeholders around the globe. We have begun socializing this standard with partners, and many have expressed a willingness and desire to align on the common methodology for identifying, analysing and countering FIMI. The

[1] The DISARM framework or the DISinformation Analysis & Risk Management is an open-source framework designed for describing and understanding the behavioural parts of disinformation/FIMI. It sets out best practices for fighting such activities through sharing data & analysis, and can inform effective action. The Framework has been developed, drawing on global cybersecurity best practices.

[2] https://oasis-open.github.io/cti-documentation/stix/intro.html

[3] The OpenCTI project (Open Cyber Threat Intelligence) is a platform meant for processing and sharing knowledge for cyber threat intelligence purposes. It has been developed by the French national cybersecurity agency (ANSSI) along with the CERT-EU (Computer Emergency Response Team of the European Union).

European Union and the United States will continue to expand the network of partners around this shared standard and identify ways to fill gaps in terms of both capacity and funding.

Enhancing the preparedness against FIMI in third countries together with Civil Society Organisations ('CSOs) and platforms – The European Union and the United States organised several workshops to bring together civil society organisations, academic institutions, and media outlets from Africa and Latin-America, as well as platforms active in these regions, to explore how a multi-stakeholder community can step up its actions in coordinating the response to FIMI and how the European Union and the United States can support those actions. Next to this, we are gathering comparable insights from fact checking networks, academic institutions, and media outlets in African and Latin-American countries[4] to further deepen understanding of information manipulation and disinformation, such as narratives and tactics, in third countries and the needs and capacity of local and regional stakeholders to respond to those risks.

The European Union and the United States intend to further enhance support for capacity building in third countries, including by exploring additional actions to support and reinforce civil society and fact-checking organisations that facilitate the fight against FIMI on online platforms through our respective development funding mechanisms[5]. We are also supporting media literacy and basic digital competence training in Africa, Latin-America and EU Neighbourhood countries to ensure that citizens have the ability to recognise misinformation, as well as disinformation and other forms of FIMI, hateful and harmful speech and address these challenges through a bottom-up approach. A free and pluralistic media landscape is also essential to counteract misinformation, as well as disinformation and other forms of FIMI.

Call for action to platforms - The European Union and the United States also call upon online platforms to ensure the integrity of their services and to effectively respond to disinformation and FIMI, building on the example of the EU's Code of Practice on Disinformation. In particular, such responses should be targeted to the local or regional context, be grounded on research of local information environments and values, include adequate cultural and language capabilities, ensure timely and effective responses to requests from fact checkers, academic institutions, and media outlets, step-up efforts during critical periods, including elections and public emergencies, integrate the work of fact-checkers in their services, compensate fact-checkers for their work, and provide increased transparency and accountability around their actions to counter disinformation and FIMI.

[4] See for example EDMO's report on "Challenges and opportunities of cooperation among continental networks of fact-checking organizations" https://edmo.eu/2023/04/24/from-the-eu-to-the-world-challenges-and-opportunities-of-cooperation-among-continental-networks-of-fact-checking-organizations/

[5] The EU is currently undertaking a study looking at main actors and methods of disinformation in LATAM, Asia and Sub-Saharan Africa and providing recommendations for DG INTPA and partners to act in this space.