**Response to Committee on Foreign Affairs draft report on the state of cyber defence capabilities**

Dear MEP,

The RIPE NCC is one of the world’s five Regional Internet Registries, responsible for allocating and registering Internet number resources (IP addresses and Autonomous System Numbers) for Europe, the Middle East and parts of Central Asia. We also provide a number of technical services that support the functioning of the global Internet, including running one of the 13 root name server clusters that form the backbone of the global domain name system. As such, the RIPE NCC supports the online operation of millions of European businesses and lets European citizens enjoy the myriad benefits generated by digitalisation.

Given the role that the RIPE NCC plays in the technical operation of the Internet, we reviewed the European Parliament’s Committee on Foreign Affairs draft own-initiative report on the state of cyber defence capabilities with interest, and hereby offer several suggestions for your consideration.

First, we would urge the European Parliament, when considering restrictive measures available to deter and respond to cyber attacks (as stated in paragraph 11 of the draft report), to discount any such measures that would contradict the European Union’s values with regards to Internet governance and which could lead to a fragmented, more difficult to access and fundamentally less secure Internet for citizens of the EU and those beyond its borders.

As stated in the Joint Communication to the European Parliament and the Council: The EU’s Cybersecurity Strategy for the Digital Decade, “In line with its values, the EU strongly supports and promotes the multi-stakeholder model for Internet governance. No single entity, government, or international organisation should seek to control the Internet.”

The European Commission also stated during a meeting of the International Telecommunications Union in December 2020 that, “...impos(ing) a hierarchical structure to the Internet might bring high-risks of fragmentation, of decreased network resilience, and could harm the openness of the global internet. This does not seem to be in line with the European vision for the internet, which is one of a single, open, neutral, free, secure and un-fragmented network, supporting permission-less innovation, privacy and user empowerment. It would also represent a significant threat to the continued stability & security of the Internet.”

We therefore suggest adding the following text to the end of paragraph 11:

“...welcomes the imposition of such restrictive measures in July 2020 and October 2020 as a credible step in strengthening the EU’s cyber diplomacy toolbox, while respecting the European vision for the Internet, which is one of a single, open, neutral, free, secure and un-fragmented network;”

Second, we urge the European Parliament to expand its focus on working in close coordination with, “Member States, the EU institutions, NATO, the United States and other strategic partners” (as stated in paragraph 25) to include working with the technical experts in all Member States who are ultimately responsible for the technical operation of the Internet. Again, as stated in The EU’s Cybersecurity Strategy for the Digital Decade, “To advance multi-stakeholder cooperation on cybersecurity issues, the Commission and High Representative, in line with their respective competences, aim to reinforce regular and structured exchanges with stakeholders, including the private sector, academia and civil society, underlining that the interconnected nature of cyberspace requires all stakeholders to exchange upon, and take their specific responsibilities to maintain a global, open, stable and secure cyberspace.”

In light of the interconnected nature of the global Internet, and given the importance of Internet access to the protection and realisation of human rights, as recognised by the UN, we strongly believe that a foundational understanding of the technical impact of specific strategies — including restrictive or countermeasures with the potential to affect a large number of citizens’ Internet access — should be a crucial element of the EU’s cyber defence strategy. We would therefore ask the European Parliament to include “technical stakeholders” in its list of partners in the realm of cyber defence.

We would be happy to further discuss these issues with you or a member of your staff. Please don’t hesitate to let us know if you have any questions or require any further information.

Chris Buckridge

Head of External Relations

RIPE NCC