Effective EU cybersecurity legislation and decisive diplomacy in the cyberdomain

Suggestions for the new European Commission

Digital threats are ever-present. Improving the cyber posture of the EU is a top priority for the Netherlands. Optimizing our joint cybersecurity requires striking a continuous and complex balance between regulation and maintaining enough room for innovation. In doing so, solid legislation and *the use of foreign policy tools to discourage and deter malign cyber actors, are two sides of the same coin. With a view to the new European Commission, the Netherlands would hereby like to share its policy priorities in the field of cybersecurity, cyber diplomacy and digital diplomacy.*

A. Successful implementation of EU legislation and streamlining of the cybersecurity landscape

During the current legislative term, cybersecurity has been – rightfully so – made a top priority. Many policies, directives and acts that strive to strengthen the EU's cyber posture have been introduced. Whilst these efforts are crucial to ensure the cybersecurity of the Union, it is now time to shift the focus to implementation, where Member States, the Commission and the EU agencies work hand-in-hand towards tangible results.

The primary goal of the new Commission should be *evolution rather than revolution:* fully consolidate ongoing efforts, create necessary preconditions and incentives to support Member States to effectively implement the future-proof cyber legislation, and reduce complexity of and overlap within the EU cyber landscape. Due account should be given to this principal as part of impact assessments. Key is the focus on *implementation, harmonisation* and *innovation***.** The Netherlands proposes to take on board the following actions:

Implementation

- Perform a **stock taking exercise** of the different legal acts (sectoral and/or horizontal) and their interplay[i], coherence of the roles and responsibilities of different actors and networks active in the cyber domain and their interaction[ii], and its coherence with other non-legislative instruments[iii]. The exercise should include (non)legislative instruments in policy fields other than cybersecurity where they include references to existing cybersecurity measures.
- Ensure **sufficient financial means for CRA implementation** by small and micro companies, inter alia by exploring the possibility to financially support notified bodies via EU funding for the purpose of giving rebates to small and medium-sized enterprises (SMEs) who need a conformity assessment.
- Assist Member States in **implementing the NIS2 Directive** at national level through swift completion of the implementing acts and by providing support in the NIS Cooperation Group on specific topics such as harmonization of perspectives on risk management measures across the EU (art 21), the well-functioning of the European vulnerability database and information exchange on cyber incidents through the European CSIRT-network, and sharing of possible privacy-sensitive information with third countries.[iv]
- **Swiftly implement the Act on a high level of cybersecurity of EU institutions, bodies and agencies (EUIBA's)**, accompanied by a decisive Interinstitutional Cybersecurity Board, enhancement of the security culture within EUIBAs and an allocation of adequate resources for IT, striving towards 10 %.
- Timely implement the **cybersecurity requirements under the Radio Equipment Directive (RED)** with its accompanying standards – a precondition for a successful implementation of the CRA.
- **Modernize the Blueprint on Large Scale ICT incidents** via a Council Recommendation to provide a clear, agile and up to date overview of cyber crisis management procedures.

- **Assess the varying tasks of ENISA** (in the context of the review of the CSA) to strengthen ENISA's capabilities to provide support to Member States.

Harmonisation

Standards are crucial to further underpin the implementation of EU cyber legislation, leveraging the expertise of all involved and striving towards international alignment as much as possible.

Enable standardization organizations to rapidly develop cybersecurity standards together with industry necessary for implementation of CRA and other (legislative) measures, inter alia by providing sufficient funding for industry participation (within existing budgets of the current MFF and without pre-empting discussions on the next MFF) and by giving experts sufficient leeway between legal certainty and technical feasibility. **Where** possible, European (legislative) measures should align with **or build on** international standards **that are often already part of the cybersecurity policy of businesses and organisations**.

- Provide **insight to different sectors on cybersecurity related requirements** deriving from different EU legislation on the basis of a mapping supported by ENISA.[v]
- Undertake an in-depth assessment and consultation process to explore possibilities for **regulating and standardizing cybersecurity of ICT services and processes**, with a view to future revisions of the CRA and completing the regulatory framework for cyberspace.
- Ensure **effective coherence between the CRA and the CSA** based on a holistic approach.
- Develop a **joint action plan** with the EEAS to promote **EU cybersecurity standards in EU external relations**, such as the US-EU TTC and Digital Partnerships with value-aligned partners, and coordinate where possible, the development of cybersecurity standards with likeminded partners such as the US.
- Continue the **EU coordinated risk-approach** to the security of communication networks and ICT supply chains, as laid out in the 5G security toolbox and the NIS2.

Innovation

Besides a continuous investment in skills, more focus is needed on automation and innovation of cybersecurity services to scale-up cooperation between governments and the private sector - leveraging the opportunities new technologies offer us, like AI and quantum, to more efficiently provide such cybersecurity services, without closing our eyes to the risks.

- Engage in a regular dialogue and strengthen **cyber foresight capabilities on the future impact of key technologies** on the cybersecurity landscape at European level.
- Develop and deploy measures that stimulate research and development (R&D) cooperation to strengthen the Union's (global) technological leadership and digital open strategic autonomy in cybersecurity. Such measures should lower financial and administrative barriers for innovative SMEs and research institutes to participate and cooperate in national and EU-funded cybersecurity innovation projects. Particular attention should be given to innovation cooperation to ensure a timely and secure transition to post quantum cryptography.[vi]
- **Swiftly operationalize the European Cyber Competence Center** (ECCC) and its national counterparts in Member States, whilst coupling it with EU research & innovation funding streams and applicable EU policies and strategic agendas.
- Address the **skills gap**, through targeted efforts via the ECCC and the EU Cyberskills Academy in close cooperation between the Commission, Member States, the private sector and civil society.

B. Future development of the Cyber Diplomacy instruments

When it comes to deploying Common Foreign Policy and Security-instruments to protect our interests in the cyber domain, we are not yet using our full potential. The Netherlands believes that the urgency around the geopolitical impact of cyberthreats, aimed at the EU and its partners, needs to increase. The following measures may contribute to this ambition. The Netherlands is aware that these actions to a certain extend fall under the competence of the Council:

- More frequent discussions on **structural cybercampaigns and consequent options for action**, where possible accompanied by an INTCEN-briefing and input from ENISA and CERT-EU. It is important the EU focuses more on **patterns of behavior**, rather than individual incidents. Also, not every discussion of an incident needs to center around the option of a technical or political attribution. Often, it is warranted to focus more on technical aspects and public messaging.
- Encourage **more frequent use of Cyber Diplomacy Toolbox (CDT)** in order to make sure the EU maintains its credibility as a proactive geopolitical cyber actor. Sanctions are an essential element but also the 'softer' parts of the toolbox – as mentioned in the implementing guidelines – should be prioritized.
- **Consistent use of the Cyber Sanction Regimes**, as we can be certain that cyberthreats will not diminish. Consistent use is also instrumental to maintain the credibility of the regime. The Netherlands calls on the EEAS to regularly put forward new proposals, at least once a year, and to encourage Member States to do the same.
- Work out the possibility for **sectoral restrictive measures in response to cyberincidents** (as mentioned in the implementing guidelines), to assure a more sustained and strategic approach to the current threat landscape.
- More **frequent discussion on cyberthreats in PSC, CRP *and* FAC**. In line with the strategic compass, PSC should be provided with presentations, for instance once per presidency, on the cyberthreat landscape for the EU. Presentations could come from EEAS (incl INTCEN), Commission, ENISA and CERT-EU.
- Take the **NATO-EU partnership** forward together with all NATO Allies and EU Member States, in spirit of full mutual openness and in compliance with the decision-making autonomy of the respective organizations.
- Organize a **regular cyber exercise,** similar to the EU CyCLES cyber exercise, that involves all EU stakeholders. These should be organized (bi)annually.
- More strategic discussions on strengthening **joint activities in cyber capacity building**, including as part of the Global Gateway strategy. Cyber diplomacy policy discussions in the HWPCI need to be better synchronized with CCB efforts by DG NEAR, DG INTPA and other relevant DG's.
- Ensure that the **EU Digital4Development Hub provides continuous updates**, including calls for EU Member States to join Team Europe Initiatives on cyber security.
- Asses how **cyber capacity building can be utilized to strengthen partnerships** with third countries that are of strategic interest, to develop a stronger EU shared narrative in line with the Global Gateway strategy.

C. Digital Diplomacy

The further development of the global digital economy, as well as the Internet in its entirety, need to be based on democratic values and fundamental rights. To effectively navigate competing approaches from other geopolitical actors, the EU must prioritize investing in its economic strength and fostering

technical expertise. Additionally, it should leverage its normative influence to reinforce these values and rights. The Netherlands encourages the new Commission to take on board the following priorities:

- Coordinate **digital partnerships and cooperation with third countries more closely with Member States**, especially if discussions cover topics that fall within the responsibilities of different council working parties. Timely – and well prepared – discussions in, and involvement of, the HWPCI and the Telecom WP are key, prior to meetings with third countries, and after they have taken place.
- **Engage proactively in upcoming multilateral processes on digital governance, including Internet Governance.** 2024 and 2025 are key years for global discussions on the governance of AI, the Internet and broader digital issues with the negotiations of both the Pact for the Future and Global Digital Compact as well as the WSIS+20 review. A leading role for the EU and its Member States in these negotiations is necessary to enshrine both the concept of the public core and the necessary application of this multistakeholder model in new multilateral agreements.
- **Enhanced EU coordination for these processes.** In 2015 we managed to negotiate a relatively favorable WSIS+10 review, partially due to the close coordination within the EU and with like-minded partners. In order to replicate this result the upcoming years, enhanced coordination is required between the institutions and EU Member States, but also across different pillars of digital governance, e.g. through strong links between the HWPCI, Telecom WP, CONUN, HLIG and DDN, as well as between DG INTPA, DG CONNECT, DG HOME and the EEAS.
- An **ambitious stance on AI Global Governance**. Building on the Council Conclusions on the EU's Digital Diplomacy and the principles of the AI Act, the Commission should strive to play a leading global role in shaping a responsible, trustworthy, human rights based and secure use of AI that delivers solutions to the world's greatest challenges, building on principles that also underpin the EU's policy and regulatory initiatives and ensure its full compliance with international law.
- **Make more efficient use of existing diplomatic coalitions**. With regards to the Freedom Online Coalition, the Netherlands is in favor of close cooperation between the coalition and the EU. Other efforts, such as the Declaration on the Future of the Internet and the related recently instigated "Global Initiative for the Future of the Internet" need to be complementary to existing efforts, operationalize already agreed objectives of the EU and effectively mobilize global partners in support of our shared vision on digital governance.

---

[i] Horizontal legislation such as the Cyber Resilience Act, revised Network- and Information Securitiy Directive (NIS2), the Regulation on the European Cyber Competence Centre, the Cyber Security Act, the Act on a High Level of cybersecurity of EU institutions, bodies and agencies.. Sectoral legislation with cyber components such as Digital Operational Resilience Act, the Radio Equipment Directive, the Network Code on cross-border electricity flows, eIDAS regulation, European Electronic Communications Code, and potentially the EU Space Law.

[ii] Non exhaustive: EU cooperation networks such as EU CyCLONe, EU CSIRTs Network, the NIS Cooperation Group, Network of National Coordination Centres, the Network of Cross-Border Cyber Hubs, ENISA's National Liaisons Officers Network. EU organisations such as CERT-EU, ENISA, European Cyber Competence Centre, EEAS, Interinstitutional Cybersecuirty Board, Cyber Crisismanagement Taskforce and so forth.

[iii] Cyber Diplomacy Toolbox, EU Cyber Sanction regime, EU Cyber Defense Policy, EU Cyber Skills Academy, 5G toolbox, coordinated risk scenario's and assessments and other non-legislative initiatives deriving from the EU Cyber Strategy of 2021.

[iv] https://english.ncsc.nl/publications/publications/2024/february/22/non-paper-on-europe-wide-incident-reporting-under-nis-2

[v] For example, companies offering cloud services are potentially subject to requirements from NIS2, CRA, CSA, DORA, AI Act and Member States legislation.

[vi] Joint paper on quantum key distribution by Germany, France, Sweden and the Netherlands: https://www.aivd.nl/documenten/publicaties/2024/01/26/position-paper-on-quantum-key-distribution