The Cyber Diplomacy Compass. *07.2026 Edition*

Outcomes and the way forward from the first edition of the Cyber Diplomacy Compass: building a common approach to knowledge and exchange between diplomatic and stakeholder expert communities.

HELD AT

European Union Delegation to the United Nations
New York, 16–17 July 2026

ORGANISED BY

EU Cyber Direct · EUISS

PARTICIPANTS

50+ UN delegates and expert practitioners from across regions

IN SHORT |

The UN Global Mechanism on ICTs opens a permanent forum in which non-governmental expertise is called to play a critical role alongside Member States. In few fields is that role so warranted: the organisations that operate networks, respond to incidents, set standards and track threats hold much of the knowledge on which serious work on ransomware, critical infrastructure protection and emerging technologies depends. What remains unsettled is how that knowledge reaches the process, and whether delegations are equipped to use it. That was the question the Cyber Diplomacy Compass set out to explore.

This first edition, featuring the Chair of the first biennium, H.E. Ambassador López, the co-facilitators of the Dedicated Thematic Groups and Katherine Prizeman of the UNODA Secretariat, brought more than 50 UN delegates and expert practitioners from across regions into a working conversation ahead of the plenary week, on the same questions and before positions were fixed.

OUTCOMES

A proof of concept.

What came of it is less a set of positions than a proof of concept. Delegates arrived with questions they needed answered, practitioners with operational knowledge that rarely finds a route into a negotiating text, and put together informally the two produced an exchange of a quality that neither general statements nor corridor conversation delivers.

That was clearest in the exchange on norms and international law, where discussion moved quickly past whether the framework applies to how a State would demonstrate compliance in a concrete incident, a question that cannot be answered without those who handle incidents. Participants returned to the practical obstacles: the absence of shared terminology across diplomatic, legal and technical communities, the uneven functioning of points of contact, and the value of parallel diplomatic and technical channels, so that a technical exchange during an incident need not wait on a political one.

The session on capacity building described an ecosystem that is well populated but poorly coordinated, with recurring gaps in needs assessment, knowledge retention when personnel rotate, and evaluation of what programmes leave behind. DTG2 adds most value by improving what exists, keeping assistance demand driven and mapping who is already doing what. It also emerged that capacity must be understood more widely than it usually is: translating technical knowledge into policy language, and judging when in a cycle to intervene, are capacities in their own right, as unevenly distributed among expert communities as among governments. Building them is what turns presence into contribution.

On Artificial Intelligence the exchange was more exploratory, which was itself informative. Participants identified attribution, vulnerability management and critical infrastructure protection as the areas where emerging capabilities most directly unsettle existing assumptions, but the discussion surfaced questions faster than answers. Those questions are answerable only with the technical communities working closest to the capabilities in question.

The two days also clarified what makes such exchange work. Expert contribution during the OEWG years was real but invisible, resting on individual relationships and disappearing with the people who cultivated them. What the DTGs make possible is contribution that is timed, targeted and traceable: knowledge that arrives while text is being drafted, answers a question a delegation has posed, and whose use is visible in the record. All three proved achievable when the format was designed for them.

THE WAY FORWARD

What follows from this first edition of the Cyber Diplomacy Compass.

Start at national level. The obstacles identified in the norms session, absent terminology, uneven points of contact, communities that do not routinely speak to one another, are domestic before they are multilateral, and little of that can be resolved in New York. National multistakeholder platforms, established and resourced, give delegations a standing channel to the expertise held within their own cybersecurity ecosystems, and give industry, the technical community and civil society a route into national positions.

Structure the channel within the process. If contribution is to be timed, targeted and traceable, the format has to be built for it: speaking opportunities framed around specific questions rather than open invitations, briefers selected on transparent criteria with regional balance, and expert input acknowledged in plenary statements and DTG reporting. The exchange must also run both ways, since knowledge offered to a question no delegation is asking rarely reaches the text.

Sustain the community between sessions. The quality of the Compass exchange owed much to participants who already knew the terrain and each other. Fluency of that kind cannot be improvised on a December agenda.

The way forward towards December.

The immediate horizon is the first meetings of the Dedicated Thematic Groups, and the months ahead will determine what knowledge arrives there. EU Cyber Direct will use the intersessional period to take these three directions forward, and warmly invites delegations and expert communities to shape what the next edition takes up.

KEY TAKEAWAYS

01 **Move from agreement to application**

Early work should concentrate on how States apply norms, international law, confidence building measures and capacity building commitments in practice.

02 **Frame expert input around specific challenges**

Expert knowledge is most useful when States and facilitators identify the question, the expertise or the practical problem on which input is needed, rather than offering general speaking opportunities.

03 **Connect legal, policy and technical communities**

Operationalisation requires shared terminology, national coordination and practical structured exchanges involving diplomats, legal advisers, technical experts, infrastructure operators and security institutions.

04 **Reflect on novel approaches to capacity building**

DTG2 should strengthen needs assessment, coordination, knowledge retention and evaluation within the existing ecosystem, while keeping assistance demand driven and sustainable. Capacity also means the ability to translate technical knowledge into policy language, and to judge when in a cycle to intervene.

05 **Let knowledge flow both ways**

Diplomats need accessible expert knowledge, but expert communities equally need clarity on States' priorities, constraints and expectations. Knowledge offered to a question no delegation is asking rarely reaches the text.

06 **Build the contribution early, and keep it going**

Policy relevant contribution depends on coordination, concise recommendations and engagement with States, regions and the Chair throughout the intersessional period, not only during meetings in New York.

07 **Make stakeholder expertise contribution traceable**

Expert input acknowledged in plenary statements and DTG reporting is input that can be evaluated, and therefore repeated. Visibility is what turns contribution from a relationship into a practice.

If you are interested in the Cyber Diplomacy Compass or would like to learn more, please reach out to **Andrea Calderaro** at **andrea.calderaro@iss.europa.eu**.