



General Assembly

Distr.: General
21 May 2024
English
Original: Chinese/English/French/
Russian/Spanish

Seventy-ninth session

Item 93 of the preliminary list*

Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

Summary

The present report provides a consolidated summary of elements from the submissions received from Member States pursuant to General Assembly resolution [78/237](#), without prejudice to their individual positions. It consolidates States' views on security of and in the use of information and communications technologies, in particular on the future regular institutional dialogue on these matters under the auspices of the United Nations. Views received from Member States by the communicated deadline are reflected in full in the annex to the present report. The report concludes with observations of the Secretary-General.

* [A/79/50](#).



Contents

	<i>Page</i>
I. Introduction	3
II. Background	3
III. Views on regular institutional dialogue on security of and in the use of information and communications technologies.	4
IV. Observations and conclusions of the Secretary-General	10
Annex	
Replies received from Governments	12
Australia	12
Azerbaijan	15
Canada	17
China	19
Cuba	20
Czechia	21
Denmark	23
Egypt	24
Estonia	28
France	30
Georgia	36
Germany	37
Ireland	40
Japan	42
Latvia	45
Netherlands (Kingdom of the)	47
New Zealand	49
Russian Federation	51
Singapore	53
Türkiye	54
United States of America	74
Venezuela (Bolivarian Republic of)	79
Replies received from intergovernmental organizations	80
European Union	80

I. Introduction

1. By paragraph 8 of its resolution 78/237, the General Assembly invited Member States to continue to inform the Secretary-General of their views and assessments on security of and in the use of information and communications technologies, in particular on the future regular institutional dialogue on these matters under the auspices of the United Nations, and requested the Secretary-General to submit a report based on those views to the General Assembly during its seventy-eighth session for further discussion between Member States in the meetings of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 at its eighth session in 2024. The present report is submitted pursuant to that request.

2. On 5 January 2024, the Office for Disarmament Affairs circulated a note verbale to all Member States drawing their attention to paragraph 8 of resolution 78/237 and seeking their views on the matter. The views received by 1 May 2024 are reproduced as an annex to the present report. Views received after that date have been posted to the Meetings Place portal of the Office for Disarmament Affairs.¹

3. Section II of the present report provides background information related to State discussions on the matter of regular institutional dialogue on security of and in the use of information and communications technologies. Section III provides a consolidated summary of elements received from Member States, without prejudice to their individual positions. Section IV sets out the observations and conclusions of the Secretary-General.

II. Background

4. Under the auspices of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, States continue to discuss, in accordance with the agreed agenda of the working group contained in document A/AC.292/2021/1, the question of the establishment, under United Nations auspices, of regular institutional dialogue on related matters with the broad participation of States. Over the course of seven substantive sessions of the working group from December 2021 through March 2024, States engaged in focused discussions to further discuss proposals on regular institutional dialogue, including the proposal for a programme of action.

5. Through the working group's second annual progress report, adopted by consensus in July 2023 (A/78/265), States agreed, in principle, that a future mechanism for regular institutional dialogue would be based on the following common elements, and agreed to continue discussions on additional elements:

(a) It would be a single-track, State-led, permanent mechanism under the auspices of the United Nations, reporting to the First Committee of the General Assembly;

(b) The aim of the future mechanism would be to continue to promote an open, secure, stable, accessible, peaceful and interoperable information and communications technology environment;

(c) The future mechanism would take as the foundation of its work the consensus agreements on the framework of responsible State behaviour in the use of

¹ <https://meetings.unoda.org/ga-cl/general-assembly-first-committee-seventy-ninth-session-2024>.

information and communications technologies from previous reports of the open-ended working group and the Group of Governmental Experts;

(d) It would be an open, inclusive, transparent, sustainable and flexible process which would be able to evolve in accordance with States' needs, as well as in accordance with developments in the information and communications technology environment.

6. States further emphasized the importance of the principle of consensus regarding both the establishment of the future mechanism itself and the decision-making process of the mechanism. In addition, States, in a position to do so were encouraged to consider establishing or supporting sponsorship programmes and other mechanisms to ensure broad participation in the relevant United Nations processes.

7. Throughout the discussions in the open-ended working group on a future regular institutional dialogue on matters related to information and communications technology security, States reflected on the potential scope and objectives, structure, modalities, including for decision-making, and implementation follow-up. To facilitate discussions, the Chair of the open-ended working group provided a discussion paper on draft elements for a permanent mechanism on information and communications technology security in February 2024, followed by a revised version in May 2024. Two dedicated intersessional meetings on the topic of regular institutional dialogue were also requested through the second annual progress report. At those sessions, States would also engage in focused discussions on the relationship between the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security and the open-ended working group.²

III. Views on regular institutional dialogue on security of and in the use of information and communications technologies

General understandings and principles

8. In their submissions, several States emphasized the threat of malicious activity in the use of information and communications technologies and noted the growing international concerns regarding potential threats to international security and stability. Concern was expressed over the excessive development by a number of States of information and communications technology capabilities for purposes that were inconsistent with international law and with the objectives of maintaining international stability and security. It was noted that certain actors had breached international law through activity involving information and communications technologies. Concern was also expressed over the impact of malicious activity on the safety and well-being of individuals.

9. Some States noted that information and communications technologies could be a catalyst for human progress and development, while it was also noted that such technologies could be used for purposes that were inconsistent with the objectives of maintaining international security and in a manner that negatively affected economic and social development.

10. Many States emphasized that, in the light of the current security environment, it was necessary that a future regular institutional dialogue on security of and in the use of information and communications technologies be focused on further promoting an open, secure, stable, accessible and peaceful information and communications technology environment. Some States also underscored the importance of

² See [A/78/76](#).

international cooperation among States to maintain international stability in that domain.

11. Many States noted that there was a growing demand for a permanent decision-making mechanism on related matters under the auspices of the United Nations. Furthermore, many States also underscored the centrality of building on agreements reached in previous processes under United Nations auspices, including the groups of governmental experts and the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.³ Some States stressed the need to build on that “collective acquis”, noting that it was composed of existing norms of responsible State use of information and communications technologies, the applicability of international law to State use of those technologies, confidence-building measures and capacity-building. The view was also expressed that a future mechanism should create space for more in-depth discussions on practical implementation of the agreements previously reached. In that regard, the view was also expressed that the intergovernmental points of contact directory should serve as an integral component of a future mechanism.

12. Several States emphasized the importance of continuity in terms of the consensus outcomes reached in previous processes. In a similar vein, several States noted that the new institutional mechanism or platform should be established following the conclusion of the mandate of the ongoing open-ended working group on security of and in the use of information and communications technologies 2021–2025. Some States underscored that this should be done no later than 2026 to ensure continuity.

13. Several States emphasized the importance of avoiding duplication of international efforts in that area and cautioned against the pursuit of parallel processes, referring to related capacity challenges for delegations. Many States emphasized the importance of a single-track, permanent and inclusive regular institutional dialogue under United Nations auspices. Some States noted that the establishment of a single, inclusive, permanent mechanism would also contribute to predictability and institutional stability, while avoiding the need to negotiate new mandates at regular intervals. It was also noted that small and developing States with limited resources would not be able to sustainably participate in dual-track, parallel processes. Moreover, the view was also expressed that a future mechanism should serve as a comprehensive one-stop shop to address information and communications technology security.

14. Some States affirmed that international law, in particular the Charter of the United Nations, was applicable and essential to maintaining peace, security and stability in the information and communications technology environment. In that regard, the view was expressed that more in-depth discussions in a future mechanism could be held on how international law applied. The suggestion was made for a future mechanism to explore a dedicated workstream on that topic. The view was expressed that a future mechanism could serve as an inclusive framework for discussions on international law, including to share national views, convene expert briefings and explore capacity-building activities in that area.

15. States reflected on various fundamental principles that should underpin a future mechanism for regular institutional dialogue on security of and in the use of information and communications technologies, including openness, inclusivity and transparency, and that such a mechanism should be action-oriented, single-track and democratic in nature. The view was expressed that the future mechanism should be State-led and be underpinned by compliance with the principles of the Charter, such

³ See [A/65/201](#), [A/68/98](#), [A/70/174](#), [A/75/816](#) and [A/76/135](#).

as the sovereign equality of States, the non-use of force or threat of use of force, and the peaceful settlement of disputes. It was also suggested that it should incorporate appropriate flexibility and evolutionary development in line with the changing needs of States and the emergence of new tasks in the field of ensuring security in the use of information and communications technologies.

16. Several States referred to the proposal for a programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. It was noted that this proposal had been reflected in previous reports of related United Nations bodies, including the consensus annual reports of the open-ended working group. It was also noted that the proposal had been supported by a cross-regional group of States and could serve as a permanent structure for discussions on information and communications technologies in the context of international security established following the conclusion of the current open-ended working group.

17. Several States noted that a permanent open-ended working group should be established immediately following the conclusion of the current one mandated through 2025. Those States noted that the current open-ended working group had proven its efficiency and relevance as the most appropriate format for such a mechanism and for a permanent decision-making open-ended working group mandated to focus on further promoting an open, secure, stable, accessible and peaceful information and communications technology environment through, inter alia, the development of legally binding rules, norms and principles of responsible behaviour of States and the creation of an effective mechanism for their implementation, as elements of a future universal treaty on ensuring international information security.

Scope and objectives

18. Many States emphasized that the overarching objective of a future regular institutional dialogue on security of and in the use of information and communications technologies was to contribute to international peace and security in that domain. Several States noted that a future mechanism should promote an open, secure, stable, accessible and peaceful information and communications technology environment. Some States also noted that a future mechanism should facilitate dialogue and cooperation among States and contribute to the prevention of conflict and misunderstandings.

19. Several States underscored that the consensus recommendations of the previous United Nations processes, resulting in a consolidated framework for responsible behaviour of States in the use of information and communications technologies, should remain a central focus of a future institutional mechanism. Several States emphasized the importance of supporting the implementation of previously agreed outcomes, while others noted that a future mechanism should consider practical implementation of the agreements reached by the open-ended working group. The suggestion was made that a future mechanism could develop concrete guidance to support States in the implementation of the agreed normative framework, as well as enhance understanding of the framework itself.

20. In their submissions, States reflected on the need to further develop the existing framework. Some States noted options for identifying any gaps, developing additional norms or formulating new rules and legally binding obligations. Several States supported the pursuit of a legally binding instrument, while others underscored that further development and updating of the framework could take place, if necessary, in response to new threats as they evolved over time. Several States noted that the mechanism should strike a balance between two equally important aspects of work: implementation of the established framework and its further development.

21. The view was expressed that a future mechanism should look forward and backwards to focus on both observation and implementation of the existing agreed framework for responsible State behaviour in the use of information and communications technologies, in particular the enrichment of capacity-building, and the formulation of new norms in response to the latest developments, such as on data security, and the development of new action plans on capacity-building and a legally binding instrument.

22. Many States emphasized that the topic of capacity-building should feature centrally in a future mechanism. Some States underscored the importance of synergizing existing efforts, including related initiatives by the International Telecommunication Union and the World Bank. Reference was made to the agreed principles of capacity-building annexed to the second annual progress report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025.⁴ Several States noted that a future mechanism should facilitate capacity-building efforts, including through exchanging information on best practices. Several States underscored the importance of needs-based and targeted efforts. The view was expressed that the capacity-building function of a mechanism must be directly tied to States' national-level efforts to implement the normative framework of responsible State behaviour.

23. The possibility of a dedicated funding mechanism, drawing upon the experiences of existing facilities in other United Nations forums, to support related capacity-building efforts was also raised. A suggestion for a voluntary cross-regional "partnering system" was made, through which States of varying capacities could be matched to enhance cooperation and exchange good practices. There was a proposal for a multi-component capacity-building mechanism, which would include exchanges on the threat landscape, self-identification of capacity needs and the matching of needs with resources, as well as a "feedback loop" for exchanges on related experiences.

24. Several States noted that a future mechanism could serve as an overarching institutional framework for related initiatives and efforts in the area of information and communications technology security, including the intergovernmental points of contact directory.

25. Other potential areas of focus were suggested by States, including the development of a common understanding of how international law applied to the use of information and communications technologies and how existing norms could be adapted to the specific characteristics of the domain. The view was expressed that a future mechanism could advance discussions on existing and emerging threats and how international law, including international humanitarian law and human rights law, applied to the use of information and communications technologies by States. The development and implementation of confidence-building measures and mechanisms for practical cooperation between States were also identified as items to address.

Establishment, modalities and decision-making

26. States variously reflected on the modalities for the establishment of a future mechanism, as well as preparatory efforts prior to its establishment. The view was expressed that the contributions submitted by Member States in the framework of the ongoing open-ended working group, including on the programme of action proposal; the report of the Secretary-General on a such a programme of action, prepared pursuant to General Assembly resolution 77/37;⁵ the present report; and relevant

⁴ A/78/265, annex C.

⁵ A/78/76.

recommendations contained in the reports of the ongoing open-ended working group, should represent the basis for the establishment of the future mechanism in terms of its scope, structure and modalities.

27. Many States emphasized the importance of reaching consensus on the scope, structure and modalities of the future mechanism. Many States expressed support for the further elaboration and development of the mechanism within the current open-ended working group. Several States supported further focused, dedicated discussions in the current open-ended working group to develop the mechanism and seek consensus on its format and structure. With regard to the programme of action, several States supported the holding of dedicated intersessional meetings on that proposal in 2024 and 2025 to develop further aspects of the mechanism. Further discussions on the budgetary implications were also suggested.

28. The possibility of establishing a future regular institutional dialogue through a consensus resolution of the General Assembly was noted. In that regard, the view was expressed that an Assembly resolution should establish a permanent open-ended working group. The view was also expressed that the current open-ended working group could establish the future mechanism through a political declaration to be subsequently endorsed by the General Assembly. It was suggested that affirming States' commitment to be guided by the framework for responsible State behaviour could constitute a key element of such a political declaration.

29. With regard to the specific proposal for a programme of action, several States noted support for its establishment through a political declaration. It was suggested that the declaration could be complemented by a resolution of the First Committee describing the tasks, structure and modalities of the programme of action. The convening of an international conference held no later than 2026 to develop and adopt such a declaration was also suggested. The view was expressed that, should the current open-ended working group fail to reach consensus on a final report, including agreement on a mechanism, a more comprehensive international conference or other preparatory process established through the General Assembly would be needed to ensure the continuity of those important multilateral discussions.

Follow-up mechanism and implementation

30. States made various suggestions for the follow-up mechanism, including regular meetings, such as plenary meetings and review conferences, as well as intersessional meetings, including of technical working groups. Annual formal meetings of the mechanism were also proposed. Proposals on the frequency of plenary meetings varied from every two to every three years. The view was expressed that the future mechanism should convene biennial meetings to implement its agreed programme of work. The view was also expressed that it could be useful to periodically review the operations of the permanent mechanism to ensure that its approaches were relevant to the dynamic operating threat landscape.

31. Some States supported the creation of technical working groups to focus on specific priority issues, such as the applicability of international law and the development of new norms, rules and principles, as well as legally binding obligations, as appropriate. The view was expressed that technical working groups would constitute the essence of an action-oriented mechanism. A proposal was made for subsidiary subgroups to consider specific aspects of the mechanism's mandate. The view was expressed that meetings of technical working groups on specific issues during the intersessional period should be held in a hybrid format to facilitate the broad participation of States. It was noted that meetings of subgroups should not be held in parallel to ensure the full participation of delegations. To facilitate the broad participation of States, a fellowship programme was suggested.

32. States suggested various periodicity for potential review conferences, including every three, four or six years. Some States noted that such review conferences should review the framework for responsible State behaviour with a view to its updating, as necessary, and provide strategic direction for the mechanism's work. The view was expressed that review conferences should consider whether additional norms, rules, principles or binding obligations should be developed on a consensus basis.

33. Many States addressed the importance of consensus decision-making in a future mechanism. Some States emphasized that decisions on substantive issues must be taken by consensus. Several States expressed the view that the principle of consensus decision-making exclusively by States should be set out clearly in the document establishing the future mechanism. States suggested various forms of consolidating decisions by States in a future mechanism, such as progress reports to the General Assembly on a biennial basis and annual procedural reports accompanied by relevant consensus decisions.

34. Some States noted the possibility of voluntary national reporting in the framework of a future mechanism. Reporting on national implementation of the normative framework, as well as on national practices, was suggested. The use of existing tools such as the national survey of implementation of United Nations recommendations on responsible use of information and communications technologies by States in the context of international security and the United Nations⁶ was suggested.

35. Several States noted that while decision-making would remain the exclusive prerogative of States, interaction with regional and subregional organizations could be beneficial, including to leverage synergies and build on existing capacity-building structures and platforms. The suggestion was made to hold intersessional meetings with representatives of such organizations on an annual basis based on consultations with groups of countries and the respective chair of the future mechanism. The exchange of best practices at the international, interregional and regional levels was also proposed.

36. States variously reflected on engagement with non-governmental entities in a future mechanism, referring to modalities of participation in other United Nations forums as examples, such as the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the use of Information and Communications Technologies for Criminal Purposes and the Open-ended Working Group on Ageing. Many States noted that multi-stakeholder participation was important for the mechanism's future functioning. It was noted that inclusive stakeholder engagement in the future regular institutional dialogue would be instrumental to achieving the common objective of maintaining peace and security in the information and communications technology domain and could bring valuable expertise on matters such as threat assessment and the implementation of norms. Some States supported the participation of non-governmental entities in line with the modalities agreed in the current open-ended working group. Several States supported the formal participation of and regular consultations with stakeholders, while others stated that engagement with non-State actors should be strictly consultative and informal, such as through annual intersessional meetings.

37. Some States identified the Office for Disarmament Affairs as the appropriate entity to serve as the secretariat of a future mechanism.

⁶ <https://nationalcybersurvey.cyberpolicyportal.org>.

IV. Observations and conclusions of the Secretary-General

38. Safeguarding the peace and security of the information and communications technology domain remains an urgent task. While concern over the malicious use of these technologies by a range of actors grows, the international community is faced with a widening digital divide and a fast-approaching deadline for achievement of the Sustainable Development Goals. Concrete measures to prevent the extension and further escalation of conflict to this domain, including to protect human life from malicious activity, are imperative.

39. While there are formidable challenges facing the international community in maintaining the peace and stability of the information and communications technology domain, there is likewise a solid foundation upon which to build. Over the course of more than two decades, through processes under the auspices of the General Assembly, States have made critical progress in identifying existing and emerging threats, unpacking the applicability of international law to the use of information and communications technologies by States, developing a framework of responsible State behaviour in the use of these technologies, and considering confidence-building measures and capacity-building initiatives. This progress has been cumulative and consistent, and made on the basis of consensus agreements. Thus, there is a strong foundation for further progress.

40. The efforts undertaken by States in the framework of the ongoing open-ended working group on security of and in the use of information and communications technologies 2021–2025 are evidence of the potential for further concrete action towards the common objectives of a peaceful and secure information and communications technology environment. Consistent progress in this forum demonstrates that, with sufficient political will, not only can common agreements be reached, but practical actions can also be taken. In this regard, I welcome the consensus agreement reached by States to establish a global directory of intergovernmental points of contact to enhance interaction and cooperation between them. This is a meaningful step that promotes international peace and security and increases transparency and predictability.

41. Against this backdrop, States recognized the critical importance of maintaining regular institutional dialogue on such matters to provide sufficient space to make continuous progress. The relevance of these issues is only expected to increase as such technologies become increasingly ubiquitous and a larger part of our daily lives.

42. There is general agreement among States that such regular institutional dialogue is best suited to take place under the auspices of the United Nations, which provides a fully inclusive platform for such discussions. There is also common understanding that such a dialogue supports the objectives of strengthening international peace, stability and prevention of conflict in the information and communications technology environment. States also affirm several critical principles that would underpin such a dialogue, for example, inclusivity, transparency and an action-oriented approach. Furthermore, there is common understanding on the need for a single-track mechanism that facilitates the broadest participation of States.

43. Based on these broad agreements and widely held views, reaching consensus agreement on a future regular institutional dialogue on information and communications technologies in the context of international security appears as an achievable task. Building on the successes already achieved, States have a tremendous opportunity in the ongoing open-ended working group to find common ground on a single-track, permanent mechanism under the auspices of the United Nations that would operate in an open, inclusive and transparent manner. The common elements for future regular institutional dialogue agreed by consensus in the 2023 annual

progress report of the open-ended working group are a logical and useful point of departure. Such matters are too significant not to seize this opportunity to build further trust and confidence. A permanent mechanism under United Nations auspices represents the next logical phase of multilateral consideration of these matters, building upon past success and setting the stage for future progress.

Annex

Replies received from Governments

Australia

[Original: English
[1 May 2024]]

Australia welcomes the opportunity, in response to the invitation in General Assembly resolution [78/237](#), to provide its views on advancing responsible State behaviour in cyberspace in the context of international security and further regular institutional dialogue.

This submission builds upon submissions provided by Australia in response to resolutions [77/37](#) in 2023, [76/19](#) in 2022, [75/32](#) in 2021, [74/28](#) in 2020, [70/237](#) in 2016, [68/243](#) in 2014 and [65/41](#) in 2011 on developments in the field of information and telecommunications in the context of international security.

Australian Cyber Security Strategy 2023–2030

On 22 November 2023, the Minister for Cyber Security, Clare O’Neil, launched the Australian Cyber Security Strategy 2023–2030, which sets out Australia’s vision for domestic and international cybersecurity through a whole-of-nation approach to building cyberresilience.

The Strategy identified six shields to build stronger cyberdefences and bounce back quickly following a cyberincident: (a) strong businesses and citizens; (b) safe technology; (c) world-class threat-sharing and -blocking; (d) protected critical infrastructure; (e) sovereign capabilities; and (f) resilient regional and global leadership.

The Strategy sets out Australia’s continuing commitment to shape, uphold and defend international cyberrules, norms and standards, including by upholding international law and norms of responsible State behaviour in cyberspace, and deploying all arms of statecraft to deter and respond to malicious actors.

Uphold international law and norms of responsible State behaviour in cyberspace

Australia will collaborate with our existing partners and build new partnerships to uphold international law and the agreed framework for responsible State behaviour that underwrites our stability, prosperity, independence and sovereignty in cyberspace.

All countries have agreed to a rules-based cyberspace, founded on existing international law and norms. International law, complemented by agreed voluntary norms of responsible State behaviour, confidence-building measures and capacity-building, provides a robust framework for predictability and stability in cyberspace. When implemented and adhered to, this framework provides a toolkit to address threats posed by State-generated and State-sponsored malicious cyberactivity.

Australia will work with our international partners in United Nations discussions to clarify how international law applies in cyberspace and strengthen implementation of the framework for responsible State behaviour in cyberspace. Such efforts will include enhancing cooperation through regional forums, including as part of the Pacific Islands Forum and through engagement with the Regional Forum of the Association of Southeast Asian Nations.

Deploy all arms of statecraft to deter and respond to malicious actors

Australia will deploy all arms of statecraft to deter and respond to malicious cyberactors. Australia will work with our international partners to take action to impose costs on individuals and organizations that make cyberspace less safe and secure. This includes calling out instances where States act to undermine or breach international law and norms, and imposing sanctions on those who carry out or facilitate significant cyberincidents – when we have sufficient evidence and it is in our national interests to do so.

In all its actions, Australia will uphold existing international law and the agreed voluntary norms of responsible State behaviour in cyberspace.

Support a cyberresilient region

Australia will continue to work with our neighbours in the Pacific and South-East Asia to build a more cyberresilient region. Our cooperation and assistance will continue to be coordinated by Australia's Ambassador for Cyber Affairs and Critical Technology.

Australia is refocusing Australia's cybercooperation and capacity-building efforts to be more targeted, impactful and sustainable and to enable our neighbours to better prevent cyberincidents and recover quickly when they occur. Recognizing that people engage with cybersecurity issues in different ways, our efforts will continue to consider gender equality, disability and social inclusion. This includes continuing support for the United Nations women and peace and security agenda, as well as Australia's National Action Plan on Women, Peace and Security 2021–2031.

When severe cyberincidents occur in our region, Australia will be better positioned to respond to requests for assistance. Australia is establishing a regional cybercrisis response team in the Department of Foreign Affairs and Trade, drawing on expertise from government, industry and the technical community. In response to government requests following significant cyberincidents in the region, the team will help to contain the spread and impact of cyberincidents and restore critical services and infrastructure.

Regular institutional dialogue

Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security

Australia supports the establishment of a single, permanent, flexible, inclusive, transparent, and action-oriented mechanism, under the auspices of the First Committee, to discuss, implement and advance the framework for responsible State behaviour in cyberspace, agreed and reaffirmed by consensus by the General Assembly. The framework consists of international law, norms and confidence-building measures and is supported by coordinated capacity-building. The programme of action should provide a forum where all 193 Member States can meaningfully engage in both discussion and action on a regular and ongoing basis. The programme of action should be able to grow, pivot and develop – it should support implementation of the existing agreed framework and allow for potential further development of the framework, by consensus, as new threats and challenges arise.

In its resolution [77/37](#), the General Assembly welcomed the proposal to establish the programme of action and requested the Secretary-General to seek the views of Member States on the scope, structure and content for the programme of action. In that report ([A/78/76](#)), it was recommended that States continue to discuss

the potential scope, structure, principles, content, functions and follow-up mechanism of the programme of action proposal under the auspices of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, drawing on the views expressed in the report while also taking into consideration the regional and subregional consultations organized by the Office for Disarmament Affairs pursuant to General Assembly resolution [77/37](#).

The open-ended working group plays a key role in the elaboration and preparatory work for the programme of action. The programme of action should build on the hard-fought consensus gains and cumulative discussions of the past six successive groups of governmental experts and the inaugural and current open-ended working groups. A permanent mechanism represents the next phase or evolution in United Nations cyberarchitecture that builds upon what has come before and guarantees that these issues are accorded the attention and importance they merit going forward.

In its resolution [78/16](#), the General Assembly decided to establish a mechanism under the auspices of the United Nations, upon the conclusion of the 2021–2025 open-ended working group and no later than 2026, that would be permanent, inclusive and action-oriented, with the specific objectives affirmed in General Assembly resolution [77/37](#) and with the common elements for future regular institutional dialogue agreed by consensus in the 2023 annual progress report of the 2021–2025 open-ended working group.

Australia supports the proposal for an international conference to be convened, in 2025, to adopt the founding document of the programme of action, on the basis of the preparatory work done in the 2021–2025 open-ended working group.

Australia supports a founding document for the programme of action setting out the commitments of States and providing a mechanism that could be endorsed by an General Assembly resolution. The founding document, which could be set out as a political declaration, should:

- Endorse and reaffirm States' political commitment to the framework (including the application of existing international law in cyberspace) as agreed in the reports of the groups of governmental experts¹ and the report of the open-ended working group.²
- Recall existing and emerging threats to international security related to the malicious use of information and communications technologies (ICTs), building on the threat assessments contained in the reports of the groups of governmental experts and the open-ended working group.
- Establish a permanent institutional mechanism to advance implementation of this framework (including supporting States' capacities to do so) and the relevant modalities.
- Allow for further development and updates to the framework, as appropriate, to include consensus principles, recommendations and commitments in the event that the General Assembly, by consensus, endorses a report of the open-ended working group, the Group of Governmental Experts or other United Nations processes, or by consensus agreement at a programme of action review conference.
- Set out focus areas of work for the programme of action based upon issues that the international community agrees to discuss and address.

¹ See [A/65/201](#), [A/68/98](#), [A/70/174](#) and [A/76/135](#).

² [A/75/816](#).

- Clearly foster and encourage engagement with relevant members of the multi-stakeholder community in relevant areas.

In relation to rules of procedure, Australia reiterates that the programme of action should require agreement on all issues by consensus (including reports, recommendations and declarations).

To ensure that programme of action activities are evidence-based and data-driven, the programme of action should emphasize supporting implementation efforts, including through specific, targeted, coordinated capacity-building. Measures for dedicated capacity-building should be elaborated clearly within the programme of action. To promote targeted capacity-building that is based upon need and founded upon an evidence base, the programme of action might encourage Member States to periodically survey and self-report on their implementation of the framework (for example, every three years, or otherwise in line with the review conference cycle), using a standardized reporting mechanism, the national survey of implementation of United Nations recommendations on responsible use of ICTs by States in the context of international security (available at <https://nationalcybersurvey.cyberpolicyportal.org/>).

Australia recognizes the importance of the multi-stakeholder community, including civil society, the private sector, academia and the technical community, in contributing to a free, open, secure, stable, accessible and peaceful cyberspace. Australia proposes that the programme of action allow for regular and institutionalized consultation with relevant stakeholders.

In summary, Australia emphasizes that the programme of action should have a clear mandate that builds upon and reaffirms the agreed framework; be flexible, both substantively, in that the framework may be further developed by consensus, and procedurally; support implementation efforts through voluntary reporting and in implementing the framework through capacity-building; and be inclusive, in that decisions on matters related to international security remain the prerogative of States, while discussions and working groups are open to the multi-stakeholder community.

Australia looks forward to continuing to work with the Secretary-General, the Office for Disarmament Affairs and Member States to develop an effective, flexible and inclusive programme of action.

Azerbaijan

[Original: English
[1 May 2024]]

In recent years, cyberspace has evolved significantly, which offers prospects to enhance our daily life, from safety and security to the speed of communication and the use of digital technologies. Advances in cyber and critical technology underpin the future prosperity of the world, while they also have the potential to undermine stability and predictability. Therefore, it is essential to foster capacity-building measures, adequate protective capacities and digital services that will contribute to a more secure cyberspace.

Efforts taken at the national level to strengthen information security and promote international cooperation in this field

Azerbaijan supports the work of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, established pursuant to General Assembly resolution [75/240](#). As one of the co-sponsors of Assembly resolution [78/237](#), Azerbaijan has taken several steps to

strengthen its information security and promote international cooperation on cybersecurity.

It should be noted that the Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027, approved by the Decree of the President of the Republic of Azerbaijan dated 28 August 2023, serves to enhance the national information security level for secure utilization of modern information and communications technologies (ICTs) by the State, society and individuals, entailing the identification and implementation of measures to ensure the security of the State, private networks and critical information infrastructure, as well as the protection of personal data, thereby contributing to the creation of more favourable conditions for upholding human rights and freedoms enshrined in the Constitution of the Republic of Azerbaijan. Being the first strategy in the field of information security and cybersecurity in the Republic of Azerbaijan, it stands as an integral component of the State's policy regarding ICTs and outlines its primary goals, directions, priority tasks, respective solutions and a plan of comprehensive measures governing in this domain.

Moreover, in the Action Plan of the Strategy, under section 8.9.2.3., it notes “a continuous measure to organize the development of international cooperation and the study of international experience in the field of cybersecurity at the level of information security entities, including the National Computer Emergency Response Team and other computer emergency response teams”, with the primary goal being the development of cooperation with international computer emergency response team centres and securing membership in international computer emergency response team centres. Currently, practical work is being carried out with a view to expanding mutual activities and the exchange of experiences.

It is worth noting that the Rules for Ensuring the Security of Critical Information Infrastructure in the Republic of Azerbaijan and the Rules on the Structure, Creation and Management of the Register of Critical Information Infrastructure Objects were approved by the relevant decisions of the Cabinet of Ministers of the Republic of Azerbaijan in 2023.

In addition, as a result of the joint actions implemented by the State Security Service of the Republic of Azerbaijan and the Association of Cybersecurity Organizations of Azerbaijan, the position of our country in the international ranking table of the National Cyber Security Index shifted from eighty-sixth to fiftieth place in 2023.

The State Service for Special Communication and Information Security of the Republic of Azerbaijan has developed draft guidelines for ensuring information security, to be presented to government agencies aimed at ensuring information security in State institutions, including the identification of preventive and corrective measures against potential threats in the corporate information environment.

A cyberhygiene project has been implemented to enhance cyberresilience against cyberthreats and increase awareness in the field for employees of State institutions, as well as the private sector and business owners.

A cyberfestival, the Critical Infrastructure Defense Challenge 2023, jointly organized by the State Service for Special Communication and Information Security and the State Security Service, was held on 26 and 27 October 2023 and was aimed at enhancing the experience, knowledge and skills of local and foreign companies and public and private sector institutions operating in the field of cybersecurity, critical infrastructure and the financial and telecommunication sectors.

At the International Conference on Cyber Diplomacy organized by the National Institute for Research and Development in Informatics in April 2023 in Romania, it was decided that Azerbaijan would host the next conference in 2024.

As a result of practical activities carried out with a view to forming and developing the national ecosystem in the field of cybersecurity, Azerbaijan's position in international rankings has significantly improved. According to the Global Cybersecurity Index 2020, organized by the International Telecommunication Union, Azerbaijan improved its position by 15 points, ranking fortieth among 194 countries with a score of 89.31.

With regard to international collaboration in the mentioned field, participants from the various agencies of the Republic of Azerbaijan have attended the international events dedicated to cooperation in combating cyberthreats, exchange of information and experience on cybersecurity incidents, developing policies and strategies in the field of cybersecurity. This includes the meetings of the open-ended intergovernmental Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, the events held within the framework of CyberEast, the European Union Agency for Law Enforcement Training and the Training and Operational Partnership against Organized Crime projects jointly financed by the European Union and the Council of Europe.

Canada

[Original: English]
[16 April 2024]

The trend of increased malicious activity in cyberspace in recent years heightens the impetus to work efficiently to mitigate threats that could potentially undermine international security and stability.

The need for increased collaboration and action-oriented efforts must be matched with a commensurate United Nations mechanism on cybersecurity. Canada stresses the need to build on the collective acquis (the existing norms and our common understandings on how international law applies), and to create a space where more in-depth, concrete and technical discussions can take place, in a manner that is intrinsically intertwined with our discussions in plenary settings. Canada considers that the future regular institutional dialogue should function as a virtuous cycle of threat assessments, framework implementation discussions, capacity-building and review of any identified gaps to be addressed. Working on real-life matters, or on scenarios that emulate such matters, is more likely to shed light on tangible mitigation solutions. The future regular institutional dialogue should be action- and results-oriented and demonstrate sustained and measurable progress.

As owners and operators of the cyberspace infrastructure, and as our eyes and ears on the ground, the multi-stakeholder community is particularly well-situated to provide high-quality and unique input, in a consultative manner, into our work. Ensuring meaningful stakeholder engagement in the future regular institutional dialogue will be instrumental to achieving our common objective of maintaining cyberstability. Engaging the multi-stakeholder community in such a way is also the most promising approach to enhance and facilitate opportunities for the inclusion of small and developing States in our work. This in turn maximizes the potential for increased global cyberresilience for all. By being truly inclusive, the future regular institutional dialogue yields a stronger potential to receive the buy-in that can enable the good-faith implementation and development of responsible State behaviour in cyberspace.

Concerns and interests of all States, including with regard to the further development of the framework, should be taken into account in the future regular

institutional dialogue, through equal State participation at the United Nations. Decisions on substantive issues should be adopted by consensus.

Canada refers to, and reiterates, the views that it has expressed on the future regular institutional dialogue in the context of the Secretary-General's report on a programme of action, further to General Assembly resolution 77/37, of April 2023. These views notably reflect that Canada recognizes and welcomes the reports and recommendations adopted by consensus to date (e.g. the 2021 reports of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security and the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security). Canada considers that this open-ended working group's best course of action to deliver on its mandate, as provided for in General Assembly resolution 75/240, is to decide on a single-track, permanent, action-oriented and inclusive regular institutional dialogue.

Canada welcomes the opportunity to provide views, again, on the future regular institutional dialogue. Canada considers that the current open-ended working group mechanism is not optimal or sufficient to achieve our collective objectives. Canada would not support a repetition of or permanent renewal of the current open-ended working group mechanism. Rather, Canada strongly believes that a programme of action, developed within the open-ended working group and, ideally, agreed by consensus, is the best route to ensure a single-track, permanent, action-oriented and inclusive regular institutional dialogue on cybersecurity. This process would allow for more focused engagement on the implementation of norms and more in-depth discussion on how international law applies. It would also ensure better, action-oriented coordination (there is no such coordination within the current open-ended working group) between discussion on concrete implementation of the *acquis* and targeted capacity-building.

Canada recalls that substantive discussions on the programme of action as the future regular institutional dialogue have taken place since 2021, including in the context of the working paper circulated within this open-ended working group.¹ Canada recognizes and supports calls by other Member States to have a single-track process to discuss cybersecurity at the United Nations. As such, Canada cautions against creating a separate parallel process for regular institutional dialogue that would compete with the programme of action that received support from 161 Member States through General Assembly resolution 78/16. This would be an undue and unnecessary duplication, and it would impose unnecessary labour and financial costs on Member States.

The programme of action's structure and functioning will be decided through an international conference, at which a political declaration will be adopted. It is envisioned that the programme of action would be serviced by the Office for Disarmament Affairs as its secretariat. There will be review conferences to provide strategic direction, open-ended plenary discussions akin to those that exist under the current open-ended working group mechanism, and technical meetings or working groups to coordinate the elements of the thematic discussions that are relevant to address specific threats (e.g. identifying capacity-building activities most relevant to implement norms, and apply international law, to ransomware).

The programme of action will leverage investments in capacity-building and technical assistance as essential ingredients to further responsible State behaviour in cyberspace and to facilitate cooperation between States. It will establish regional

¹ See <https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf>.

engagement through cooperation with regional organizations to leverage synergies and coordinate initiatives.

The programme of action will go further than issuing Chair reports. In addition, it will show sustained and measurable progress. It will seek to fill the accountability gap between the acquis and actual practice by solidifying commitments and engaging in reporting or review mechanisms to enable optimal capacity-building activities in order to enhance responsible State behaviour worldwide.

China

[Original: Chinese]
[29 April 2024]

Views of the Government of China on a future permanent mechanism for institutional dialogue

With reference to General Assembly resolution [78/237](#) on developments in the field of information and telecommunications in the context of international security, the position and views of the Government of China on a future permanent mechanism for institutional dialogue are as follows:

The question of a future permanent mechanism is of great importance to how the United Nations proceeds with the development of information security matters. China supports the establishment of a single future permanent mechanism for an institutional dialogue on cybersecurity, with universal participation, within the United Nations framework. Reaching consensus on a future permanent mechanism in the framework of the Open-ended Working Group is the only option for all parties. China does not support any attempt to establish a permanent mechanism outside the Working Group. We are against starting over from scratch, as it would lead to division in United Nations information security processes and fuel geopolitical discord and confrontation between blocs. That is not in the interests of any member States.

With regard to the structure and functions of the future permanent mechanism, it should consolidate the important achievements made in maintaining the United Nations information security processes over the past 26 years and seek long-term development for the future. The structure can include two parts: one “looking back”, focusing on compliance with and implementation of the existing framework for responsible State behaviour in cyberspace, especially for enriching and improving action plans for capacity-building. The second part should be forward-looking, focusing on keeping pace with the times to formulate new standards, including for data security, promoting the formulation of a relevant legal instrument and proposing new action plans for capacity-building. China put forward the Global Initiative on Data Security to propose practical solutions to data security issues. The Initiative stipulates that countries must not require their companies to store in their territory data generated or acquired abroad; they must respect other countries’ sovereignty, jurisdiction and right to manage data security and that they must not directly access data from companies or individuals in other countries without such countries’ legal authorization to do so. The Initiative put forward specific proposals for the protection of critical infrastructure and supply chain security. It has been circulated as an official document of the United Nations General Assembly. China is prepared to work with all parties to promote the formulation of international rules for digital governance that reflect the wishes and respect the interests of all parties.

The future permanent mechanism should be led by Member States while at the same time ensuring multi-stakeholder participation, as is currently the case in the Open-ended Working Group. Review conferences could be held every five years, with

two or three plenary sessions convened every year. During the first three years of the review cycle, focused substantive discussions could take place and annual reports could be adopted, and decisions on important issues of broad interest to Member States could be taken, by consensus. In the fourth year of the review cycle, the preparatory process for the review conference could be initiated, and rolling texts could be drafted under the Chair's name. In the fifth year of the review cycle, substantive discussions could be held, primarily on the basis of the Chair's rolling text, with a substantive consensus concluded or negotiated, and the work for the next five years mapped out.

China stands ready to continue to actively participate in the relevant process and contribute to the establishment of the future permanent mechanism.

China hopes that these views can be reflected in the relevant reports of the United Nations Secretary-General.

Cuba

[Original: Spanish]
[29 April 2024]

Developments in information and communications technology are having an increasing impact in all areas of society. We must prevent this progress from jeopardizing the security of States.

Cuba reiterates that information and communications technology should be used in a peaceful manner and that States should behave responsibly, for the common good of humankind and to further the sustainable development of all countries.

We reaffirm that the only way to prevent cyberspace from becoming a stage for military operations is through joint cooperation among all States.

It is imperative that the General Assembly adopt a legally binding international instrument that complements applicable international law, addresses the significant legal gaps in the field of cybersecurity and makes it possible to effectively respond to the growing challenges and threats we are facing.

The open-ended working group on security of and in the use of information and communications technologies 2021–2025 is the appropriate forum for achieving this.

The role played by this inclusive, transparent working group in initiating regular intergovernmental dialogue in the area of security and use of information and communications technology should be respected and preserved. We call for the continuation of its work in that format, so that it can yield results that all States agree upon.

All States must respect existing international standards in this field. Access to the information or telecommunications systems of another State should be in line with the international cooperation agreements concluded and should be based on the principle of consent of the State concerned. The nature and scope of exchanges must respect the laws of the State which is granting access.

The hostile use of telecommunications, with the declared or hidden goal of subverting the legal and political order of States, is a violation of internationally agreed rules in this area and an illegal and irresponsible use of this media.

Cuban airwaves have been under constant attack from abroad, through illegal radio and television broadcasts disseminating programming designed to incite the overthrow of the constitutional order established by the Cuban people.

On average in 2023, over 7,000 hours of programming against Cuba per month were transmitted illegally using 21 frequencies from the United States, in contravention of the purposes and principles of the Charter of the United Nations, international law and the rules of the International Telecommunications Union.

The economic, commercial and financial blockade imposed by the United States Government against Cuba for over 60 years has caused severe losses to the Cuban people, including in the use and enjoyment of information and communications technology.

We reiterate that we unequivocally reject the imposition of unilateral coercive measures that run counter to international law and hinder assistance, cooperation and technology transfer.

In our region, it is recognized that information and communications technology has the potential to provide new solutions to development challenges, foster sustained, inclusive and equitable economic growth and help to achieve the 2030 Agenda for Sustainable Development.

Attention has also been drawn to the need to promote an open, secure, stable, accessible and peaceful information and communication technology environment, as reflected in the declaration adopted at the eighth Summit of the Community of Latin American and Caribbean States, held in Kingstown in 2024.

Cuba reiterates that international cooperation is critical to addressing the dangers of misuse of information and communications technology.

Czechia

[Original: English
[30 April 2024]]

Czechia is fully committed to advancing the global debate on cybersecurity in the United Nations and is grateful for the progress made so far by both the open-ended working groups and the Groups of Governmental Experts.

One of the key achievements of the open-ended working group and the Group of Governmental Experts is that they have developed and consolidated a framework for responsible State behaviour in cyberspace.

In this context, Czechia believes that the implementation of the framework for responsible State behaviour in cyberspace should be the central theme of the future institutional dialogue. Furthermore, Czechia supports the establishment of a permanent, single-track, inclusive and action-oriented mechanism under the auspices of the United Nations upon the conclusion of the current open-ended working group in 2025.

At the same time, we believe that, in order to establish a future institutional dialogue that would work effectively for the benefit of us all, it is important to continue the debate on its concrete form within the current open-ended working group. Currently, we as an international community have just over a year to conduct this debate.

With the regard to the debate within the open-ended working group, Czechia would like to draw your attention to the fact that the most developed, discussed and also consensual proposal for a future institutional dialogue is the programme of action to advance responsible State behaviour in the use of information and communications technologies (ICTs).

In contrast, we believe that resolution 78/237 on developments in the field of information and telecommunications in the context of international security does not build on the incremental approach and consensus reached in the open-ended working group in recent years. It appears to prioritize the interests of a narrow group of States.

The programme of action debate has been ongoing continuously since 2020, and Czechia has been actively involved in it. We recognize the value of the ongoing discussion on the programme of action within the open-ended working group in shaping the direction of the programme of action and in clarifying a number of potentially controversial points. We believe that it is important to continue this debate to define the content and modalities of the future mechanism. In the light of the above, we suggest that intersessional meetings and dedicated sessions of the open-ended working group should be organized in 2024 and 2025 to focus on particular aspects of the programme of action, including the budgetary implications.

In addition, Czechia would like to draw attention to certain aspects of the programme of action that emerged from the discussion about the programme of action and that Czechia considers to be the most significant advantages of the programme of action:

- The programme of action would bring institutional stability to the international debate regarding ICTs. It would represent a permanent institutional framework underpinning all cyber-related debates within the United Nations. This would avoid the need for periodic discussions about establishing a new working group dedicated to the use of ICTs.
- The programme of action would support the implementation of the framework for responsible State behaviour and enable further discussion on the framework's development, if necessary.
- The programme of action would work to operationalize capacity-building principles as part of its action-oriented objectives and foster implementation within cyber capacity-building projects. It could potentially leverage existing and potential capacity-building efforts, increase their visibility and improve their coordination. For example, it might be beneficial to explore coordination with cyber capacity-building activities undertaken in other venues such as the International Telecommunication Union.
- The programme of action would facilitate meaningful participation and collaboration with non-governmental stakeholders. Engaging the private sector, academia and civil society would bring valuable expertise on matters such as threat assessment and the implementation of norms, including measurement of progress made.
- The programme of action is designed to serve as a comprehensive framework, potentially encompassing other initiatives that have been discussed or agreed upon within the open-ended working group.

With regard to the specific modalities, Czechia is in favour of the idea of annual plenary sessions and specialized technical working groups' meetings in the intersessional period.

- The creation and termination of a particular working group would be entirely within the competence of States.
- The scope of and preparatory work for these technical discussions would be limited to topics identified in plenary sessions. The discussions would be attended, for example, by a limited number of experts from governments and, when relevant, other stakeholders such as academia. In particular, these working groups could focus on topics such as the protection of critical infrastructure,

cyberincident response and the applicability of concrete provisions on specific issues under international law in cyberspace.

- If this is set up well, we believe that having intersessional technical working groups can make our work significantly more efficient and also reduce the burden on individual delegations.
- It might be beneficial to consider holding not all intersessional working group meetings in New York, but to discuss other locations as well.

Denmark

[Original: English
[1 May 2024]

Denmark considers the implementation of the United Nations framework for responsible State behaviour in the use of information and communications technology (ICT) pivotal to ensuring a global, open, stable and secure cyberspace. The international community recognizes that existing international law and the Charter of the United Nations in its entirety is applicable in the ICT environment, and Denmark remains committed to the implementation of this framework in regard to cyberspace.

Over the past 20 years, significant progress has been made in developing a consolidated framework for responsible behaviour of States in cyberspace, including the application of international law, voluntary norms, capacity-building and confidence-building measures. The framework has repeatedly been endorsed by consensus by the General Assembly, most recently in the 2023 consensus annual progress report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025.

Denmark, together with the European Union, finds that parts of resolution [78/237](#) on developments in the field of information and telecommunications in the context of international security, adopted by the General Assembly on 22 December 2023, is based on non-consensual text. More specifically, the sixteenth preambular paragraph and operative paragraph 5 are based on proposals merely supported by a limited group of States. Denmark is concerned that this could lead to a reinterpretation of existing consensual documents. Therefore, Denmark was not able to support resolution [78/237](#).

Regarding the request pursuant to operative paragraph 8 of the resolution

The United Nations has repeatedly called for a permanent United Nations mechanism on cyberissues in the context of international security. With the General Assembly decision in October 2023 to establish a programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security, we have delivered on the aforementioned call.

Significant progress has been made in discussions on the future mechanism, and Denmark would like to express the following additional views concerning the future regular institutional dialogue.

This institutional dialogue should focus on supporting the implementation of the normative framework, as was also made clear by the 2019–2021 Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, which concluded that future institutional dialogue should be “an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven, and results-based”.¹

¹ [A/75/816](#), para. 74.

The programme of action should provide a permanent and institutional mechanism to follow up on the implementation of agreed norms, support and promote capacity-building, and provide and regularly update recommendations. At the same time, the programme of action should be flexible and allow further development of the framework, based on lessons learned during the implementation of the existing commitments.

Denmark finds it crucial to acknowledge that all stakeholders have a meaningful role in shaping the future of cybersecurity. To ensure an inclusive dialogue, it is essential to allow relevant stakeholders, such as businesses, non-governmental organizations, and academia, to formally participate in consultations and continuously share their views. This demonstrates a commitment to harnessing the collective wisdom of diverse perspectives. This inclusivity is vital for creating effective and comprehensive dialogue that addresses the multifaceted challenges of cybersecurity.

The programme of action could hold annual formal meetings and allow for technical meetings, working groups focusing on relevant aspects to meet throughout the year. The future mechanism should convene periodic review conferences to review the framework for responsible State behaviour, to update the framework, as necessary, and to provide strategic direction for the mechanism's work.

In the remaining part of this open-ended working group cycle, time and effort should be dedicated to further elaborating on aspects of the programme of action. To ensure a smooth transition to the programme of action, it is relevant to discuss the budgetary implications of a permanent mechanism and identify relevant actors in the United Nations to carry out these functions moving forward.

Egypt

[Original: English
[26 February 2024]]

I. Introduction

1. Member States share the growing international concerns regarding the proliferation of malicious uses of information and communications technologies (ICTs) and the excessive development by a number of States of information and communications technology (ICT) capabilities for purposes that are inconsistent with international law and with the objectives of maintaining international stability and security and that may adversely affect the integrity of the infrastructure of other States, to the detriment of their security in both civil and military fields.
2. The United Nations has already made progress towards addressing these concerns through the assessments and recommendations of the 2010, 2013, 2015 and 2021 Groups of Governmental Experts, as well as those of the 2021 Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security,¹ thereby establishing a cumulative and evolving framework for responsible State behaviour in the use of ICTs, elaborated by these processes.
3. Member States have been called upon to be guided in their use of ICTs by the 2010, 2013, 2015 and 2021 reports of the Groups of Governmental Experts and the 2021 report of the Open-ended Working Group, as well as the first and second annual progress reports of the ongoing open-ended working group on security of and in the use of information and communications technologies 2021–2025. Moreover, this

¹ See [A/65/201](#), [A/68/98](#), [A/70/174](#), [A/75/816](#) and [A/76/135](#).

agreed framework has stressed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.

4. The existing framework of norms, rules and principles for responsible State behaviour in the use of ICTs can reduce risks to international peace, security and stability, without limiting or prohibiting actions that are otherwise consistent with international law.

5. A proposed United Nations programme of action to advance responsible State behaviour in the use of ICTs in the context of international security was initiated in 2020 by Egypt and France and has been developed since then by a cross-regional group of States, as reflected in the final reports of the Groups of Governmental Experts and the 2021 report of the Open-ended Working Group, as well as the first and second annual progress reports of the ongoing open-ended working group.

6. The Secretary-General issued a report (A/78/76) consolidating States' views on the scope, structure, principles, content, preparatory work and modalities for establishment of the programme of action.

7. Any future mechanism on regular institutional dialogue must build on the acquis and the existing agreed framework that has been endorsed by the General Assembly by consensus.

8. The new mechanism or platform shall be established following the conclusion of the mandate of the ongoing open-ended working group after 2025. This means that there will be no chance of any duplication of efforts or the creation of parallel tracks. It should represent a "one-stop shop" and comprehensive platform under the auspices of the United Nations, addressing issues related to developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies.

9. Member States agreed in principle that the regular institutional dialogue mechanism would be single-track, State-led, permanent, inclusive, transparent and flexible.²

II. Objectives and scope of the future United Nations mechanism for regular institutional dialogue

10. To serve as a regular institutional dialogue platform that would allow the participation of all Member States in a single-track, permanent, inclusive, transparent, flexible, action-oriented, results-based and consensus-driven process that builds on the existing framework.

11. To promote an open, secure, stable, accessible, peaceful and interoperable ICT environment.

12. To prevent conflicts arising from the use of ICTs and seek the settlement of relevant disputes by peaceful means.

13. To anchor the established cybertools (points of contact directory and all other proposals to be adopted by the open-ended working group) with a view to maintaining their effective functioning and reviewing, as appropriate.

14. To elaborate concrete guidance to support Member States in their implementation of the agreed norms, rules and principles, including through promoting international cooperation and assistance.

² A/78/265, para. 55.

15. Its scope should focus on the following three pillars:

(a) **Implementation of the existing agreed outcomes.** Periodically assessing the implementation of the agreed framework by Member States by reviewing their voluntary national implementation reports, which should follow an agreed standardized reporting template;

(b) **Development of the existing framework.** Identifying the gaps and the diverse challenges faced by Member States in their implementation of the framework and promoting relevant actionable recommendations to respond to these challenges, as well as resuming deliberations on the conceptual issues such as the applicability of intentional law or the need for elaborating new rules and legally binding obligations in this domain;

(c) **Promoting capacity-building.** Taking practical steps to promote international cooperation and periodically assessing whether additional actions are needed to respond to the current and emerging challenges, taking into the rapidly evolving environment; exchanging information on best practices that can be implemented at the national, regional and international levels (including legislative and administrative frameworks, as well as measures taken towards protecting critical infrastructure); and providing concrete support for capacity-building based on the recipient State's own needs assessment and in accordance with the capacity-building principles contained in document [A/76/135](#). A dedicated funding mechanism for the relevant activities should be envisaged, including the possibility of relying on both existing and new instruments, such as the World Bank Cybersecurity Multi-Donor Trust Fund.

III. The establishment of the future mechanism for regular institutional dialogue

16. The views and contributions submitted by Member States in the framework of the ongoing open-ended working group on the programme of action proposal and the reports of the Secretary-General pursuant to General Assembly resolutions 77/380 and [78/237](#), as well as the relevant possible recommendations contained in the reports of the open-ended working group, shall represent the basis for the establishment of the mechanism in terms of its scope, structure and modalities.

17. Member States should continue their active participation in the ongoing open-ended working group established pursuant to General Assembly resolution [75/240](#) with a view to reaching consensus reports, including recommendations on the establishment of the future regular institutional dialogue mechanism.

18. The mechanism should be further elaborated and developed within the current open-ended working group in a manner that avoids any duplication of efforts or the creation of competing processes and preserves the consensual spirit in addressing the international security aspects of ICTs within the United Nations.

19. The mechanism shall be established after the conclusion of the current open-ended working group's mandate in 2025 through recommendations of the final report of the ongoing open-ended working group, while the possibility of establishing the future regular institutional dialogue through a consensual General Assembly resolution based on inclusive and transparent consultations and preparations could be considered. Member States may agree within the ongoing open-ended working group to establish the mechanism through a political declaration that could be endorsed by a General Assembly resolution, including the suggested modalities of the mechanism. The outcome of the Summit of the Future may include a reference to an initial agreement on this matter.

IV. Structure and possible modalities

Periodic meetings

20. The mechanism, which may take the form of a programme of action, should convene a review conference every six years that would focus on the following:

(a) Examining and reviewing the implementation of the mechanism, identifying the main priorities for action in the following years and consequently adopting a programme of work for subsequent meetings;

(b) Considering whether additional norms, rules, principles or binding obligations should be developed on a consensus basis to update the framework.

21. The mechanism should convene regular biennial meetings to implement the programme of work adopted by the review conference and follow up on the implementation of the agreed norms, rules and principles by the Member States through review of their periodic national implementation reports.

22. The Chair of each session shall convene preparatory consultative meetings prior to each review conference and follow-up biennial meetings.

23. The agreed mechanism may decide, by consensus, to hold intersessional meetings or to establish informal working groups to focus on specific related issues, including the applicability of international law and the elaboration of new norms, rules and principles, as well as legally binding obligations or instruments, as appropriate.

Reports

24. Under the agreed mechanism, Member States would be encouraged to voluntarily submit their national implementation reports every two years on a rotating basis, with a minimum of one report every three cycles (every six years). This process could be guided by the model national survey of implementation of United Nations recommendations on responsible use of ICTs by States in the context of international security. Member States may also wish to include in their national implementation reports a section that elaborates their priorities and needs in the area of capacity-building.

25. Each biennial meeting and review conference shall adopt a final report by consensus, including an outcome document to be submitted to the following session of the First Committee for its consideration and endorsement.

Decision-making

26. The programme of action shall adopt its decisions on substantive issues by consensus.

Secretariat

27. The Office for Disarmament Affairs should provide secretariat services for the mechanism.

Participation of stakeholders

28. The mechanism is an intergovernmental process in which negotiation and decision-making are exclusive prerogatives of Member States.

29. The mechanism will be committed to engaging with the relevant stakeholders in a systematic, sustained and substantive manner.

30. Relevant non-governmental organizations in consultative status with the Economic and Social Council in accordance with resolution 1996/31 would inform the secretariat of their interest in participating in the work of the mechanism.
31. Other interested non-governmental organizations relevant and competent to the scope and purpose of the mechanism should also inform the secretariat of their interest in participating by submitting information on the organization's purpose, programmes and activities in areas relevant to the scope of the mechanism. These organizations would accordingly be invited to participate, on a non-objection basis, as observers in the formal sessions of the mechanism.
32. Accredited stakeholders will be able to attend the formal meetings of the programme of action, make oral statements during a dedicated stakeholder session, and submit written inputs. Member States shall be encouraged to utilize the non-objection mechanism judiciously, bearing in mind the spirit of inclusivity.
33. Where there is an objection to a non-governmental organization, the objecting Member State will make known its objection to the Chair of the mechanism and, on a voluntary basis, make known to the Chair the general basis of its objections. The Chair will share any information received with any Member State upon its request.
34. The Chair will organize informal consultative meetings with stakeholders during the intersessional period.
35. The mechanism may facilitate coordination with the relevant regional and subregional initiatives, including through their possible participation and contributions.

Estonia

[Original: English
[30 April 2024]]

As mandated by the General Assembly in its resolution [78/237](#), Estonia would like to submit a national position on the future regular institutional dialogue on the security of and in the use of information and communications technologies (ICTs).

Over recent years, threats in the use of ICTs in the context of international security have continued to intensify and evolve significantly in the current challenging geopolitical environment. Increasing threats in the use of ICTs are leading to growing challenges related to negative effects on economic and social development and have implications for national and international stability. These implications continue to be at the forefront of multilateral discussions, as illustrated by the work of the Group of Governmental Experts and the open-ended working group.

Following the broad support of a cross-regional group of countries to establish a programme of action, we support the programme of action as a permanent institutional mechanism under the First Committee with a focus on the implementation of the agreed framework for responsible State behaviour in cyberspace, while also allowing for the further development of the framework, if appropriate. We believe that such a regular institutional dialogue would contribute to reducing tensions, preventing conflict and promoting their peaceful use.

This national position is an update of Estonia's national contribution included in the report of the Secretary-General on the programme of action ([A/78/76](#)), which builds on, inter alia, the progress reflected in General Assembly resolution [78/16](#) and discussions within the 2021–2025 open-ended working group.

1. **The programme of action should be based on the existing *acquis* and the framework for responsible State behaviour, focusing on State use of ICTs in the**

context of international peace and security. Estonia believes that ICTs must be employed in a manner consistent with the objectives of maintaining international stability and security and in accordance with the agreed *acquis* and the framework of responsible State behaviour. We underline that Member States should be guided in their use of ICTs by the 2010, 2013, 2015 and 2021 reports of the Groups of Governmental Experts and the 2021 report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. The programme of action mechanism should be built on these premises and be guided by the objective of preserving an open, stable, secure, accessible and peaceful ICT environment. Estonia finds that several existing or proposed initiatives, such as the global points of contact directory, would offer instrumental support to the effective functioning of the programme of action format.

2. The programme of action should be a neutral format providing for institutional stability. From the perspective of a small State, it is necessary to have clarity and institutional stability regarding further processes related to the discussions on State use of ICTs. Estonia thus advocates for the establishment of a single permanent structure for furthering the open-ended working group discussions, after the end of the current open-ended working group, on security of and in the use of information and communications technologies 2021–2025. We support furthering discussions on the structure, modalities and timeline for establishing the programme of action as a mechanism for advancing responsible State behaviour in the use of ICTs, taking into account the views of all Member States. Estonia supports the option of establishing the mechanism via an international conference, as agreed in the General Assembly resolution [77/37](#) by no later than 2026. Estonia believes that the proposed programme of action format would remove the need for the Assembly to debate the creation of new cyberprocesses every two, three or four years. It is our hope that the programme of action framework would be seen as a useful and neutral framework by Member States and there would be no need for parallel processes.

3. The programme of action should offer a holistic framework for advancing various topics proposed during the open-ended working group in an inclusive manner. We welcome the increasing interest of Member States in contributing to various topics that are focused upon during the ongoing debates of the open-ended working group sessions. The current discussions of the open-ended working group have been substantial, with a range of ideas proposed by different Member States. We believe that the programme of action framework could offer a “go-to” venue for Member States to raise issues related to ICTs and international peace and security. The programme of action could therefore provide for a holistic framework for these ideas to be brought forward and analysed in greater detail.

4. The programme of action should also include clear and transparent modalities for the substantial involvement of the multi-stakeholder community to further benefit from their expertise and knowledge. Engaging the multi-stakeholder community will support Member States in implementing the framework for responsible State behaviour and designing as well as delivering needs-driven capacity-building efforts to increase cyberresilience globally. Equally, the programme of action could also enhance regional engagement through cooperation with regional and thematic organizations to leverage and build upon relevant existing initiatives.

5. The programme of action should allow for more flexible, yet focused format for continuing the discussions on the framework of responsible State behaviour. Estonia would like to underline that the design of the programme of action framework should also take into account the challenges regarding limited capacities of small States and thereby be built on reasonable expectations as regards projected workload:

(a) We suggest that the elements of the programme of action mechanism could include annual plenary meetings to address topics under the main pillars of the framework for responsible State behaviour;

(b) We also support focused discussion in the format of working groups open to all interested participants, including on, but not limited to, threats, capacity-building, confidence-building, norms as well as international law. Another option could be focusing these working groups on more thematic topics such as critical infrastructure protection. The participation in the working groups should be voluntary and the creation of such workstreams would be decided by States in annual plenary meetings;

(c) We also support the organization of review conferences (for example, every four years), which would allow participants to take stock of progress and consider any further possible amendments to the mandate as well as the organization of work or the programme of action.

6. **Among other topics, the programme of action should offer an inclusive framework for the discussions on international law.** Estonia welcomes the increasingly active and substantial discussions on international law and how it applies to the State use of ICTs. Member States would benefit from a deepened understanding of and shared views on how existing rules apply, and from a more detailed analysis of any possible gaps. The programme of action would be well positioned to offer an inclusive venue for continuing these discussions. In particular, the programme of action could offer a platform for the following elements in discussing international law: (a) continuing discussions on how international law applies to cyberspace; (b) sharing national views; (c) dedicated meetings on how international law applies in the use of ICTs, focusing on specific topics to allow for more detailed elaboration; (d) expert briefings; (e) scenario-based discussions; and (f) capacity-building on international law.

7. **The programme of action should be action-oriented and with a strong focus on capacity-building.** An integral part of the future discussions should be the implementation of the agreed-upon framework for responsible State behaviour. The programme of action could also encourage voluntary reporting of national implementation efforts, which would contribute to many goals such as confidence-building, transparency, as well mapping capacities and needs. The programme of action should take stock of existing capacity-building initiatives in a well-coordinated and complementary manner. For example, the design of the programme of action should take note of existing mapping exercises and resources, such as the Cybil Portal and the European Union CyberNet mapping of the cyber capacity-building projects of European Union member States.

France

[Original: French]
[30 April 2024]

I. Introduction

For more than 20 years, States have recognized that information and communications technology (ICT) is a catalyst for human progress and development, but that it can also be used for purposes that are inconsistent with the goal of maintaining international stability and security.

Since 2003, the First Committee of the General Assembly has established a series of working groups that have worked to maintain international peace, security and stability in the digital environment. To that end, these working groups have

consolidated a framework for responsible State behaviour in the use of ICT, which the General Assembly has approved by consensus in several resolutions.¹

The working groups have also discussed the establishment of a regular institutional dialogue to address issues related to the use of ICT in the context of international security.

It has been emphasized that such a dialogue should be especially focused on supporting the implementation of the framework. In particular, the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (2019–2021) concluded that the future regular institutional dialogue “should be an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven, and results-based”.² States also emphasized the “utility of exploring mechanisms dedicated to following up on the implementation of the agreed norms and rules”.³

States noted that the framework was cumulative and evolving in nature and that additional norms could be developed over time. They also noted the possibility of future elaboration of additional binding obligations, if appropriate.⁴ The future regular institutional dialogue must support the implementation of the existing agreed framework, but also allow for its possible further development in the future, especially in response to the emergence of new challenges and threats.

In this context, the proposal put forward since 2020 by a cross-regional group of States to establish a programme of action would provide the First Committee with a permanent institutional mechanism for monitoring the implementation of the agreed framework and, if necessary, for developing it further.

In his report on the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security (A/78/76), the Secretary-General recommended that States continue to discuss the potential scope, structure, principles, content, functions and follow-up mechanism of the programme of action proposal under the auspices of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, drawing on the views expressed in the report while also taking into consideration the regional and subregional consultations organized by the Office for Disarmament Affairs pursuant to General Assembly resolution 77/37.

The present submission is an update of the national submission of France for document A/78/76 that reflects the progress made in the light of the adoption of General Assembly resolution 78/16 and the ongoing discussions in the 2021–2025 open-ended working group.

II. Scope and objectives

As a mechanism of the First Committee, the programme of action would address issues related to the use of ICT in the context of international security. Its main objective would be to contribute to the maintenance of international peace and security by preserving an open, safe, stable, accessible and peaceful digital environment.

¹ See General Assembly resolutions 70/237 and 76/19.

² A/75/816, annex I, para. 74.

³ A/75/816, annex I, para. 73.

⁴ General Assembly resolution 76/19, tenth preambular paragraph.

To that end, the objectives of the programme of action should be:

- Cooperation: to reduce tension, prevent conflict and promote the peaceful use of ICT through a cooperative approach to addressing cyberthreats and inclusive dialogue among States and with stakeholders.
- Stability: to promote stability in cyberspace by supporting the implementation of, and, where appropriate, further developing the framework for responsible State behaviour on the basis of international law, including international humanitarian law and human rights law, norms of responsible State behaviour, confidence-building measures and capacity-building.
- Resilience: to contribute to bridging the digital divide and strengthening global resilience by implementing the framework for responsible State behaviour.

III. Structure and content

Organizational structure

The programme of action could be based on a policy document which would serve, *inter alia*, to:

(a) Reaffirm the political commitment of States to the framework for responsible State behaviour, as affirmed in the relevant resolutions and reports.⁵ This founding commitment would take into account the consensus outcomes adopted by the open-ended working group on security of and in the use of information and communications technologies 2021–2025, such as the establishment of a global intergovernmental directory of points of contact, the possible establishment of a global cooperation portal or the idea of a threat registry. A future programme of action must be based on these consensus outcomes;⁶

(b) Establish a permanent institutional mechanism aimed at: (i) promoting the implementation of the framework, including through relevant capacity-building for States; (ii) further developing the framework, as appropriate; and (iii) encouraging multi-stakeholder cooperation in relevant areas.

The programme of action, as a permanent mechanism, could be based on the following organizational structure:

- Regular plenary meetings, which could be held on an annual or semi-annual basis (France is open to further discussions on the optimal periodicity of such meetings, taking into account States' capacities and the need for the programme of action to keep pace with developments in the digital field). These meetings would make it possible to: (a) discuss existing and emerging threats; (b) consider the implementation of norms, rules and principles; (c) continue discussions on how international law applies to the use of ICT and identify potential gaps; (d) discuss the implementation of confidence-building measures; (e) identify capacity-building priorities, including on the basis of voluntary reporting; and (f) identify actions to take in the future and determine the work programme for intersessional meetings. Consensus decisions could be taken at the annual meetings to create technical workstreams, which would be open to

⁵ Including General Assembly resolution [76/19](#), the 2010, 2013, 2015 and 2021 consensus reports of the groups of governmental experts, the 2021 report of the Open-ended Working Group (2019–2021) and the first progress report of the 2021–2025 open-ended working group. It should be borne in mind that the future consensus outcomes of the current working group will enrich this cumulative and evolving framework.

⁶ See General Assembly resolution [77/37](#), second preambular paragraph, and Assembly resolution [78/16](#), second preambular paragraph.

all States and stakeholders, to address specific issues (see below). The participation of technical and legal experts would be encouraged.

- Intersessional meetings, which would advance the work programme agreed upon at the annual meetings. They could take the form of technical open-ended meetings or working groups focused on specific workstreams, in line with the priorities and areas of work identified at the annual meetings.
- Review conferences, which could be held, for instance every four years, to consider whether the framework should be updated and to further develop it, if appropriate (see below). A dedicated workstream could be created to deepen discussions on how international law applies to the use of ICT, and to assess whether there are gaps in the framework that might warrant its further development.

Content

(a) Promoting implementation of the framework

Under the programme of action, voluntary reporting on national measures taken to implement the framework would be encouraged, either through the establishment of a purpose-built reporting system or through the promotion of existing mechanisms (such as the model national implementation survey of the United Nations Institute for Disarmament Research or national reports to the Secretary-General). This reporting would make it possible to identify priorities with respect to the implementation of the framework and to assess capacity-building needs.

At the annual programme of action meetings, actionable recommendations on national implementation efforts could be adopted and regularly updated. Consistent with the organizational structure described above, open-ended technical meetings or working groups could be established at the annual meetings of the programme of action with the aim of advancing discussions on specific issues related to the implementation of the framework.

For example, a thematic priority for the implementation of the framework might be identified at an annual meeting (implementation of a particular norm or confidence-building measure, security of digital products and services, critical infrastructure protection, etc.). In order to further discussions on such a priority, share technical expertise and discuss best practices and challenges, a dedicated workstream could be established at the annual meeting. Work under the workstream would be open to all States and carried out at the intersessional meetings of the programme of action. The conclusions and recommendations of the open-ended technical meetings or working groups would be submitted to the next plenary meeting.

The programme of action would support capacity-building measures related to the implementation of the framework, and would serve to enhance multi-stakeholder cooperation in this area as well as the coordination of efforts with other relevant initiatives.

- States may wish to consider establishing, as part of a future programme of action, a voluntary fund to finance certain activities aimed at promoting the framework for responsible State behaviour. Such a fund could be modelled on the United Nations Trust Facility Supporting Cooperation on Arms Regulation.⁷ Initiatives or projects funded by this instrument should be in line with terms of reference, which could be defined at the first meeting of the programme of action (promoting adherence to the framework, adhering to the guiding

⁷ United Nations Trust Facility Supporting Cooperation on Arms Regulation, see <https://disarmament.unoda.org/unsca/>.

principles for capacity-building agreed upon in the final report of the Open-ended Working Group (2019–2021), etc.).

- The programme of action would also be used to leverage existing efforts and initiatives. The programme of action meetings and the intersessional meetings of a technical working group on capacity-building would allow States to discuss capacity-building priorities (taking into account needs identified as a result of voluntary reporting) and stakeholders to present relevant initiatives. A “certification” system could be developed as part of the programme of action with a view to endorsing and promoting activities in line with its objectives.
- Representatives of other organizations (such as the International Telecommunication Union or the cybersecurity multi-donor trust fund of the World Bank) could deliver briefings at meetings of the programme of action to ensure coordination and complementarity between the capacity-building measures taken by different entities (each acting within its own mandate and area of competence).

(b) Developing the framework

In order to address new challenges, the framework could be updated as necessary (by enabling discussions on the further development of the framework, including by deepening common understandings on the norms and on how existing international law applies in the use of ICT, identifying any gaps in those understandings and, if appropriate, considering the need for additional voluntary, non-binding norms or additional legally binding obligations)⁸ at regular meetings or review conferences, on the basis of consensus.

(c) Multi-stakeholder participation

Mindful that “States bear primary responsibility for the maintenance of international peace and security”⁹ and that they must retain their central role (including exclusive decision-making power) in any First Committee process, France supports enhanced dialogue and cooperation with stakeholders in the context of a future programme of action.

- Decision-making and negotiation of outcome documents would remain the exclusive prerogatives of States.
- However, the value of further strengthening collaboration, when appropriate, with civil society, the private sector, academia and the technical community has been repeatedly emphasized by the relevant working groups of the First Committee.¹⁰ Cooperation with these actors could be critical to States’ fulfilling their commitments under the responsible behaviour framework. In addition, these stakeholders themselves have “a responsibility to use ICTs in a manner that does not endanger peace and security”.¹¹ Private actors can also bring valuable expertise to discussions and contribute to capacity-building efforts.
- The organizational arrangements for programme of action meetings should therefore allow stakeholders to participate in formal sessions, deliver statements and provide input, as is the case in other First Committee processes where their expertise is useful, such as the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems convened under the Convention on Prohibitions or Restrictions on the Use of Certain

⁸ See General Assembly resolution 78/16, para. 3 (b).

⁹ A/75/816, annex I, para. 10.

¹⁰ A/75/816, annex I, para. 22.

¹¹ A/75/816, annex I, para. 10.

Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects.¹² Such arrangements would be conducive to a more transparent process by allowing for multi-stakeholder dialogue in a formal setting.

- To ensure the inclusiveness of these meetings, the participation of stakeholders from each regional group should be encouraged and supported, including through specific sponsorship programmes.

IV. Modalities and preparatory work for the establishment of a programme of action

Preparatory work

France supports the continuation of focused and dedicated discussions in the 2021–2025 open-ended working group to further develop the programme of action and to seek consensus on its establishment.

In their final reports, the Open-ended Working Group (2019–2021) and the Group of Governmental Experts (2019–2021) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security recommended that the programme of action be further developed, including through the 2021–2025 open-ended working group. In its 2022 progress report, the 2021–2025 open-ended working group also called for focused discussions on the programme of action.

Through the regional consultations held in 2023 and the report of the Secretary-General ([A/78/76](#)), it was possible to gather the views of a large and diverse group of States. In his report, the Secretary-General stresses that consideration of the programme of action proposal in an inclusive and transparent manner, firmly based on previous consensus agreements and progress made in the General Assembly, is a worthwhile endeavour. In its second annual progress report, the 2021–2025 open-ended working group took up this endeavour by agreeing in principle and by consensus on “common elements”¹³ with a view to developing, in a constructive manner, a common understanding of a future mechanism for regular institutional dialogue.

In its resolution [77/37](#), the General Assembly provided that the report of the Secretary-General on the programme of action would be submitted to it and would serve as a basis for further discussion in the 2021–2025 open-ended working group. In its resolution [78/16](#), the Assembly highlighted that the 2021–2025 open-ended working group should play a key role in further work on the programme of action, with a view to its establishment upon the conclusion of the open-ended working group and no later than 2026.

Therefore, intersessional meetings and dedicated sessions of the 2021–2025 open-ended working group should be held in 2024 and 2025 to further develop the various aspects of the programme of action and to draft its founding document.

Establishment

France is in favour of continuing discussions on the precise modalities for the establishment of the future mechanism.

In its resolution [77/37](#), the General Assembly referred to the convening of an “international conference” as an option for establishing the programme of action (as

¹² Article 49 of the rules of procedure of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (adopted in 2016 within the framework of the Fifth Review Conference of the High Contracting Parties to the Convention).

¹³ [A/78/265](#), para. 55.

had been done for the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects). In its resolution [78/16](#), the Assembly decided to establish a mechanism under the auspices of the United Nations, upon the conclusion of the 2021–2025 open-ended working group and no later than 2026, that will be permanent, inclusive and action-oriented, with the specific objectives affirmed in General Assembly resolution [77/37](#) and with the common elements for future regular institutional dialogue agreed by consensus in the second annual progress report of the 2021–2025 open-ended working group. If States so decide, an international conference could be convened in 2025 to adopt the founding document of the mechanism, on the basis of the preparatory work done by the 2021–2025 open-ended working group.

This international conference should make decisions on the basis of consensus, at least on substantive issues. Relevant stakeholders should be allowed to participate (they could be accredited in a similar manner to the participants in sessions of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Combating the Use of Information and Communications Technologies for Criminal Purposes, as set out in General Assembly resolution [75/282](#)).

The General Assembly could then adopt a resolution welcoming the outcome of the conference and decide to convene the first meeting of the newly created mechanism.

Georgia

[Original: English
[20 March 2024]]

Regarding the future regular institutional dialogue on the use of information and communications technologies under the auspices of the United Nations: Georgia views the programme of action to advance responsible State behaviour in the use of information and communication technologies in the context of international security as the optimal approach to advance United Nations initiatives regarding cybersecurity and responsible State behaviour in cyberspace.

In a current security environment with unpredictable and rapid geopolitical developments, certain actors threaten the rules-based international order by using a combination of conventional and unconventional methods of warfare. Regrettably, there are cases when some actors breach international law through cyberoperations.

The global community must persist in holding such actors accountable for their illicit and unacceptable conduct in cyberspace, ensuring that legal consequences follow such actions.

The programme of action could function as an appropriate platform for targeted dialogues on the application of international law in cyberspace after the culmination of the current open-ended working group on security of and in the use of information and communications technologies 2021–2025 in 2025.

We advocate for the programme of action to serve as a unified framework within the First Committee dedicated to addressing cybersecurity concerns, providing a reliable structure conducive to action-oriented initiatives and tangible advancements.

The absence of capabilities on the national, regional and global scales presents a significant challenge. The programme of action should therefore aid national endeavours in enacting the normative framework and offer capacity-building assistance to narrow the digital gap.

Georgia welcomes the establishment of a global intergovernmental points of contact directory. This initiative marks a significant step forward in enhancing international cooperation and coordination in the realm of cybersecurity in the United Nations context.

Given the rapid pace of information and communication technology evolution, the future international framework must possess ample flexibility to ensure its future relevance. This international forum should incorporate a mechanism enabling the periodic revision of its framework through consensus, facilitated by regular plenary meetings or review conferences. These gatherings could reassess the existing framework and, if suitable, decide to enhance or develop it further.

Georgia firmly supports the transparent and inclusive multi-stakeholder approach, emphasizing the active involvement of both State and non-State actors in the framework of the institutional dialogue on these matters.

Germany

[Original: English]
[30 April 2024]

A. Underlying principles of the programme of action

Germany advocates the establishment of a programme of action as an action-oriented, permanent, transparent, flexible and inclusive forum for regular institutional dialogue on security of and in the use of information and communications technologies within the First Committee. The programme of action should be the single-track follow-up mechanism of the current open-ended working group on security of and in the use of information and communications technologies 2021–2025. It should become operational no later than 2026 to implement the results of the working group after the completion of its mandate, reiterating the decision contained in General Assembly resolution 78/16 to establish a mechanism under the auspices of the United Nations, with the specific objectives reaffirmed in resolution 78/37 and with the common elements agreed in the consensus second annual progress report of the 2021–2025 open-ended working group (A/78/265).

Parallel processes or double structures need to be avoided to not overburden States' capacity to meaningfully participate and to ensure action-oriented discussions. To prepare for a smooth transition, discussions among States about the scope, structure and content of the programme of action need to be continued within the current open-ended working group, with the ambition of finding consensus on the substance and modalities of the programme of action. The goal should be that all Member States endorse such a programme of action at a dedicated conference to be held back-to-back with the last session of the working group in 2025.

The overall purpose of the programme of action is to contribute to international peace and security in cyberspace by facilitating dialogue and cooperation among States on the implementation of the existing international framework for responsible State behaviour in the use of information and communications technologies (ICTs). This requires:

- Cyber capacity-building in accordance with the guidelines agreed in the 2021 final report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, as well as the agreed principles of capacity-building confirmed in annex C to the second annual progress report. Leveraging synergies with mechanisms contained in other forums will be instrumental in avoiding the duplication of structures and the dilution of resources.

- Confidence-building measures, including the effective implementation of the initial, non-exhaustive list of confidence-building measures agreed on in the second annual progress report (A/78/265, annex B), in particular the global points of contact directory.
- Exchange of best practices at the international, interregional and regional levels.
- Meaningful participation of relevant stakeholders.

Moreover, the programme of action should constitute the permanent platform for advancing discussions on existing and emerging threats, as well as on how international law, including international humanitarian law and human rights, applies to the use of ICTs by States. Further discussions and where appropriate, development of the international framework of responsible State behaviour in cyberspace should be possible within the programme of action in order to adapt and respond to new threats as they evolve over time.

The programme of action should provide the overarching institutional framework for other cybersecurity mechanisms currently under preparation in the working group, such as a cyberportal, as suggested by India, and a cyberrepository, as suggested by Kenya.

The overarching goal, specific objectives and underlying principles of the programme of action should be anchored in the form of a political declaration to be agreed by the General Assembly. The declaration should be complemented by a First Committee resolution describing the tasks, structure and modalities of the programme of action. Both the political declaration and the First Committee resolution should be based on the outcome of the dedicated conference to be held in 2025, as mentioned above.

B. Tasks, structure and modalities of the programme of action

Building on the lessons learned from previous and existing instruments, the tasks of the programme of action should be designed in a way that ensures the effective, inclusive and transparent participation of States and allows for measuring progress on the implementation of the framework of responsible State behaviour, including through a voluntary reporting mechanism such as the national survey of implementation of United Nations recommendations on responsible use of ICTs by States in the context of international security of the United Nations Institute for Disarmament Research (UNIDIR). Capacity-building and cooperation, among States as well as with regional organizations and non-State actors, are key to addressing those areas where national implementation is lagging behind.

Based on the common elements agreed in the consensus second annual progress report, the structure and modalities of the programme of action should include:

- (a) Annual conferences, to be held at Headquarters in New York:
 - (i) To review and measure progress of the implementation of the framework and the defined tasks;
 - (ii) To discuss the potential evolution of the framework including by further advancing the joint understanding of the application of international law in cyberspace;
 - (iii) To adopt decisions on specific topics;
 - (iv) To exchange information on current and emerging threats to international peace and security resulting from the use of ICTs;
 - (v) To further elaborate cyber capacity-building measures;

(vi) To consider the possible further evolution of the programme of action in an incremental way, based on the needs of Member States, taking into account changes in the threat landscape and following the understanding that the programme of action is a flexible instrument;

(b) The implementation and further elaboration of confidence-building measures based on the global points of contact directory that was established by the current open-ended working group. Beyond being a confidence-building measure in itself, the directory should provide the basis for the implementation of the global non-exhaustive list of confidence-building measures agreed in the second annual progress report, with the overall objective of reducing the risk of misunderstanding and conflict in cyberspace. It should also be used to discuss, adopt and implement additional global confidence-building measures. By facilitating the development and implementation of dedicated confidence-building measures, the directory would constitute a central pillar of the programme of action, focusing on the implementation of the existing framework;

(c) Review conferences every four to six years to allow for potential adaptation of the programme of action to the dynamic evolution of cyberspace and the associated risks to international peace and security;

(d) The Office for Disarmament Affairs acting as the secretariat of the programme of action. In addition to preparing the annual meetings and review conferences, the Office will also be in charge of administering the global points of contact directory and other confidence-building measures;

(e) UNIDIR providing States with relevant monitoring and review instruments (e.g. norms implementation checklists as agreed in the consensus second annual progress report) and conducting research activities related to the implementation of the framework;

(f) The possibility of additional meetings of technical workstreams in the intersessional period. Dedicated technical workstreams could focus, *inter alia*, on topics such as advancing cyber capacity-building, confidence-building measures, the application of international law, including international humanitarian law, and current and emerging threats. Participation in the workstreams should be voluntary, open to all States and regionally balanced. The number and set-up of workstreams, including the participation of stakeholders and the frequency of meetings and potential hybrid working modalities, should take into account the capacities of States to participate meaningfully and should be decided by consensus at the annual meetings.

States will retain the exclusive right to negotiate outcomes and make decisions within the programme of action. At the same time, the programme should provide for mechanisms to engage with non-governmental stakeholders (multilateral and regional organizations, civil society, the private sector and academia). The programme of action should provide for opportunities for inclusive and meaningful stakeholder participation in a similar manner to the modalities of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (in particular, any veto by a Member State of the participation of a stakeholder should be justified publicly; exclusion of stakeholders would be decided by a vote). This includes the right to speak and submit written inputs at meetings, review conferences and additional meetings of technical workstreams during the intersessional period. Furthermore, hybrid options of participation should be made available for the majority of formats in order to increase the inclusiveness of the deliberations.

In particular in the area of confidence-building measures and capacity-building, existing initiatives and structures at the regional and subregional levels or in other

forums should be leveraged and synergies built (for example with regional organizations, the World Bank Cybersecurity Multi-Donor Trust Fund and the Global Forum on Cyber Expertise).

Existing funding facilities in other United Nations forums, such as the Saving Lives Entity fund or the United Nations Trust Facility Supporting Cooperation on Arms Regulation in the area of arms control, could provide useful guidelines for establishing a mechanism to support cyber capacity-building efforts in the form of training and the sharing of best practices. Furthermore, a fellowship programme to facilitate broad capital representation from delegations of developing countries could be envisaged.

A voluntary, cross-regional “partnering system” could be established, in which a State that has high capacities with respect to the implementation of the framework of responsible State behaviour in cyberspace is paired with one or more States with lower capacities. Such a mechanism would enhance cooperation among States, facilitate dialogue and the exchange of best practices, and increase capacities of States for overall norm implementation. The “adopt a confidence-building measure” approach of the Organization for Security and Cooperation in Europe could be used as a reference model in that regard.

Ireland

[Original: English
[1 May 2024]

As an open society with a highly interconnected, digitalized economy, Ireland is acutely conscious of the deteriorating international security environment, particularly with regard to the increase in malicious cyberactivities. Recognizing this, we have taken action domestically, and with our European Union partners, to increase resilience, build our capacity to identify, prevent and deter threats, and to promote a global, open and secure cyberspace with international law and human rights at its core.

However, we have been unambiguous in our position that the global nature of the challenge requires a comprehensive international response. Ireland supported, and was encouraged by, the consensus development of the United Nations normative framework for responsible State behaviour in the use of information and communications technologies (ICTs). The framework was a crucial product of multiple consensus recommendations from both the Groups of Governmental Experts (2010, 2013, 2015 and 2021) and the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (2021). The two most recent consensus annual progress reports of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 also endorsed the framework.

Last year, Ireland published its national position supporting the application of international law in cyberspace, one of the four pillars of the normative framework. Ireland is committed to working with other European Union member States and international partners to act in accordance with the normative framework and to promote peace and stability through its implementation globally.

Ireland believes that the implementation and enhancement of the normative framework is essential to the maintenance of international security in cyberspace, and should therefore be central to any mechanism for regular institutional dialogue. The proposed future framework for regular institutional dialogue that may follow the present open-ended working group, as envisioned specifically in proposals for a programme of action, recognizes that the normative framework is essential, and allows for periodic review conferences to examine the framework.

Ireland has consistently given its full support to the particular approach to regular institutional dialogue for ICT security as advocated by the programme of action, which proposes an inclusive and action-oriented mechanism for a permanent future dialogue. The programme of action approach would provide for a permanent, regionally inclusive, multi-stakeholder and transparent dialogue under the auspices of the United Nations. Widespread support for the programme of action, as set out in resolutions of the First Committee of the General Assembly has been consistently in evidence, both during the deliberations of the open-ended working group and through the votes of a broad and regionally diverse group of States at the Assembly.

Ensuring all States can harness the benefits of ICTs, while mitigating the risks through capacity-building measures, is a key pillar of the normative framework, and a priority for Ireland. It is incumbent upon States to narrow the digital divides and build resilience to malicious cyberactivities.

The First Committee resolution [78/237](#), entitled “Developments in the field of information and telecommunications in the context of international security”, does not reflect the significance of the normative framework, or the broad range of perspectives voiced by many Member States, and therefore Ireland was unable to support it. Ireland does not believe that the approach proposed in this resolution can provide for the needs of the majority of Member States. In fact, Ireland has concluded that the resolution may serve to undermine the incremental and consensus-based method through which the open-ended working group has been able to make progress over the past years.

Ireland remains hopeful for the establishment by consensus of a future mechanism for future regular institutional dialogue before the end of the current open-ended working group, and will work with all States to promote an inclusive, action-oriented model that reflects the normative framework.

Discussions on how the programme of action approach in particular could be organized have included proposals for annual formal sessions, with open-ended detailed discussions and technical meetings on specific policy issues throughout the year. Technical groups could address issues such as gender, digital divides and the role of non-governmental entities in the implementation of the normative framework. Technical workstreams should be voluntary, open to all States, and result in operational conclusions grounded in the lessons learned from the implementation of the normative framework.

Building on the trans-regional support for First Committee resolutions that have advocated a programme of action approach, this particular mechanism could enhance regional engagement and cooperation with regional organizations to support needs-based capacity-building.

Encouragingly, the programme of action as proposed would also allow for formal participation and regular consultations with relevant stakeholders, including the private sector, academia and civil society, to provide input on relevant issues. Ireland strongly favours multi-stakeholder participation in regular institutional dialogue, firmly believing that it will better focus efforts on supporting States in implementing the framework for responsible State behaviour and of needs-driven capacity-building to increase cyberresilience.

In order to have a fully operational regular institutional dialogue by the end of the term of the open-ended working group, Ireland supports the organization of intersessional meetings and dedicated sessions of the open-ended working group in 2024 and 2025, including on budgetary implications.

Japan

[Original: English]
[30 April 2024]

1. Introduction

Japan supports the establishment of a programme of action to advance responsible State behaviour in cyberspace as a future mechanism. Japan believes that the programme of action is the right forum for the continuation of our discussions on responsible State behaviour in cyberspace. The programme of action, as an action-oriented framework, should serve as a platform to support the efforts of each country to implement the agreed norms and principles for responsible State behaviour by encouraging the sharing of best practices and mapping the specific challenges that each country faces.

The programme of action shall be the single follow-up mechanism of the current open-ended working group on security of and in the use of information and communications technologies 2021–2025 and become operational to implement the results of the open-ended working group after completion of the latter's mandate. The programme of action will be established after the mandate of the ongoing open-ended working group and will not be a dual track.

Japan would like to make the best possible contributions to discussions, bearing in mind that the programme of action will hopefully serve as a format for the actual implementation of the internationally agreed norms and principles.

This contribution is an update of Japan's national contribution included in the report [A/78/76](#) to take into account the progress enabled by General Assembly resolution [78/16](#) and the continuation of discussions within the 2021–2025 open-ended working group.

2. Scope/objectives

The purpose of the programme of action is to contribute to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment.

To that end, the programme of action should seek in particular to achieve the following objectives:

- (a) Provide recommendations to guide national efforts to implement the norms and principles of responsible State behaviour;
- (b) Encourage voluntary reporting on national practices in order to identify the needs and challenges of each Member State;
- (c) Support capacity-building, tailored to the needs and challenges, requested by recipient countries;
- (d) Be inclusive and ensure broad Member State and multi-stakeholder participation.

Moreover, the programme of action shall constitute a permanent platform for advancing recurrent items by facilitating discussions on existing and emerging threats, on the elaboration of confidence-building measures and on how existing international law applies to cyberspace.

3. Structure and content

(a) Structure to advance the implementation of the framework

In specifying the scope, structure and content of the programme of action, the efforts of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects can be used as a reference. The Programme of Action on Small Arms provides specific measures at the national, regional and international levels. Each country then submits a voluntary report on its legal and institutional development and other practices and holds an annual review meeting.

For the cyber programme of action, the voluntary report should include a checklist on the status of implementation of the norms in each country, such as the status of efforts to develop policies, laws and guidelines for critical infrastructure protection, and the status of incident response in each country or region. It would be meaningful if each Member State would also specify and include what kind of capacity-building is necessary. This exercise should facilitate providing a framework to support the national practice to implement the norms in each country.

The structure and modalities of the programme of action should include regular plenary meetings on a yearly or twice-a-year basis to be held at the United Nations. The programme of action plenary meetings would be able to adopt, and regularly update, actionable recommendations for national implementation efforts. For example, plenary meetings may identify a thematic priority for the implementation of the framework, such as the implementation of a given norm, existing and emerging threats, protection of critical infrastructure, etc.

To support further exchanges on this topic, the plenary meetings may decide to create dedicated workstreams, or open-ended technical meetings or working groups, which would take place in the intersessional meetings of the programme of action plenary meetings and would submit their conclusions to the following plenary meetings.

To complement discussions on the future evolution of the framework, review conferences would be convened in the framework of the programme of action at a frequency to be determined with a view to taking into account the rapid evolution of technology and to not being burdensome, especially for delegations from developing countries.

The global points of contact directory established by the current open-ended working group would constitute an integral part of the programme of action for the implementation and further elaboration of confidence-building measures.

(b) Capacity-building

The programme of action would support capacity-building efforts in relation to the implementation of the framework, ensuring multi-stakeholder involvement.

It would be meaningful for the programme of action to identify the gaps in the capacity of Member States to implement the framework and leverage existing capacity-building initiatives so that the gaps can be filled.

During the programme of action meetings, briefings could be delivered by representatives of other organizations (e.g. Cybersecurity Capacity-building Centre of the Association of Southeast Asian Nations and Japan, the International Telecommunication Union and the World Bank Cybersecurity Multi-Donor Trust Fund) in order to ensure coordination and complementarity between capacity-building activities taken by each structure.

The programme of action should function as a platform under the auspices of the United Nations in order to synergize and leverage existing efforts implemented by other

regional organizations, rather than conducting capacity-building programmes on its own.

(c) International law and norms

In May 2021, Japan submitted and published the basic position of the Government of Japan on international law applicable to cyberoperations, and reaffirms that existing international law, including the Charter of the United Nations in its entirety, is applicable to cyberoperations. It states its present position on how existing international law applies to cyberoperations, focusing its views on the most important and most basic matters. Japan continues to hope that the announcement of basic positions on international law applicable to cyberoperations by the Governments of various States and the application of international law in international and domestic courts and tribunals will deepen the shared international understanding of how international law applies to cyberoperations under the programme of action.

The programme of action would also encourage voluntary reporting of national implementation efforts, either by creating its own reporting system or by promoting existing mechanism (e.g. the national survey of implementation of United Nations recommendations on responsible use of ICTs by States in the context of international security of the United Nations Institute for Disarmament Research or national reports to the Secretary-General). This reporting would serve as a basis for identifying priorities regarding the implementation of the framework and map needs in terms of capacity-building.

The programme of action plenary meetings could discuss how to deepen the understanding of the application of international law in cyberspace. A dedicated workstream could also be created to advance exchanges on how existing international law applies to cyberoperations. The dedicated workstream could, on the basis of the mandate from the Member States, be employed to share national views and conduct scenario-based discussions. Such dedicated workstreams may focus on general issues, specific concepts of international law or thematic topics, such as cyberoperations against critical infrastructure, while also covering relevant principles of international law.

(d) Multi-stakeholder involvement

Stakeholders are at the centre of cyberspace, be it as owners and operators of elements of the infrastructure, or as the voice of communities. Given the interconnected nature of cyberspace, it is essential to engage the multi-stakeholder community in the United Nations discussion.

The programme of action would enable engagement and collaboration with the multi-stakeholder community, including to allow for the most optimal capacity-building activities possible.

4. Preparatory work and modalities for the establishment of the future mechanism

Japan supports further focused discussions within the 2021–2025 open-ended working group to further elaborate the future mechanism.

Latvia

[Original: English]
[30 April 2024]

The framework for responsible State behaviour in the use of information and communications technologies (ICTs) has for a long time – since 2003 – been on the agenda of the First Committee of the General Assembly and discussed in several Groups of Governmental Experts, as well as open-ended working groups, emphasizing the increasing importance of the responsible use of ICTs in maintaining international stability and security. Cooperation among States is vital to effectively address growing threats in cyberspace and to build confidence among States. For these reasons, it is time to decide on the establishment of a permanent mechanism within the United Nations to address cybersecurity matters in a long-term manner.

Cyberattacks are becoming more sophisticated, destructive and frequent than ever in the modern interconnected world. The cyberlandscape is evolving constantly. Cyberattacks against critical infrastructure, politically motivated attacks, ransomware attacks and malicious use of artificial intelligence (AI) are on the rise. The relevance of cybersecurity is therefore undeniable in the international security debate.

In order to tackle the unprecedented level of malicious activity in cyberspace, Latvia is increasing its own cybersecurity and resilience. Among other things, Latvia organizes and conducts cyberthreat hunting operations both nationally and within the European Union, and our governmental institutions share knowledge and experience with citizens and public and private entities. In 2023 and 2024, Latvia, along with other European Union Member States, has repeatedly publicly condemned malicious cyberactivities, including cyberattacks targeting democratic processes and institutions.

The proposal to establish “regular institutional dialogue” under the auspices of the United Nations has been discussed previously in the First Committee and is noted in the final report of the open-ended working group 2019–2021.¹ The open-ended working group 2019–2021 concluded that any future mechanism for regular institutional dialogue should be “an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven, and results-based”.² In the 2023 annual progress report of the open-ended working group 2021–2025, States agreed on common elements, most notably, on a single-track, State-led, permanent mechanism.³

Growing cyberthreats require State energy and resources to be focused on enhancing cooperation and trust among States in the long term rather than on discussions regarding the modalities of a new mechanism taking place every few years and risking future progress fragmentation. Latvia, as a small State, supports a single-track approach which would facilitate effective use of limited resources.

Responding to the call for the establishment of a permanent mechanism to advance responsible State behaviour in the use of ICTs in a coherent and long-term approach, a programme of action has been proposed.⁴ General Assembly resolutions

¹ Final report of the open-ended working group 2019–2021, paras. 68–74.

² Ibid., para. 74.

³ Second annual progress report of the open-ended working group 2021–2025 (A/78/265), para. 55 (a).

⁴ <https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf>.

[77/37](#)⁵ on the programme of action in 2022 and [78/16](#)⁶ on the programme of action in 2023 received broad support from States at the General Assembly, and this initiative has been developed in a transparent, inclusive and incremental manner.

Programme of action as a permanent United Nations mechanism

Latvia believes that, by resolutions [77/37](#) and [78/16](#), the General Assembly has granted a strong mandate to proceed with the establishment of the programme of action. The programme of action should be a permanent, inclusive, action-oriented, State-led mechanism within the First Committee and a platform for all States to participate. Its overarching objective would be to contribute to the strengthening of international peace and security and to the prevention of conflicts and misunderstandings among States. The scope of the programme of action should be matters related to the use of ICTs in accordance with international law and the implementation of the United Nations framework for responsible State behaviour in cyberspace. As noted in General Assembly resolution [77/37](#), the programme of action would “take into account the consensus outcomes adopted”⁷ by the open-ended working group 2021–2025.

Stability and security in cyberspace will be advanced by supporting the implementation and further development, if appropriate,⁸ of the framework for responsible State behaviour, based on the international law, including the Charter of the United Nations in its entirety. As agreed in the reports of the Group of Governmental Experts in 2013, 2015 and 2021 and the reports of the open-ended working group in 2021 and 2022, international law, including international humanitarian law, is applicable and essential to maintaining peace, security and stability in cyberspace.

In order to advance implementation of the framework for responsible State behaviour, the programme of action would support relevant and needs-based capacity-building activities. It is important to advance collective work on capacity-building and to share our experience and best practices to improve both national and global resilience to cyberthreats.

Annual formal sessions could be held in the framework of the programme of action. Between formal sessions, the work of the programme of action could be organized within technical working groups dedicated to specific issues. For example, a technical working group could work to further enhance understanding of how international law applies to the use of ICTs. Recommendations prepared by the technical working groups would be adopted at the formal sessions. Further priorities of the programme of action should be reviewed periodically during Review Conferences.

The technical groups could be created and terminated by decisions of the formal sessions. The technical working groups must be inclusive and open to all States, ensuring that national experts can participate offline or online (hybrid format). Decisions on the technical groups and on their working modalities should be made with consideration to the capacity and resources of small States.

⁵ General Assembly resolution [77/37](#), Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security.

⁶ General Assembly resolution [78/16](#), Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security.

⁷ General Assembly resolution [77/37](#), para. 2.

⁸ General Assembly resolution [76/19](#), preambular para. 10.

Regular and full-fledged dialogue with stakeholders – civil society, private sector, academia – is essential and should be facilitated through the programme of action. Their expertise in the ever-evolving cyberdomain is invaluable, and thus their input is relevant for advancement of the implementation of responsible State behaviour. Stakeholders themselves also “have a responsibility to use ICTs in a manner that does not endanger peace and security”⁹ as well, as they are the ones driving development of the new technologies.

Further focused discussions should be organized in 2024 and 2025 at the remaining sessions and intersessional meetings of the open-ended working group 2021–2025 to continue to elaborate the different aspects of the programme of action, including the modalities for its establishment. The programme of action should be operational upon conclusion of the open-ended working group 2021–2025.

Netherlands (Kingdom of the)

[Original: English]

[1 May 2024]

Introduction

The Netherlands continues to be deeply concerned by the growing risk of the malicious use of information and communications technologies (ICTs) by State and non-State actors to international security and stability, economic and social development and the safety and well-being of individuals. It is also noted that different levels of capacity for ICT security among States can increase vulnerability in an increasingly interconnected world.

To address these challenges, States have developed, through the work of a series of intergovernmental processes, a cumulative and evolving framework for responsible State behaviour in the use of ICTs in the context of international security. The General Assembly has repeatedly endorsed this framework through consensus resolutions.

To build on these achievements, the Netherlands underlines the need to establish a regular institutional dialogue after the conclusion of the current open-ended working group on security of and in the use of information and communications technologies 2021–2025 established pursuant to General Assembly resolution [75/240](#). To this end, the Netherlands supports the initiative to establish a future programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security, welcomed by the General Assembly in resolutions [77/37](#) and [78/16](#).

Pursuant to operative paragraph 8 of resolution [78/237](#) entitled “Developments in the field of information and telecommunications in the context of international security”, the Netherlands hereby submits its views and assessments on security of and in the use of information and communications technologies, in particular on the future regular institutional dialogue on these matters under the auspices of the United Nations. The views presented below further build on the Netherlands submission for the report of the Secretary General pursuant to resolution [77/37](#) ([A/78/76](#)).

Within the open-ended working group 2021–2025, considerable progress has been made on finding common ground on the future mechanism for regular institutional dialogue on international ICT security. In this regard, the Netherlands welcomes the common elements on regular institutional dialogue contained in the 2023 annual progress report of the open-ended working group. The Netherlands

⁹ Final report of the open-ended working group 2019–2021, para. 10.

remains committed to making further progress on this matter within the open-ended working group 2021–2025.

Scope and objectives

Reaffirming operative paragraph 4 of General Assembly resolution 78/16, the Netherlands is of the view that a mechanism should be established under the auspices of the United Nations, upon the conclusion of the 2021–2025 open-ended working group and no later than 2026, that will be permanent, inclusive and action-oriented, with the specific objectives affirmed in General Assembly resolution 77/37 and with the common elements for future regular institutional dialogue agreed by consensus in the 2023 annual progress report of the 2021–2025 open-ended working group.

The Netherlands supports the initiative to establish under United Nations auspices a programme of action to advance responsible State behaviour in cyberspace in the context of international security. The programme of action should build upon the common elements for future regular institutional dialogue agreed by consensus in the 2023 annual progress report of the open-ended working group and base decisions regarding the scope, structure, content and modalities on consensus outcomes of the 2021–2025 open-ended working group.

Structure and modalities

The Netherlands shares the view that the programme of action should be an inclusive, transparent, consensus-driven and results-based process. The mandate for the programme of action could be derived from a founding document affirming States' political commitment to be guided by the framework for responsible State behaviour in cyberspace, and establishing a mechanism to further operationalize its objectives.

The programme of action should be open to participation by all United Nations Member States, permanent observers, intergovernmental and other organizations and specialized agencies. While States have the primary responsibility for the maintenance of international peace and security, the programme of action should also allow for the meaningful participation, including in formal settings, of relevant non-governmental stakeholders, including the private sector, academia and civil society.

The structure of the programme of action could comprise:

- (a) Periodic review conferences to assess the evolving cyberthreat landscape and the programme of action initiatives, to update the framework as necessary and to provide strategic direction;
- (b) Open-ended plenary discussions to discuss ongoing and emerging threats, further discuss how international law applies, discuss the implementation of confidence-building measures, identify priorities for capacity-building and consider the implementation of norms, rules and principles and to provide guidance for the open-ended technical meetings and practical initiatives;
- (c) Open-ended technical meetings and/or working groups for action-oriented discussions, open to the participation of relevant stakeholders and dedicated to specific issues.

Preparatory work and modalities for establishment of the programme of action

Resolution 78/16, resolution 77/37 and the report of the Secretary-General (A/78/76) provide an initial road map towards establishing the programme of action. In 2025–2026, after the conclusion of the open-ended working group, the Netherlands envisages an international conference, open to non-governmental stakeholders,

building upon the preparatory work done, including in the 2021–2025 open-ended working group, to be held to adopt the founding document and/or political declaration.

Capacity-building in a future mechanism

Without prejudice to the outcomes of the open-ended working group and decisions by the General Assembly on the establishment of a future mechanism, the Netherlands proposes the following elements to facilitate cyber capacity-building to advance the implementation of the evolving and cumulative framework and bolster international cooperation in this regard. This proposal is centred around a four-step cycle:

(a) Exchanges on the threat landscape by exchanging technical expertise on threats and considering how to address these threats through the lens of the consensus framework for responsible State behaviour in cyberspace;

(b) Self-identifying capacity needs through voluntary reporting against the cumulative and evolving framework for responsible State behaviour. Existing methods for voluntary reporting can be utilized, for example the UNIDIR (Mexican-Australian initiative) national survey of implementation of United Nations recommendations on responsible use of ICTs by States in the context of international security;

(c) Matching needs with resources. The future mechanism could function as a convening platform. Furthermore, given the universal character and recognition of the United Nations, the United Nations Secretariat could play a role in facilitating the coordination on the work of organizations and structures on cyber capacity-building. The future mechanism could build on existing tools such as the Cybil Portal of the Global Forum on Cyber Expertise, and, potentially, proposals currently under consideration of the open-ended working group 2021–2025 such as the capacity-building catalogue and global cybersecurity cooperation portal proposed by Member States;

(d) A feedback loop whereby States could exchange experiences in their implementation efforts and cyber capacity-building activities, which could inform further discussions on the use of ICTs by States in the context of international security.

Capacity-building efforts as part of the future mechanism should be undertaken in accordance with the principles for capacity-building agreed in the 2023 annual progress report of the open-ended working group.

New Zealand

[Original: English]
[30 April 2024]

1. Cybersecurity has been a topic of discussion among States, under the auspices of the United Nations, for more than 20 years. Successive working groups – groups of governmental experts and open-ended working groups – have allowed for regular exchanges on issues relating to cybersecurity in the context of international security.

2. These working groups have delivered important foundational outcomes that collectively contribute to international security and stability, through the establishment of a framework for responsible State behaviour in cyberspace – endorsed by the United Nations General Assembly and based on four pillars:

- International law – all United Nations members agree that international law applies to States' conduct in cyberspace

- Norms of responsible State behaviour online in peacetime
- Confidence-building measures to support transparency, predictability and stability
- Capacity-building measures aimed at ensuring that all States can lower the risks of increased connectivity, while still benefiting from it

3. New Zealand fully endorses the decision of the General Assembly in resolution [78/237](#) to establish a mechanism under the auspices of the United Nations, upon the conclusion of the 2021–2025 open-ended working group and no later than 2026, that will be permanent, inclusive and action-oriented, with the specific objectives affirmed in General Assembly resolution [77/37](#) and with the common elements for future regular institutional dialogue agreed by consensus in the 2023 annual progress report of the 2021–2025 open-ended working group.

4. We envisage this mechanism being the “permanent home” of cybersecurity discussions in the context of international security at the United Nations, at the conclusion of the current 2021–2025 open-ended working group, and building on the proposal adopted in United Nations resolutions [77/37](#) and [78/237](#). We welcome and support the resolution put forward by France, on behalf of a cross-regional group, which provides a clear and transparent pathway for all States to consider the scope, structure, content and modalities of the future mechanism in a way that complements the current open-ended working group. In this regard, we support the establishment of a programme of action that is:

(a) The single, permanent mechanism for United Nations cybersecurity discussions after 2025, ensuring predictability and institutional stability. Negotiating agreed modalities for a permanent mechanism would also deliver long-term efficiencies. Revisiting and agreeing modalities for successive working groups has required lengthy, recurring negotiations, taking time away from important substantive discussions;

(b) Anchored in the agreed framework for responsible State behaviour in cyberspace, including consistent with international law and international human rights obligations, ensuring that the programme of action builds on, and enhances, the foundational work of successive Groups of Government Expert and open-ended working groups to advance responsible State behaviour online;

(c) Inclusive – multi-stakeholder participation involving Governments (which bear responsibility for international peace and security in cyberspace), companies, civil society, technical experts, academics and other organizations which contribute to a free, open, secure and interoperable Internet. New Zealand supports modalities that include participation (including statements and submission of written reports) by non-government stakeholders in discussions, including any formal and informal meetings and review conferences;

(d) Action-oriented, including a focus on practical action to advance the framework for responsible State behaviour and promoting capacity-building measures that support States to implement the framework, and mechanisms for accountability and monitoring;

(e) Flexible and adaptable, to respond to emerging threats.

Russian Federation

[Original: Russian]
[9 April 2024]

Concept paper on a permanent open-ended working group with a decision-making function on security of and in the use of information and communications technologies

Co-authors: Republic of Belarus, Burkina Faso, Republic of Burundi, Republic of Cuba, Democratic People's Republic of Korea, Republic of Mali, Republic of the Union of Myanmar, Republic of Nicaragua, Russian Federation, Republic of the Sudan, Syrian Arab Republic, State of Eritrea, Venezuela (Bolivarian Republic of), Republic of Zimbabwe

Discussions within the United Nations open-ended working group on security of and in the use of information and communications technologies (ICTs) 2021–2025 have demonstrated the international community's demand for the establishment of a single permanent decision-making mechanism on this issue under the auspices of the United Nations. We believe the optimal format for such a mechanism to be an open-ended working group, which has proven in practice its effectiveness and relevance.

The mandate of a future permanent open-ended working group with a decision-making function should focus on further promoting an open, secure, stable, accessible and peaceful ICT environment through the practical implementation of the agreements reached in the 2021–2025 open-ended working group. Issues under the mandate include:

- The continued development of legally binding rules, norms and principles on the responsible behaviour of States and the establishment of effective mechanisms for their implementation, as elements of a future universal treaty on ensuring international information security;
- The development of a common understanding of how international law applies to the use of ICTs and how existing norms can be adapted to the specifics of the information space (its cross-border dimension, anonymity and the possibility of introducing hidden functions);
- The development and implementation of confidence-building measures and mechanisms for practical cooperation between States, including through established channels of communication between authorized entities/bodies and a global intergovernmental directory of points of contact, in order to counter information security threats associated with ICTs and their use and to prevent inter-State conflicts in the global information space;
- The establishment of mechanisms and programmes to assist States in improving the capacity to protect their national information resources, taking into account specific needs.

The following principles should underpin a future permanent open-ended working group:

- Openness, inclusiveness, democracy and transparency;
- The leading role of States in promoting dialogue on security in the use of ICTs by States, under the auspices of the First Committee of the United Nations General Assembly;

- Compliance with the principles of the Charter of the United Nations (the sovereign equality of States, the non-use of force and threat of force, and the peaceful settlement of international disputes);
- Any decisions are made by consensus and solely by States;
- International efforts to ensure security of and in the use of ICTs should not be duplicated across several United Nations negotiating platforms;
- Continuity with the consensus outcomes and recommendations of previous open-ended working groups and groups of governmental experts;
- Flexibility and the ability to evolve as the needs of States change and new ICT security challenges emerge.

Procedural issues:

- Any decisions taken within the permanent open-ended working group shall be approved by consensus among States (this parameter should be clearly stated in the General Assembly resolution establishing the permanent open-ended working group);
- Timeline: the permanent open-ended working group should begin work at the conclusion of the current open-ended working group and hold two formal sessions per year at United Nations Headquarters in New York (all Member States are to be represented without exception);
- Reporting format: progress reports to the United Nations General Assembly, adopted by consensus once every two years;
- Structure: as needed, United Nations Member States may decide to establish subsidiary subgroups to address specific aspects of the mandate in a more detailed, in-depth manner. However, meetings of such subgroups should not take place simultaneously in order to ensure full participation of all delegations;
- Governance: the work of the permanent open-ended working group shall be conducted by a bureau, consisting of a Chair, two Vice-Chairs, a rapporteur and, if necessary, subgroup Chairs (also with the status of Vice-Chairs). The composition of the bureau shall be approved by consensus every two years by States on the basis of equitable geographical distribution, on a rotational basis from each of the regional groups.

It would be advisable to provide the permanent open-ended working group with a mechanism for swiftly formalizing decisions as they are agreed upon (under the silence procedure and subsequent approval at the next session). Practical steps should be taken to maintain continuous information exchange between States through an appropriate electronic portal.

It would be useful to envisage the permanent open-ended working group cooperating with relevant regional organizations and associations through consultations by its Chair with groups of countries and through intersessional meetings held with their representatives once a year.

Participation by non-State actors (non-governmental organizations, the business community and the scientific and academic communities) in the work of the permanent open-ended working group should be of a purely consultative and informal nature; for example, through once-a-year intersessional meetings. The right to attend official events as observers shall be granted only to accredited (agreed by consensus among States) non-State actors.

Singapore

[Original: English]

[1 May 2024]

Singapore remains committed to an open and inclusive global conversation on cybersecurity, and it is in this regard that we see commitment by all States to a single-track future regular institutional dialogue as being of utmost importance. A single-track future regular institutional dialogue is crucial in fostering universal acceptance and recognition of the cumulative and evolving framework for responsible State behaviour in the use of information and communications technologies (ICTs) agreed by all Member States at the United Nations since 1998, and in providing a common global platform for the further development and implementation of this framework. In this regard, it is important that all States are able to focus their efforts on a single process to ensure that discussions remain substantive and not suffer fragmentation. Small and developing States with limited resources would also not be able to sustainably participate in dual-track, parallel processes.

Singapore believes we should continue to build upon the four common elements of regular institutional dialogue agreed in the second annual progress report of the open-ended working group on security of and in the use of ICTs 2021–2025 (A/78/265, para. 55) to build the trust and confidence that we need to reach consensus on a single-track permanent mechanism.

It is important that States use the limited remaining time and space to work on building a common vision on the way forward for regular institutional dialogue within the current open-ended working group. The priority task at hand should be consensus-building. In this regard, Singapore supports the proposal made by Brazil at the seventh substantive session of the open-ended working group for a moratorium on the tabling of resolutions relating to ICT security in the First Committee of the General Assembly until the current open-ended working group concludes its work in 2025. We support the Chair of the open-ended working group in continuing to convene discussions on the way forward for regular institutionalized dialogue, with a view to further developing and refining a consensus proposal for such dialogue.

As a next step, we believe that it would be productive for the current open-ended working group to agree on the scope, structure, objectives and frequency of meetings within the future mechanism. Answering these practical questions is a logical way to build on the common elements that all States have already agreed upon. Doing so will also give delegations, in particular smaller delegations with limited resources, early clarity on their work after 2025, allowing them to begin the planning necessary to optimize their participation in a meaningful manner. To ensure a sustainable foundation for a permanent universal, single-track mechanism, Singapore also emphasizes that the design of the future mechanism must be sufficiently broad and accommodating to facilitate continuing and future discussions on the proposals and priorities of all delegations. In particular, it would be useful to periodically review the operations of the permanent mechanism to ensure that our approaches are relevant to the dynamic operating threat landscape. In this regard, Singapore supports the approach and structure presented in the Chair's discussion paper of 20 February 2024 on draft elements for the permanent mechanism. Singapore looks forward to working constructively with all delegations on further refining these draft elements with a view to their adoption by consensus in the third annual progress report of the current open-ended working group.

Türkiye

[Original: English]

[1 May 2024]

Information and communications technologies have become an indispensable part of society and economy by affecting every aspect of life. These technologies are used in many areas by both individuals and States. Today, States' skills in developing and using technology play an important role in development and growth. Information technologies have become the main actor of development in almost every field, from transportation to communications, from the defence industry to medical science, and from production to education and trade.

Studies indicate that technological trends will accelerate in the next few years. Among these, those which can bring about new technological standards and new business lines and make significant changes in existing ones stand out. The Internet of Things, 5G, big data, blockchain, artificial intelligence, autonomous vehicles and smart robots are seen as technologies that will shed light on our present and future.

On the other hand, while these technologies provide us with many opportunities, they also bring cybersecurity risks. The structures of cyberthreats are becoming more complex, and their numbers are increasing day by day, and, according to research, it has been determined that there will be more than 493 million ransomware attempts worldwide in 2022.¹

In this regard, cybersecurity is a must that needs to be addressed at every stage for the healthy development and integration of technology. Security vulnerabilities in information and communications systems may cause these systems to be out of service or misused or cause loss of life, large-scale economic damage, disruption of public order and/or violation of national security.

Ensuring cybersecurity is not only a necessity to combat threats in areas where technology is intense but also an important factor affecting the welfare and national security of countries owing to the risks that it brings to the course of social and economic life. In the light of all these developments, countries spend very high amounts in the field of cybersecurity, develop cybersecurity technologies and direct their efforts to ensure their security in the cyberenvironment and increase their resistance against attacks.

The issue of combating cyberthreats is considered a national policy in our country. In this context, studies to ensure national cybersecurity are carried out by the Ministry of Transport and Infrastructure at the strategic level and by the Information and Communication Technologies Authority (BTK) at the technical level. In addition, other institutions and organizations also contribute to these studies.

As part of the studies carried out since 2012, "National CyberSecurity Strategy and Action Plans" have been prepared and implemented. Most recently, in accordance with the "National Cybersecurity Strategy and Action Plan (2020–2023)", studies have been carried out to protect the cybersecurity of critical infrastructures 24/7, increase the competencies of cyberincident response teams and the safe use of cyberspace by all segments of society, keep cybersecurity awareness at a high level, share information and cooperation with national and international stakeholders, develop mechanisms that will ensure protection, minimize cybercrimes and increase deterrence.

In addition, the Ministry of Transport and Infrastructure has started studies to develop a new cybersecurity strategy and action plan that covers the 2024–2028

¹ www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide.

period. In this context, studies are continuing to ensure effective cooperation among all stakeholders, increase cybersecurity threat intelligence acquisition, production and sharing, increase the level of national preparedness for cyberincidents, develop expert human resources, develop rapid detection and early response opportunities and perform risk analyses for critical sectors and infrastructures.

TR-CERT (the National Cyber Emergency Response Team of Türkiye within the Information and Communication Technologies Authority) has coordinated the cyberincident response in Türkiye since 2013. Besides cyberthreat detection and cyberincident response, including before, during and after incidents; TR-CERT ensures the implementation of preventive measures against cyberthreats and ensures cyberdeterrence.

The main focus areas in cybersecurity of TR-CERT are, namely:

- Cyber capacity-building
- Technological measures
- Gathering and diffusing threat intelligence
- Protection of critical infrastructures

Within the context of improving national cybersecurity, 14 sectoral cyber emergency response teams for critical sectors/infrastructures (such as energy, health, banking and finance, water management, electronic communications and critical public services) and more than 2,200 institutional cyber emergency response teams have also been established since 2013. All cyber emergency response teams work 24/7, under the coordination of TR-CERT in order to mitigate cyber risks and to fight against cyberthreats. TR-CERT uses detection and prevention tools for monitoring and reporting tools for information-sharing with relevant parties. TR-CERT developed the Information-sharing Platform for all cyber emergency response teams within Türkiye in order to distribute alarms, warnings and security notices, which provides an efficient and secure communications channel.

Cybersecurity exercises are another important activity for cooperation and preparedness. These kinds of exercises performed at the national and international level contribute to strengthening cyberspace and the testing of measures to be taken against potential cyberthreats. Since 2011, seven national and two international cybersecurity exercises have been organized by the Ministry of Transport and Infrastructure. Most recently, at the national level, “Cyber Shield 2022” exercises were held. After Cyber Shield 2022, with the cooperation of our Ministry of Transport and Infrastructure and the Information and Communication Technologies Authority (BTK), “Cyber Shield 2022 for the Finance Sector” was held on 20 and 21 October 2022 with the participation of public institutions and organizations. In these exercises, with the technical infrastructure and scenarios developed within TR-CERT, participants were given hands-on cybersecurity experience, and information was shared on the steps to be taken in case of potential cyberattacks. It is planned to organize an international cybersecurity exercise in the coming period.

Cybersecurity is an issue that is on the agenda of the whole world and requires efforts at the international level. Cooperation at the regional and global levels and the sharing of information and intelligence in the field of cybersecurity play an important role in helping countries cope with cyber risks and threats. In this context, Türkiye is developing bilateral, regional and international cooperation in this field; participates in and contributes to the policy and strategy-making activities of international organizations such as the United Nations, the North Atlantic Treaty Organization (NATO), the Organization for Security and Cooperation in Europe (OSCE), G20, the Organisation for Economic Co-operation and Development, the Economic

Cooperation Organization, D8, the Centre for Security Cooperation (RACVIAC), the Organization of Turkic States and so on. In addition, TR-CERT continues its activities in sharing cyberthreat intelligence through its memberships in international platforms such as the Forum of Incident Response and Security Teams (FIRST), TI, ITU, the Cybersecurity Alliance for Mutual Progress, NATO Malware Information Sharing Platform, and the Computer Emergency Response Team of the Organization of Islamic Cooperation (OIC-CERT). Our country also participates in the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCoE) as a sponsor country and is a member of the NATO Virtual Cyber Incident Support Capability (VCISC) mechanism. In addition, memorandums of understanding and bilateral cooperation are signed with many countries on cybersecurity.

TR-CERT has been accepted to the MITRE Common Vulnerabilities and Exposures Program (MITRE-CVE), and in this context, it assigns CVE numbers for the vulnerabilities of third-party software, hardware or products and provides process coordination in vulnerability management.

Türkiye is a party to several multilateral cybersecurity agreements. Türkiye ratified the Convention on Cybercrime (European Treaty Series No. 185) of the Council of Europe. Türkiye has also contributed to the studies carried out under United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. In addition, Türkiye is one of the co-sponsoring States for the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security and strongly supports United Nations General Assembly resolution 77/37 and further efforts towards the establishment of the programme of action as a permanent, inclusive, action-oriented mechanism.

1. National Cybersecurity Organization in Türkiye

Looking at the field of information and communication security, notably cybersecurity in Türkiye, it is noteworthy that progression in this field dates back to 1991. The journey of Türkiye in cybersecurity started with the introduction of cybercrimes into Turkish Criminal Law No. 765 in 1991.² Since then, it has achieved significant milestones in various areas of cybersecurity, an essential part of national security. The following is a non-exhaustive list of initiatives implemented up to 2012:

- The National Information Infrastructure Master Plan³ was crafted in Türkiye in 1999.
- The E-Türkiye Initiative Action Plan⁴ was launched in 2002.
- The E-Transformation Türkiye project was outlined in 2003 along with the Short-Term Action Plan for 2003–2004.⁵
- The introduction of Electronic Signature Law No. 5070⁶ and Turkish Criminal Code Law No. 5237⁷ in 2004.
- The release of the 2006–2010 Information Society Strategy and Action Plan⁸ in 2006.

² <https://www.mevzuat.gov.tr/MevzuatMetin/5.3.765.pdf>.

³ http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/991000_TuenaRapor.pdf.

⁴ http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/020800_E-TurkiyeEylemPlani.pdf.

⁵ <https://webdosya.csb.gov.tr/db/cbs/icerikler/2005-20180522115122.pdf>.

⁶ <https://kamusm.bilgem.tubitak.gov.tr/dosyalar/mevzuat/kanunlar/kanun.pdf>.

⁷ www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm#1.

⁸ http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060500_BilgiToplumuStratejisi.pdf.

- The establishment of the Turkish Computer Incident Response Team Coordination Center in 2007.
- Law No. 5651 on the Publications on the Internet and Combating Crimes Committed by Means of Such Publications ⁹ was enacted in 2007.
- Electronic Communications Law No. 5809 ¹⁰ was implemented in 2008 in tandem with the first National Cybersecurity Drill.
- The National Security Council Declaration in 2010 is issued, acknowledging the global reach of cyberthreats and their national security implications.
- Türkiye's alignment with the Council of Europe (CoE) Budapest Convention on Cybercrime (ETS No. 185) in the same year was achieved.
- The Council of Ministers' decision to manage and coordinate national cybersecurity efforts resulted in the establishment of the Cyber Security Council in 2012,¹¹ and the Scientific and Technological Research Council of Türkiye (TÜBİTAK) Informatics and Information Security Research Center (BİLGEM) Cyber Security Institute ¹² was established in the same year.

These milestones mark significant progress in the domain. As mentioned above, under the Parliamentary Government System era in Türkiye, the Council of Ministers approved a decision on the execution, management and coordination of National Cyber Security Studies on 11 June 2012.¹³ With this decision, the Cyber Security Council¹⁴ was established and the Ministry of Transport, Maritime Affairs and Communications (now the Ministry of Transport and Infrastructure),¹⁵ as it was then called, was tasked with carrying out the secretariat of the Council and coordinating cybersecurity activities with relevant institutions.

Over the past decade, there has been a marked increase in the pace of developments in cybersecurity sector of Türkiye. Key milestones include the launch of the country's first National Cybersecurity Strategy and Action Plan for 2013–2014,¹⁶ the establishment of the National Cyber Incident Response Center (USOM)¹⁷ within the Information and Communication Technologies Authority (BTK)¹⁸ and the publication of a declaration outlining the creation, roles and working principles of cyberincident response teams.¹⁹ In addition, cyberincident response teams (institutional cyberincident response teams, sectoral cyberincident response teams) were established within public institutions and organizations within the framework of the 2013–2014 National Cybersecurity Strategy and Action Plan. Cyberincident response teams are institutional and sectoral organizations established to rapidly identify threats and potential attacks in the cyberenvironment, and to develop and share measures for solving the problems caused by these attacks. The goal of these teams is thus to provide cyberresponse skills to institutions and organizations. At present, 14 sectoral cyberincident response teams are operating under the coordination of the National Cyber Incident Response Center (USOM), and more than

⁹ <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf>.

¹⁰ <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5809.pdf>.

¹¹ www.btk.gov.tr/siber-guvenlik-kurulu.

¹² <https://bilgem.tubitak.gov.tr/en/sge/>.

¹³ <https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf>.

¹⁴ www.btk.gov.tr/siber-guvenlik-kurulu.

¹⁵ www.uab.gov.tr/.

¹⁶ <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf>.

¹⁷ www.usom.gov.tr/.

¹⁸ www.btk.gov.tr/.

¹⁹ www.usom.gov.tr/hakimizda.

2,100 institutional cyberincident response teams are diligently working to safeguard Türkiye's cyberrealm.

The Cyber Defense Center, which was set up within the Turkish Armed Forces in 2012, has since evolved into Cyber Defence Command. Similarly, the Department of Combating Cyber Crimes, which was instituted within the General Directorate of Security in 2011, was later restructured, in 2013.

Law No. 6518,²⁰ published in 2014, introduced some regulations in the field of cybersecurity by adding articles to Law No. 5809, published in 2008, which regulates the electronic communications sector. With the articles added to Law No. 5809, the Cyber Security Council, consisting of senior executives of public institutions, was established under the presidency of the Minister of Transport, Maritime Affairs and Communication. With subparagraph (h) added to article 5 of the aforementioned law, the Ministry of Transport, Maritime Affairs and Communications was assigned the duties of “determining policies, strategies and targets for ensuring national cybersecurity, preparing action plans and conducting education and awareness-raising activities on cybersecurity”.

With this regulation, the Cyber Security Council has been designated as the main authority responsible for the final approval and effective implementation of the policies, strategies and action plans in the country determined by the Ministry of Transport, Maritime Affairs and Communications. The Council is also tasked with deciding on proposals related to the identification of critical infrastructures and determining the institutions and organizations to be exempted from all or part of the provisions related to cybersecurity.

In 2016, Law No. 6698 on Personal Data Protection²¹ and the 2016–2019 National Cybersecurity Strategy and Action Plan²² were published. In addition, with Decree Law No. 671,²³ prepared in line with the needs of the period, the Information and Communication Technologies Authority (BTK) was authorized with the statement, “The Authority shall take or require to be taken all kinds of measures to protect public institutions and organizations and real and legal persons against cyberattacks and to provide deterrence against these attacks”. Subsequently, in 2017, under the coordination of the Presidency of Defense Industries (now the Secretariat of Defense Industries (SSB)),²⁴ the establishment of the Turkish Cyber Security Cluster was initiated, the appointments of the Personal Data Protection Board were completed and the Board started its activities.

In 2018, the Cyber Security Council was abolished following the publication of Decree Law No. 703.²⁵ It was declared that the Council's responsibilities and mandate would be transferred to a “council or authority to be designated by the President”. However, despite some partial appointments related to these responsibilities, none of them have been officially transferred to any council or authority to date. With the transition to the Presidential Government System, there have also been changes in the policymaking process. The authority to formulate policies has been transferred to the President of the Republic. The Policy Boards have been tasked with formulating and developing these policies (Presidential Decree No. 1,²⁶ arts. 20–22), while the Ministries are responsible for implementing them.

²⁰ www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm.

²¹ <https://kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law>.

²² <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf>.

²³ www.resmigazete.gov.tr/eskiler/2016/08/20160817-18..htm.

²⁴ www.ssb.gov.tr/Default.aspx?LangID=2.

²⁵ <https://www.resmigazete.gov.tr/eskiler/2018/07/20180709M3-1.pdf>.

²⁶ <https://www.mevzuat.gov.tr/mevzuatmetin/19.5.1.pdf>.

As of 10 July 2018, with the implementation of Presidential Decree No. 1 of the Presidential Government System, the responsibility for “developing policy and strategy proposals related to cybersecurity” was assigned to the Security and Foreign Policies Council operating under the President (Presidential Decree No. 1, article 36/1/ğ). With Presidential Decree No. 1, the responsibility for “developing projects to enhance information security and cybersecurity” was assigned to the Digital Transformation Office²⁷ of the Presidency of the Republic of Türkiye, and in particular to the Cyber Security Department²⁸ under the Digital Transformation Office. The duties of the Department include the following:

- Developing cybersecurity strategies for public institutions and critical infrastructures, in line with policies set by the President.
- Monitoring advancements to efficiently implement nationwide cybersecurity policies, strategies and action plans.
- Conducting research to identify critical infrastructures.
- Boosting cooperation between public, private sector and universities to foster a national cybersecurity ecosystem.
- Undertaking studies to develop domestic and national cybersecurity products across all sectors, especially critical infrastructures, and promoting their usage within the public sector.
- Performing preventive and protective activities to safeguard critical technology and information assets.
- Conducting studies on the establishment and management of the information security system in public institutions and organizations that operate critical infrastructure; this includes setting technical standards and procedures, as well as principles for monitoring and directing applications.

In addition, the National Technology Directorate²⁹ was established under the Ministry of Industry and Technology (MoIT),³⁰ as outlined in Presidential Decree No. 1, published in the Official Gazette dated 10 July 2018. The Directorate was given the following responsibilities regarding cybersecurity:

- Enhancing the maturity level of cyber and information security for information technology and advanced technology products and systems.
- Developing domestic and national products in cybersecurity.
- Expanding the use of domestic and national products nationwide,
- Enhancing the data center and data processing infrastructure
- Supporting the cybersecurity ecosystem through various incentive programmes.

In summary, various laws, regulations, and other legislations have designated several institutions to oversee national cybersecurity. These institutions derive their cybersecurity-related duties from these different legislations. Similar to most other countries, cybersecurity in Türkiye is considered a shared responsibility among multiple government entities. The Digital Transformation Office and the Ministry of Transportation and Infrastructure have conducted studies related to the development of cybersecurity strategies and policies. Each organization has its own set of roles and responsibilities within its respective domain.

²⁷ <https://cbddo.gov.tr/en/>.

²⁸ <https://cbddo.gov.tr/en/departement-of-cyber-security/>.

²⁹ www.sanayi.gov.tr/merkez-birimi/c03f1f3bae27/hakimizda.

³⁰ www.sanayi.gov.tr/anasayfa.

2. Roles and responsibilities of the Digital Transformation Office on cybersecurity

Following the transition to the Presidential Government System in 2018, the Digital Transformation Office of the Presidency of the Republic of Türkiye was established under Presidential Decree No. 1, which entered into force after being published in the Official Gazette dated 10 July 2018. The mandate of Digital Transformation Office was subsequently expanded by Presidential Decree No. 48 published on 24 October 2019.³¹

The establishment of the Digital Transformation Office marked a new era and a change in mindset regarding digitalization efforts in Türkiye. Since its establishment, a more coherent and holistic inter-institutional approach to digital transformation in the public sector has begun. Accordingly, in addition to achieving a faster, more transparent and effective administration, its aim is to centrally coordinate, manage and operate the digital transformation activities carried out separately under different institutions in line with developing technologies, social demands and reform trends in the public sector. In addition, its aim is to coordinate the activities related to cybersecurity, national technologies, big data and artificial intelligence (AI) both strategically and in practice under a single roof and to implement high-level strategies effectively. As a result, under the coordination of the Digital Transformation Office, macro-level targets are set, and initiatives are carried out to protect the digital infrastructures of Türkiye and for it to become a deterrent cyberpower.

The Digital Transformation Office has the following responsibilities within the cybersecurity domain, including policy development, regulations, building a cybersecurity ecosystem, raising public awareness, capacity-building, strengthening public infrastructure and developing standards:

- Developing cybersecurity strategies for public institutions and for critical infrastructure pursuant to the policies determined by the President.
- Developing projects supporting national cybersecurity and information security.
- Following up developments in effective nationwide implementation of cybersecurity policies, strategies and action plans.
- Working on the determination of critical infrastructures.
- Making proposals to related agencies about those institutions and organizations being exempted from all or part of the provisions on cybersecurity.
- Contributing to the creation of a national cybersecurity ecosystem by enhancing collaboration among the public sector, private sector and universities.
- Determining prioritized cybersecurity areas for directing the capacity of the private sector to critical fields and preventing repetitive investments.
- Working on the development of local and national cybersecurity products in every field, including, primarily, critical infrastructure, and expanding the use of such solutions in the public sector.
- Working on preventive and protective activities for protecting critical technology and information assets.
- Establishing and operating an information security management system in public institutions and those organizations operating critical infrastructure, determining technical standards and procedures and principles and monitoring and guiding implementation.

³¹ <https://cbddo.gov.tr/en/governance-and-responsibilities>.

At present, the Digital Transformation Office is the leading authority managing cybersecurity issues for public institutions and critical sectors in our country. Besides carrying out the responsibilities of the cybersecurity board, it collaborates with all institutions to coordinate the development and efficient execution of strategies and action plans nationwide.

3. Activities and projects of the Digital Transformation Office on policy development

Although there are different definitions of the concept of cybersecurity, a simple and inclusive definition can be expressed as a security discipline applied to every point in cyberspace encompassing the components of information technologies. Given that Industry 4.0 is considered a revolution that aims to bring together information technologies and all vital mechanisms, it is expected that the cybersecurity discipline will be integrated into our life discipline as a security adaptation of this revolution.

When security discipline is not acted in accordance with the security discipline, security and privacy problems arise. When considered on a national scale, the strategic goals of protecting critical infrastructures, ensuring secure data-sharing between institutions and organizations and keeping data traffic whose source and destination is domestic within the country come to the fore. It is aimed to increase the level of preparedness for cyberincidents on an institutional, sectoral and national basis through approaches based on risk-based analysis and planning.

In order to ensure security in the digital world, Governments prepare and publish cyber-security strategies and ensure their realization and supervision by assigning relevant institutions. Our country also fulfils its duty in this regard. As a result of our country's work on this issue under the coordination of the Ministry of Transport and Infrastructure, the strategies published respectively are listed below:

- National Cybersecurity Strategy and Action Plan 2013–2014³²
- National Cybersecurity Strategy and Action Plan 2016–2019³³
- National Cybersecurity Strategy and Action Plan 2020–2023³⁴

The National Cybersecurity Strategy and Action Plans mentioned above are progressing with a holistic approach to ensure continuity and include measures to ensure security for new technologies that have entered our lives.

The latest National Cybersecurity Strategy and Action Plan (2020–2023)³⁵ was published on 28 December 2020 with the support of the Digital Transformation Office. It aims to support our country's economic development, protect social life and national security and position our country as an international brand in the cybersecurity field. In this regard, the Strategy is focused on the policies related to the four-year period, in line with Türkiye's cybersecurity vision and mission, and aims to further the achievements realized through previous strategies. The strategic objectives determined by the National Cybersecurity Strategy and Action Plan (2020–2023) were grouped into eight pillars:

- Protecting Critical Infrastructure and Increasing Resilience
- National Capacity-Building

³² <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf>.

³³ <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf>.

³⁴ <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf>.

³⁵ <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/national-cyber-security-strategy-2020-2023.pdf>.

- Organic Cybersecurity Network
- Security of New Generation Technologies
- Fighting against Cybercrime
- Developing and Fostering National and Domestic Technologies
- Integrating Cybersecurity into National Security
- Improving International Cooperation

3.1 Strategy and Action Plan Monitoring System

The Strategy and Action Plan Monitoring System has been developed to effectively manage and monitor the strategy and action plans prepared by the Presidency, as well as the activities of the Turkish Cybersecurity Cluster within the Digital Transformation Office. The system tracks the progress of actions and evaluates their performance and achievements based on predetermined objectives.

Furthermore, the Digital Transformation Office is responsible for supporting the policy development activities coordinated by the Science, Technology and Innovation Policies Board, including:

- Proposal for National Policy for Cybersecurity and Communication Infrastructure Technologies
- Proposal for National Policy For 5G and beyond Next Generation Communication Technologies
- National Roadmap for Cybersecurity Technologies

3.2 Measures in the 2023 Presidential Annual Programme

Based on the National Cybersecurity Strategy and Action Plan (2020–2023), the measures in the 2023 Presidential Annual Programme³⁶ for which the Digital Transformation Office is directly responsible or affiliated are as follows:

- National Cybersecurity Strategy will be updated, regulations and technical infrastructure for cybersecurity will be strengthened, and a strong coordination structure will be established.
 - Cybersecurity framework legislation will be prepared.
 - 2024–2027 National Cybersecurity Strategy and Action Plan will be prepared.
- Procedures and principles for the establishment of information security management systems in critical infrastructures will be determined and put into practice.
 - Information and Communication Security Guide will be updated.
- In order to benefit the cybersecurity ecosystem and develop products and solutions with higher added value in this field, cybersecurity products and technology projects involving public research institutions and universities will be developed, and the outputs of these projects will be shared with the cybersecurity ecosystem in open source code.
- Efforts will be made to strengthen the national cybersecurity ecosystem and increase its international competitiveness.
 - An international cybersecurity business forum will be organized.

³⁶ <https://www.sbb.gov.tr/wp-content/uploads/2022/11/2023-Yili-Cumhurbaskanligi-Yillik-Programi.pdf>.

- The Platform for the Dissemination of Domestic Cyber Security Products will be launched to develop an ecosystem that will enable the maturation and export of needed domestic cybersecurity products.
- In order to train a qualified labour force in the field of cybersecurity, cybersecurity curricula for vocational colleges will be developed and occupational standards will be established.
 - The existing cybersecurity curricula of vocational schools with cybersecurity curricula will be improved.
 - Occupational titles of students who will graduate from vocational schools with a curriculum in the field of cybersecurity will be determined and standards will be prepared.

3.3. Measures in the 2024 Presidential Annual Programme

Based on the National Cybersecurity Strategy and Action Plan (2020–2023), the measures in the 2024 Presidential Annual Programme³⁷ for which the Digital Transformation Office is directly responsible or affiliated are as follows:

- Cyberresilience and security maturity level will be increased against cybersecurity threats to financial markets.
 - A regulation on ensuring national cybersecurity and enhancing cyberdeterrence will be published to cover the financial sector.
- Harmonization with international standards in the field of cybersecurity and Türkiye's participation in international joint projects will be supported.
 - Taking into account international standards and European Union legislation, secondary legislation on Internet of things security will be finalized.
- Regulations will be issued to ensure national cybersecurity by taking into account the European Union Network and Information Security Directive (NIS2) and its new efforts in the field of cybersecurity and international best practices.
 - A regulation on ensuring national cybersecurity and increasing cyberdeterrence will be published.
 - Regulation studies will be carried out for the security of the Internet of things.
 - Cybersecurity inspections will be conducted for Internet of things devices.
 - Secondary regulations needed in relation to the national cybersecurity framework legislation, for which preparatory work is ongoing, will be determined.
 - Efforts will be carried out on Electronic Signature Law No. 5070 and other relevant legislation to provide a legal basis for remote signature service.
 - Awareness activities will be carried out to expand the use of remote signature service in public institutions and the private sector.
- The highest-level coordination of national cybersecurity activities will be ensured, and an effective coordination and administration structure will be established to foster inter-institutional cooperation.
 - Exclusive cybersecurity legislation regulating the functions, duties and responsibilities of the national cybersecurity organization will be published.

³⁷ <https://www.sbb.gov.tr/wp-content/uploads/2023/10/2024-Yili-Cumhurbaskanligi-Yillik-Programi.pdf>.

- Preparatory work for the 2024–2028 National Cybersecurity Strategy and Action Plan will be coordinated and a mechanism for monitoring actions and activities in the digital environment will be developed.
- Efforts will be carried out to establish a national cybersecurity emergency and crisis management plan.
- Cyberthreat intelligence-sharing network will be strengthened.
- Cyberthreat intelligence acquisition and sharing processes will be strengthened by increasing the diversity of resources and developing artificial intelligence and big data analytics applications, and efforts will be carried out for early detection and prevention of threats to national cybersecurity.
 - A needs analysis will be conducted for cyberthreat intelligence resources.
 - Incident response and coordination capacity will be increased.
 - Work will be initiated for cybersecurity projects supported by artificial intelligence and big data analytics to detect phishing domains, malware command and control centres and botnets.
- Procedures and principles for the establishment of information security management systems in critical infrastructures will be determined and put into practice.
 - Process analysis will be conducted for the establishment of information security management system in critical infrastructures.
 - Regulatory work will be carried out for the establishment of an information security management system in critical infrastructures.
- Cybersecurity standards will be established in areas of concern.
 - The certification framework established under the European Union Cybersecurity Act will be examined, and the standards needed for cybersecurity products, services and processes will be determined.
 - Articles related to the information and communications security guidelines of industry will be incorporated into the Information and Communication Security Guide.
 - A model will be developed to identify critical enterprises to be subject to audit under the Information and Communication Security Guide.
 - Preparations will be made for the audit process in accordance with the Information and Communication Security Guide.
 - Awareness activities regarding the Information and Communication Security Guide will be carried out.
- Test infrastructures for cybersecurity will be developed.
 - An analysis of the existing situation of cybersecurity application and research centres, cybersecurity test beds and integration laboratories of universities will be conducted.
- The use of domestic cybersecurity products, particularly by public institutions, will be increased.
 - A road map will be prepared for the development of the cybersecurity sector and its participation in the global market.
- Programmes will be developed to train a qualified workforce and improve career opportunities in the field of cybersecurity.

- Cybersecurity contests will be organized for qualified young employees.
- Cooperation and coordination activities will be carried out to determine occupational standards for personnel working in the field of cybersecurity.
- Training content, quality and environment will be improved in order to train the workforce in line with the needs of the cybersecurity sector.
 - Online and laboratory-based cybersecurity trainings will be conducted.
 - Online cybersecurity trainings will be continued through the Information and Communication Technologies Authority (BTK) Academy.
 - Applied cybersecurity trainings will be held at the FETİH Cyber Training Center.
- Studies will be carried out to raise public awareness on cybersecurity.
 - Studies will be carried out to develop course content on cybersecurity at primary and secondary education level.
 - Information and Communication Security Guide Compliance and Audit process and training program on information security awareness will be developed.
 - Activities such as seminars, trainings and contests will be organized for cybersecurity awareness.
- Mechanisms for the implementation of information and communication security measures, establishment, operation and audit of information security management systems in public institutions will be strengthened
 - Secondary regulations will be made for the procedures and principles on ensuring information and communication security.
 - Legislation and infrastructure studies will be carried out on the use and monitoring of domain names belonging to public institutions and organizations.

4. Activities and projects of the Digital Transformation Office on regulations and cybersecurity guidelines

Significant activities have been conducted by the Digital Transformation Office to increase national resilience by taking measures to protect both the public and private sectors against cyberthreats. The main objectives of these efforts include improving cybersecurity regulations and policies, establishing auditing mechanisms, preventing vendor lock-in in critical infrastructures, ensuring a safe technological transformation and protecting the data of the country. Some ongoing studies are summarized below:

- A draft regulation has been prepared to define procedures and principles regarding the security of websites hosted by public institutions and organizations and the allocation of “gov.tr” subdomains.
- A draft regulation on ensuring information and communication security has been prepared to provide technical requirements for the implementation of information and communication security measures. In addition, provisions for the establishment, implementation, maintenance, auditing and continuous improvement of an information security management system to prevent or mitigate information security risks are included in the draft regulation. The requirements set out in this draft regulation are intended to apply to all public institutions.

- The preparation of a national cybersecurity law is under way. The Law aims to address national cybersecurity governance and organization through a unique “Cyber Security Governance Framework” that is compatible with technological developments and will increase national resilience to current cyberthreats.

The remainder of this section summarizes initiatives that have been implemented or completed.

4.1 Presidential Circular on Information Security Measures 2019/12

The increasing digitization of information, the ease of direct access to information, the digitalization of infrastructures and the proliferation of information management systems bring serious security risks. In this context, the Presidential Circular on Information Security Measures 2019/12³⁸ was issued to reduce the security risks encountered and to ensure the security of critical types of data that may threaten national security or disrupt public order. The Circular includes 21 basic information and communication security measures³⁹ that should be followed by the public institutions and the private sector offering critical infrastructure services. To guarantee data protection, the Presidential Circular aims to ensure that data owned by a country remains within the boundaries of that country. In addition, it highlights that the production and use of national cybersecurity solutions represents one of the main priorities of Türkiye. Finally, it also states that “an Information and Communication Security Guide shall be prepared under the coordination of the Digital Transformation Office in order to mitigate and neutralize security risks and especially ensure the security of critical data”.

4.2 Information and Communication Security Guide

Further to Presidential Circular on Information Security Measures 2019/12 mentioned above, the Information and Communication Security Guide⁴⁰ document was published in 2020. The main purpose of the guide is to determine detailed cybersecurity measures to ensure the security of critical information/data and infrastructures that may lead to disruption of public order or may threaten national security. The Guide is the first national reference document published in this field and it emphasizes the need for a comprehensive security strategy that covers all aspects of information and communication security. It plays an important role in strengthening the cyberdefence capabilities of public institutions and providers of critical infrastructure services. Furthermore, both the Presidential Circular on Information Security Measures 2019/12 and the Information and Communication Security Guide require product vendors to provide a declaration that their products are free of any backdoors.

4.3 Information and Communication Security Audit Guide

In order to achieve and ensure the continuity of the achievements targeted in the Information and Communication Security Guide, the Information and Communication Security Audit Guide⁴¹ was prepared by the Digital Transformation Office and published in October 2021, with the recognition that information and communication security is possible through effective audit and surveillance activities.

Public institutions and organizations and businesses providing critical infrastructure services are expected to complete their compliance activities within the period specified in the Information and Communication Security Guide, and to carry

³⁸ <https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf>.

³⁹ cbddo.gov.tr/en/presidential-circular-no-2019-12-on-information-security-measures.

⁴⁰ cbddo.gov.tr/en/icsguide/.

⁴¹ cbddo.gov.tr/en/icsaguide/.

out audit studies at least once a year in order to ensure the compliance of their activities carried out and the measures taken.

Organizations within the scope are not only required to comply with the requirements of Information and Communication Security Guide, but also to perform regular audits and assessments of how effectively the security measures are implemented and whether the implementation process is in alignment with the related requirements. Therefore, regular audits at least once a year should be conducted by either an internal audit function or accredited third-party audit companies. Audit policies and procedures that must be conducted by the organizations within the scope are documented in the Information and Communication Security Audit Guide which was published by the Digital Transformation Office in 2021.

4.4 Information and Communication Security Auditor/Company Certification Program

The Information and Communication Security Auditor/Company Certification Program has been designed to provide the skills needed to determine the qualifications and competencies of the companies and auditors that will carry out the compliance audits in accordance with the Information and Communication Security Guide. The Program is being implemented in cooperation with the Turkish Standards Institution and the Scientific and Technological Research Council of Türkiye (TÜBİTAK). A total of 163 auditors and 23 companies have been certified and authorized under the Certification Program since 2021.

4.5 Information and Communication Security Compliance and Audit Monitoring System

The Information and Communication Security Compliance and Audit Monitoring System⁴² was developed and put into service on 4 January 2023. The system allows the monitoring of the audit results of all organizations covered by the Information and Communication Security Guide. Since then, 2,945 users and 1,191 organizations have already registered on the system. Organizations can provide information about the progress of their Information and Communication Security Guide compliance and audit activities. The current compliance level of organizations' information security management systems can also be tracked through this digital platform.

4.6 The National Cyber Security Governance Model Analysis and Reporting Project

The National Cyber Security Governance Model Analysis and Reporting Project, which was initiated to examine the cybersecurity governance model in Türkiye, has been completed. A comparative analysis was conducted by reviewing different countries' cases, and recommendations were presented for the improvement. As a result, "Cyber Security Governance Framework" was developed for Türkiye.

Following the completion of the project, a National Cyber Security Workshop was organized on 13 December 2022 to share the outputs of the National Cyber Security Governance Model Analysis and Reporting Project. More than 40 public institutions and more than 100 participants shared their opinions and suggestions during the workshop. According to the results of the workshop, it was determined that there is a need for a national cybersecurity law. Work is under way to finalize this law.

⁴² cbddo.gov.tr/en/bigdes/.

5. Activities and projects of Digital Transformation Office on the cybersecurity ecosystem

5.1 Turkish Cyber Security Cluster

In October 2017, public sector institutions, academia and the major cybersecurity companies in the private sector were invited to discuss possible cooperation among these bodies, resulting in the establishment of the Turkish Cyber Security Cluster.⁴³ Today, the cluster is operating under the coordination of the Digital Transformation Office and the Secretariat of Defence Industries (SSB) with more than 200 members, which have more than 400 products and services. Turkish Cyber Security Cluster is also a member of Global Ecosystems Partnered in Innovation and Cybersecurity (Global EPIC) since 2018.

The Turkish Cyber Security Cluster pursues several goals, including

- Increasing the number of cybersecurity companies
- Supporting the development of technical, administrative and financial capabilities of the member companies
- Improving the branding of products and services
- Improving the standards of the cybersecurity ecosystem
- Increasing the competitiveness of member companies in the national and global markets
- Improving the human capital in the field of cybersecurity
- Increasing awareness about cybersecurity throughout the society

Although there is no legal obligation for the private sector to take part in such cooperation, the emphasis is kept on the mutual trust and collaboration between public sector and private institutions. The key motivation behind this effort is to strengthen the buyer-supplier relationships, common distribution channels, joint networking opportunities and research and development activities conducted by universities with companies that can create better opportunities and benefits for both parties. Because of the shared economic interests, the companies in the cluster became more productive, more innovative and therefore more competitive than companies operating alone.

It is usually not possible to achieve success in the field of cybersecurity without the support of the highest-level public authority. Türkiye has companies that have expanded abroad and qualified, unique cybersecurity products trading overseas. Some of these products are also included in Gartner reports. The breach and attack simulation category is one of them.

5.2 Foreign Economic Relations Board (DEİK) – Digital Technologies Business Council (DIGITECH) – Cyber Security Committee

In order to increase the effectiveness of our domestic and national companies abroad, the Digital Technologies Business Council (DIGITECH)⁴⁴ was launched in June 2022 with the support of the Digital Transformation Office and under the coordination of the Foreign Economic Relations Board (DEİK). The Digital Technologies Business Council (DIGITECH) is committed to carry out projects on:

- Globalization of Türkiye's digital technologies ecosystem

⁴³ <https://siberkume.org.tr/>.

⁴⁴ www.deik.org.tr/sectoral-business-councils-digital-technologies-business-council?pm=65.

- Adapting to new trends
- Access to international finance, digital transformation and regulations

The aim of DIGITECH:

- Increasing the number of Turkish companies under Fortune 500 and the number of Turkish unicorns (Turcons)
- Making Türkiye a tech hub and creating digital corridors with other countries
- Enhancing Türkiye's export of high technology products
- Promoting the internationalization of tech companies via 144 bilateral business councils of DEİK
- Supporting digital transformation of industrial companies by partnering up with start-ups
- Increasing the venture capital in the sector in both size and number by creating platforms to bring together global venture capitals, domestic venture capitals, scale-ups and start-ups
- Identifying the problems faced by the sector and informing respective governmental bodies about those problems

The subcommittees under DIGITECH are as follows: Cloud Technology, Financial Technologies (Fintech), Mobile Technologies, Gaming, Cyber Security, Software Technologies, Innovative Technologies, Venture Capital, Health Technologies, Web3-Blockchain. As can be seen, in this structure, where Cyber Security is also a subcommittee, there is a sectoral perspective.

The development of domestic technologies in the field of cybersecurity is of strategic importance in Türkiye and is recognized as a matter of national security. Thus, emphasis is placed on creating robust, large-scale products and services that can rival their foreign counterparts. The global cybersecurity market, fuelled by increasing awareness of data risks and threats, has recently recorded significant growth. The market share of cybersecurity products and services is projected to continue to increase.

Türkiye is part of this expanding economy, collaborating with the private sector and government institutions to develop its solutions on a global scale. Accordingly, the Digital Transformation Office is working to strengthen domestic cybersecurity technologies. This endeavour is part of the mandate given by Presidential Decree No. 1, which states; To carry out studies to develop domestic and national cybersecurity products in all fields, especially critical infrastructures, and to expand their use in the public sector.

To encourage the growth of the domestic ecosystem in cybersecurity, a systematic approach has been initiated under the coordination of the Digital Transformation Office. This approach aims to integrate the incentive system with public procurement, assess the maturity levels of domestic cybersecurity products and gradually enhance and expand them.

The "Domestic Cyber Coordination Group" was formed in 2021 under the coordination of the Digital Transformation Office, with the leadership of the Secretariat of Defence Industries (SSB), the Ministry of Industry and Technology (MoIT), the State Supply Office, the Public Procurement Agency (KİK) and the Presidency of Strategy and Budget (SBB). The Ministry of Treasury and Finance (MoTF), Scientific and Technological Research Council of Türkiye (TÜBİTAK), Turkish Standards Institution, TURKSAT, the Ministry of Transportation and Infrastructure and the Information and Communications Technologies Authority

(BTK) later joined this group. The main objective is to encourage the use of domestic and national cybersecurity products across all sectors, both domestically and internationally, with a primary focus on the public sector. The activities of the group are divided into five main pillars: policy, legislation, standardization/maturity, incentive/support/financing and internationalization.

6. Activities and projects of the Digital Transformation Office on raising cybersecurity awareness

6.1 TeknoFest cybersecurity contests

The Digital Transformation Office is aware that the need for cybersecurity awareness and skills is becoming increasingly urgent given the importance attributed to information and communications technologies (ICTs). In this regard, the Digital Transformation Office also organizes contests to increase cybersecurity awareness. One of the outstanding projects is HackIstanbul. It is recognized worldwide as an extraordinary contest and has been held as part of the TeknoFest Aviation, Space and Technology Festival⁴⁵ since 2018. These contests opened their doors to all hackers around the world to showcase their talents in Istanbul, contests were held under the name “HackIstanbul”, and only in 2020 the contest was held in Gaziantep under the name: “HackZeugma”. In 2022, the Digital Transformation Office organized HackBlackSea 2022 in Zonguldak in August.

Applications for the HackMasters 2023 competition, which was held on 23 April 2023 this year, closed in March 2023. The finalists were determined during the online bounty-hunting phase. In the final phase, held on April 28, contestants were given a scenario focused on the cybersecurity of smart devices. Hackers tried to compromise systems by looking for vulnerabilities in smart home devices, mobile applications that manage them and cloud infrastructures that receive data from these devices, trying to take over the systems.

Each year, different concepts, such as operational technology systems security, bug bounty or “capture the flag” cybersecurity challenge are addressed in the contest contents. These contests aim to raise awareness on cybersecurity and to bring new talents to the sector. On the other hand, an indirect benefit of the project is the worldwide promotion of Türkiye regarding cybersecurity.

The deadline for HackMasters 2024⁴⁶ applications is 31 May 2024, and the final stage will be held in August 2024 in Istanbul as part of TeknoFest.⁴⁷

6.2 Cyber Intelligence Contest

Furthermore, the Digital Transformation Office organizes several cybersecurity camps and training programmes, as well as “capture the flag” events with relevant public institutions, such as the Ministry of National Education and the Ministry of Youth and Sports, the private sector and non-governmental organizations. These camps and training programmes ensure that enough young people are inspired to utilize their talents in cybersecurity. It is also important to note that the number of students participating in these events is over 1 million.

Moreover, the other outstanding event is the Cyber Intelligence Contest.⁴⁸ These contests are part of training and awareness activities that aim to increase the number of individuals with cybersecurity awareness, and they are very effective in this regard.

⁴⁵ www.teknofest.org/en/.

⁴⁶ <https://hackmasters.com.tr/>.

⁴⁷ www.teknofest.org/en/competitions/hack-masters/.

⁴⁸ <https://cbddo.gov.tr/en/projects/cyberintelligencecontest/>.

A total of 1.5 million students from the primary, secondary and high school levels participated in the contest.

The contest is an online event and is organized separately for the primary, secondary and high school levels. Questions are prepared by the Digital Transformation Office and finalized with the support of the Ministry of National Education by taking into account the current curriculum. Announcements are made through the social media accounts of the Digital Transformation Office, the Ministry of National Education and the EBA (education information network) platform. In the contest, the students who give the most correct answers in the shortest time possible receive surprise gifts and rewards to increase their motivation in this field.

The fourth Cyber Intelligence Knowledge Competition took place in 2023. This competition, which was first organized in October 2020 in collaboration with the Presidency and the Ministry of National Education, is aimed at primary, middle and high school levels. The competition was held on 27 December 2023, for primary school students, on 28 December 2023, for middle school students, and on 29 December 2023, for high school students. The competition had a total of 16,915 primary school, 15,955 middle school and 4,528 high school student registrations.

6.3 Digital Crew cartoon

Having conducted many studies on raising cybersecurity awareness on a national scale, the Digital Transformation Office also recognizes the need to increase digital literacy even when children are not online. This goes beyond technical know-how. It refers to the knowledge, skills and attitudes that enable children to be both safe and empowered in a digital world. One of the important projects developed for this purpose targeting children is a popular cartoon film series called *Digital Crew*.⁴⁹ It has been broadcast on Turkish Radio and Television Çocuk (“Kid”) since 2020. The main objective of this project is to increase digital cognition, literacy and awareness among children. The content of the series of *Digital Crew*, which consists of 10 episodes, was prepared in cooperation with the Digital Transformation Office. Episodes cover a wide range of topics from children’s safe Internet to cyberbullying, from Internet addiction to artificial intelligence (AI), from the Internet of things to the impact of digitalization on life and national technologies.

7. Activities and projects of the Digital Transformation Office on cybersecurity education

Undoubtedly, one of the most important components in ensuring national cybersecurity is human resources with sufficient competence and expertise. In order to meet the needs of our country in this field, the Digital Transformation Office carries out activities to increase the level of competence of the existing human resources. Some of these initiatives are detailed below.

7.1 Cybersecurity Vocational High School in cooperation with the Ministry of National Education of the Republic of Türkiye

Concrete steps were taken to develop skills and capabilities in the field of cybersecurity in formal education and, as a result, the curriculum developed for the secondary education level started in 2020.

Teknopark Istanbul Vocational and Technical Anatolian High School, Türkiye’s first cybersecurity high school, was established by the Ministry of National Education with the contributions of the Turkish Cyber Security Cluster, the Secretariat of

⁴⁹ www.youtube.com/watch?v=YnuLs6GAogM&ab_channel=CBDijitalD%C3%B6n%C3%BC%C5%9F%C3%BCmOfisi.

Defence Industries (SSB), the Digital Transformation Office and Technopark Istanbul. Located in Teknopark Istanbul, the school provides education in the fields of information technologies, network management and cybersecurity.

The Cybersecurity Vocational High School has been at the top of the preferences list since the day it was opened.

7.2 Establishment of Cybersecurity Vocational Colleges in cooperation with the Council of Higher Education of the Republic of Türkiye

The Digital Transformation Office has started a new project to train qualified personnel in the field of cybersecurity by further developing the model applied in the Cybersecurity Vocational High School mentioned above. With the cooperation protocol signed between the Digital Transformation Office and the Council of Higher Education⁵⁰ in 2022, the first step was taken for the Cyber Security Vocational Colleges.

Cyber Security Vocational Colleges, which will offer education programmes only in the field of cybersecurity, were opened in 2023. The first programme offered in these schools is “Cyber Security Analyst and Operator”.⁵¹ This programme has been launched in four of the major universities in Türkiye: Ankara University, Ege University, Gebze Technical University and Istanbul Technical University.

8. Türkiye in global indices

As a result of the adoption of digital technologies at the local and national level, cybersecurity has become as important as physical security for the country. Given the increasing threat, sufficient investments have been made in the field of cybersecurity in the public and private sectors. Many coordinated projects have been carried out in the public, private and military domains; significant investments have been made by important defence industry organizations; cybersecurity-specific institutes have been established in the academic field; and new products and technologies have been developed with national capabilities. As a result of these efforts, Türkiye has recently become one of the most successful countries in the field of cybersecurity.

Thanks to the efforts of government and public sector actors to achieve these goals, Türkiye’s ranking in the global cybersecurity indices has been positively affected.

Türkiye enjoys a high ranking in the Global Cyber Security Index, reflecting the achievements of the country to date.

According to the Global Cyber Security Index published by the International Telecommunication Union (ITU) in 2021,⁵² Türkiye ranked eleventh in the world, rising nine places as compared with the previous year and sixth in Europe.

In today’s global landscape ICTs have assumed an indispensable role. They are the sinews of our societies, intricately linking economies, Governments and individuals across the vast expanse of the globe. To imagine a world without instant communication, seamless access to information or the ability to conduct business electronically is to imagine a fundamentally different reality. ICT has demonstrably impacted every facet of the human experience, from the dissemination of knowledge and the delivery of health care to the realms of entertainment and social interaction. It is empowering citizens, fostering breakthrough innovation and driving economic growth at unprecedented rates. In addition, Governments can harness the power of

⁵⁰ <https://cbddo.gov.tr/projeler/siber-myo/>.

⁵¹ cbddo.gov.tr/ssss/siber-myo/.

⁵² www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

ICTs to deliver services with greater efficiency, transparency and inclusiveness, fostering a more participatory and robust democratic framework.

However, while this paradigm of connectivity offers immense benefits, it also comes with a significant caveat: security. As our reliance on ICTs relentlessly expands, so does the vulnerability we expose ourselves to. Malicious actors, ranging from cybercriminals seeking personal gain to State-sponsored entities with geopolitical agendas, exploit these vulnerabilities to target critical infrastructure, government systems housing sensitive data and citizens' personal information. The globally interconnected nature of ICT infrastructure creates a complex web of interdependencies, where a single security breach in one remote corner of the world can have cascading effects elsewhere, potentially disrupting essential services, causing economic hardship and undermining public confidence. The emergence of new technologies, such as artificial intelligence and the Internet of things), introduces a whole new dimension of security challenges that require immediate attention and the development of innovative solutions, as these technologies often introduce new attack vectors and complexities in securing vast networks of interconnected devices.

It is therefore imperative to carefully navigate a path that promotes a judicious balance between harnessing the immense potential of ICTs and mitigating the associated risks. States must prioritize the security of information and communications technologies and recognize it as a national security imperative. This requires a multifaceted approach. The development of robust national cybersecurity strategies, supported by strong public-private partnerships that leverage the expertise and resources of both government and industry is paramount.

Collaborative efforts between Governments and businesses to invest in cybersecurity education and awareness for both citizens and government officials are equally critical. Such education should not only include technical skills to identify and mitigate cyberthreats but also promote a culture of cyberhygiene among citizens.

Furthermore, the promotion of international cooperation on ICT security is undeniably essential. In this context, regular institutional dialogue under the United Nations umbrella is very important. Member States must work together to establish a framework of international norms, standards and legal frameworks that promote responsible behaviour in cyberspace. This framework should include information-sharing protocols to facilitate rapid response to cyberthreats, cooperative law enforcement efforts to more effectively combat cybercrime and the development of international treaties that establish norms of acceptable behaviour in cyberspace. Ultimately, the goal goes beyond purely defensive measures for building a resilient ICT infrastructure. This includes designing systems that have not only the strength to withstand cyberattacks but also the ability to recover quickly, minimize disruptions and maintain data integrity. In addition, promoting the ethical development and use of ICTs is important. Member States can ensure that this powerful technology serves the greater good of human values by prioritizing user privacy, advocating for responsible research practices that minimize the potential for misuse and ensuring transparency in the development and deployment of ICT systems.

By prioritizing security while promoting innovation, Member States can ensure that ICTs continue to play a transformative and positive role in shaping our world. This collaborative approach, coupled with continuous vigilance and adaptation, is essential to ensure a secure and prosperous digital future for all.

United States of America

[Original: English]
[1 May 2024]

Introduction

United Nations Member States have acknowledged that ICTs have the potential to be used for purposes that are inconsistent with the objectives of maintaining international peace and stability. Over the course of many years, States have come together under the auspices of the United Nations to discuss and address this issue. Through consensus affirmation of reports from the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the open-ended working group on security of and in the use of information and communications technologies 2021–2025, States have coalesced around a framework for responsible State behaviour in the use of ICTs. This framework for enhancing international stability is composed of the embrace of relevant international law, including the Charter of the United Nations, as well as a set of non-binding norms and confidence-building measures.

While the framework has received global support, its success depends on States' adherence to and implementation of its elements. As first articulated in the consensus report of the Group of Governmental Experts in 2015, States have affirmed the need to establish regular institutional dialogue with broad participation under the auspices of the United Nations.¹ Building on that effort, the open-ended working group has since continuously reaffirmed the need for States to pursue the establishment of a mechanism for future institutional dialogue.²

In addition, as noted in the most recent consensus annual progress report of the open-ended working group, States agreed on an initial set of common elements of regular institutional dialogue, and also agreed to continue discussions on a future programme of action. States agreed, importantly, that future regular institutional dialogue should take “as the foundation of its work the consensus agreements on the framework of responsible State behaviour”.³ States also agreed that future dialogue should be single-track, State-led and permanent.⁴ States further concluded the mechanism should be open, inclusive, transparent, sustainable and flexible⁵ so that it can adapt as necessary to the rapidly evolving cyberthreat landscape. In his report published in April 2023 (A/78/76), the Secretary-General underscored the urgency of establishing the programme and highlighted many of the same issues addressed by the common elements identified in the 2023 annual progress report of the open-ended working group, including that the framework “must serve as a baseline” for the programme of action.⁶ In the report, the Secretary-General also concluded that many States value the inclusive, meaningful participation of non-governmental stakeholders.⁷ States continued to call for meaningful multi-stakeholder participation in formal and intersessional meetings of the open-ended working group.

Over the course of the past two years, States have coalesced around the programme of action as the future permanent mechanism for United Nations First Committee discussions on cyberissues. Most recently, nearly all United Nations Member States voted in favour of resolution 78/16, in which the General Assembly

¹ A/70/174, para. 18.

² A/75/816, paras. 70–74, and A/78/265, para. 52.

³ A/78/265, para. 55 (c).

⁴ Ibid., para. 55 (a).

⁵ Ibid., para. 55 (d).

⁶ A/78/76, para. 42.

⁷ A/78/76, para. 40.

decisively established the mechanism under the auspices of the United Nations upon the conclusion of the current open-ended working group on security of and in the use of ICTs.

As outlined in the resolution, the programme of action will serve as a permanent, but flexible, mechanism in the United Nations to advance the work of the framework to enhance peace and security in cyberspace, including through meaningful engagement with the multi-stakeholder community and facilitating capacity-building through the role of the United Nations as an information-sharing platform.

Scope of the programme of action

General Assembly resolution [77/37](#) defined the scope and mandate of the programme of action as follows:

A permanent, inclusive, action-oriented mechanism to discuss existing and potential threats; to support States' capacities and efforts to implement and advance commitments to be guided by the framework for responsible State behaviour, which includes voluntary, non-binding norms for the application of international law to the use of information and communications technologies by States, confidence-building and capacity-building measures, as affirmed in General Assembly resolution [76/19](#), the 2010, 2013, 2015 and 2021 reports of the groups of governmental experts, the 2021 report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the first annual progress report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025; to discuss, and further develop if appropriate, this framework; to promote engagement and cooperation with relevant stakeholders; and to periodically review the progress made in the implementation of the programme of action as well as the programme's future work.⁸

In its resolution [78/16](#), the General Assembly reaffirmed the objectives of the programme of action as articulated in resolution [77/37](#) and also decided that the mechanism would have the common elements outlined in the 2023 open-ended working group progress report. Furthermore, the Assembly decided that the programme of action's scope, structure, content and modalities would be based on the open-ended working group's consensus outcomes.

Throughout the resolutions on the programme of action and the consensus resolutions that affirmed the reports of the Group of Governmental Experts and the open-ended working group, States have repeatedly affirmed the expectation that States should be guided in their actions by the assessments and recommendations of the 2010, 2013, 2015 and 2021 groups of governmental experts, as well as those of the 2021 Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, along with the current open-ended working group's consensus products (e.g. the first and second annual progress reports), and in particular "the cumulative and evolving framework for responsible State behaviour in the use of information and communications technologies elaborated and adopted by consensus through these processes".⁹ This consensus framework, articulated by the consensus Group of Governmental Experts and the open-ended working group reports and repeatedly endorsed by all Member States, is the foundation of the programme of action.

⁸ General Assembly resolution [77/37](#), para. 1.

⁹ General Assembly resolution [78/16](#), preambular para. 8.

Member States will set the programme of action's direction and update it over time, maintaining a priority focus on practical implementation and capacity-building work dedicated to the implementation of the framework. The permanent nature of the programme of action will make it a durable resource for States in these efforts.

As a permanent mechanism, the programme of action must also have the flexibility to address future threats and the agility to assess States' evolving needs and best practices to address these threats. Within the programme of action, States will also be able to consider whether and how the consensus framework should evolve over time.

Non-State stakeholders will be an integral part of the programme of action process. Almost all capacity-building efforts, international or domestic, involve private sector, civil society, academia and other non-State stakeholders' activities and expertise. The programme of action must have modalities for stakeholder participation that are as inclusive as possible to fully leverage these stakeholders' expertise.

Establishment of a programme of action

Member States must aim for a seamless transition to the programme of action in 2025 following the conclusion of the 2021–2025 open-ended working group. Such a transition must be facilitated by a final report of the open-ended working group that reaffirms the programme's mandate as defined by General Assembly resolution [77/37](#) with the consensus framework as its foundation, articulates its action-oriented structure and working methods, defines priority areas of work, confirms a maximally inclusive approach to stakeholder participation and defines next steps and detailed timing for the programme's official launch by 2026.

To fully define the modalities of the programme of action, an additional preparatory meeting or process may be needed. In addition, if the open-ended working group fails to reach consensus on a final report, a more comprehensive "international conference"¹⁰ or other preparatory process established through the General Assembly will be needed to fulfil the directive outlined in resolution [78/16](#) to launch the programme by 2026. Programme meetings must begin in 2026 to ensure the continuity of these important multilateral discussions.

Given the programme of action's mandate to address the peace and security dimensions of the use of ICTs, it will naturally be established under the First Committee of the United Nations. The Office for Disarmament Affairs is a logical secretariat for this future mechanism. The programme should function within existing budgetary resources to the greatest extent possible.

Structure

The structure of the programme of action should consist of technical working groups that meet three or four times a year, annual plenary meetings and periodic review conferences. The programme would be supported by a secretariat office within the Office for Disarmament Affairs.

The programme of action's technical working groups are the essence of its action-oriented nature – not an optional feature. To make these groups as inclusive as possible, all interested States would be invited to work together in focused groups to develop concrete recommendations that support implementation of the framework. These recommendations would be included in reports for the consideration of the plenary and, ultimately, the General Assembly.

¹⁰ General Assembly resolution [77/37](#), para. 3

These working groups must be cross-regional in composition and take a cross-cutting approach to implementing the framework, developing recommendations, assessments and best practices on issues such as:

- Defending critical infrastructure
- Facilitating cooperation between States following a serious cyberincident
- Ways to improve accountability for irresponsible State behaviour in cyberspace
- Sharing information on the evolving cyberthreat landscape
- Improving States' ability to deter and disrupt ICT threats

Issue-based discussions would facilitate cross-cutting substantive discussion on implementing the framework that breaks out of the traditional silos of threats, norms, international law and capacity-building. In the open-ended working group, States repeatedly emphasized that these topics bleed into each other and need to be considered holistically. States also agree that capacity-building, in particular, cuts across all topics. Prioritizing the conversation about capacity-building needs within the implementation working groups will lead to realistic and feasible recommendations and will speed implementation.

The annual plenary meeting should be mandated to assess the progress of the technical working groups, take forward any recommendations from those groups, discuss ongoing and emerging threats and consider the status of practical initiatives such as confidence-building measures. The plenary may provide guidance for the technical working groups and practical initiatives, as needed.

The periodic review conference should meet every three or four years (replacing the annual plenary meeting during the years of the conference) for all Member States to assess the evolving cyberthreat landscape and the results of the programme of action's initiatives and working groups, update the framework as necessary and provide strategic direction and mandates for the programme's future plenaries, working groups and other initiatives. This periodic review of the programme would give States the flexibility to adapt the programme as circumstances evolve.

Each year following the 2026 launch of the programme of action, the First Committee would affirm any consensus outcomes of the programme's annual meetings through a resolution or decision. The First Committee would also affirm outcomes of periodic review conferences when they occur.

The programme of action secretariat, operated by the Office for Disarmament Affairs, would be mandated to support the administration of the various programme meetings; maintain information-sharing platforms, communication mechanisms and archives; and administer practical initiatives and projects such as the point-of-contact directory, the threat repository and information-sharing portals.

Capacity-building

Given that countries are at all stages of developing their cyberexpertise and -skills, the United Nations has acknowledged that "capacity-building is essential for cooperation of States and confidence-building in the field of information and communications technology security".¹¹ The United Nations has a key role in convening, coordinating with and highlighting the range of multi-stakeholder actors who are actively engaged in capacity-building on relevant cyberissues, as well as implementing specific capacity-building programmes as directed by Member States.

¹¹ Ibid., preambular para. 20

The programme of action's primary capacity-building function must be directly tied to States' national-level efforts to implement the framework. The programme of action should also facilitate dedicated discussions about what types of capacity-building States need to implement the framework to ensure its efforts closely align with States' range of needs. In other words, it should aim to raise international awareness on the importance of cyber capacity-building to support the framework and facilitate coordination and information-sharing on available cyber capacity-building programmes alongside other stakeholders, while also providing guidance and best practices that States could use domestically/nationally to implement the framework.

The United States recognizes that many States still lack an in-depth understanding of the framework and its importance. Many also lack the national-level cybersecurity capacity needed to implement the framework, including domestic authorities and capabilities associated with supporting norms and confidence-building measures. There are a range of existing United Nations and non-United Nations entities with expertise in areas such as national cybersecurity policies and strategies, cyberincident management and critical infrastructure protection, domestic cybercrime legislation, cybersecurity culture, cybersecurity standards, and donor coordination and matchmaking for international cybersecurity assistance. The programme of action must not duplicate or supersede such existing efforts. All of these programmes – which are largely multi-stakeholder in nature – enhance States' national security posture and ultimately enable implementation of the framework, although they are outside of the mandate of the programme of action.

Multi-stakeholder participation

States must retain exclusive decision-making authority within the programme of action. Nonetheless, non-governmental stakeholders, including civil society, academia, regional and international bodies and the private sector, play a positive role in multilateral forums by bringing expertise to formal discussions and contributing to capacity-building efforts. Relevant non-State stakeholders must have an opportunity to actively participate in and contribute to the programme of action as observers, without the right to vote. The expertise of non-governmental stakeholders will be particularly important within technical or working groups. These technical working groups will facilitate more in-depth, practical engagement with a range of non-State stakeholders. Stakeholders could also provide periodic reports on their efforts to implement framework-focused initiatives, including capacity-building.

For the programme of action to be as inclusive as possible of interested stakeholders, including within its subsidiary technical working groups, the modalities should build upon existing gold standards for stakeholder participation, including providing transparency as to States' objections and a process for evaluating possible exclusions. For example, States can look to the Open-ended Working Group on Ageing as a model. That Group's modalities provide the opportunity for Member States to object to the participation of an organization but require objections to be raised publicly for the awareness of Member States and a subsequent vote to determine whether those organizations to which an objection was raised should be excluded. Organizations to which no Member State objects in the first round are automatically authorized to participate in the formal session.¹²

In addition to considerations for how stakeholders are accredited to attend meetings of the programme of action, modalities should also provide guidance for how accredited stakeholders can contribute to the programme's discussions in practice. In this area, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications

¹² As articulated in section F of A/AC.278/2011/2.

Technologies for Criminal Purposes could serve as a model. Its modalities allow multi-stakeholder participation to include:

- Attending any open formal session.
- Depending on the time available, making oral statements, at the end of discussions by Member States, on each substantive agenda item. Given limited time available at meetings, multi-stakeholders may consider selecting from among themselves spokespersons, in a balanced and transparent way, taking into account the equitable geographical representation, gender parity and diversity of participating multi-stakeholders.
- Submitting written materials with limitations on word count. These submissions are posted in their original language on the website of the Ad Hoc Committee.¹³

The programme of action should also leverage existing expertise and ongoing work at the regional level. Allowing those entities to participate in discussions on the programme of action, as stakeholders, would help work at the United Nations level better integrate with regional efforts and account for specific regional challenges and contexts.

Venezuela (Bolivarian Republic of)

[Original: Spanish]
[26 April 2024]

In paragraph 8 of General Assembly resolution [78/237](#), adopted on 22 December 2023, the Assembly invited all Member States to continue to inform the Secretary-General of their views and assessments on security of and in the use of information and communications technology, in particular on the future regular institutional dialogue on these matters under the auspices of the United Nations, and requested the Secretary-General to submit a report based on those views to the General Assembly during its seventy-eighth session for further discussion between Member States in the meetings of the open-ended working group at its eighth session in 2024.

In that connection, the Bolivarian Republic of Venezuela considers it necessary to stress the importance of the open-ended working group and the format of its work for the fulfilment of the mandate set out by the General Assembly in its resolution [75/240](#). The achievements of recent years, such as the establishment of the global intergovernmental points of contact directory, demonstrate that the current format of the open-ended working group has been quite successful, particularly owing to its reliance on consensus in decision-making and the approval of annual reports.

The Bolivarian Republic of Venezuela considers that the United Nations should continue to play a central, critical role in promoting dialogue on the use of information and communications technology by States. The *sui generis* nature of information and communications technology implies the need to develop new principles and rules, preferably legally binding ones, by which the gaps between existing international law and the realities of the virtual sphere can be filled.

In view of the foregoing, there is a pressing need to provide continuity to the work of the open-ended working group 2021–2025 by establishing a new, permanent open-ended working group after 2025, which will help to strengthen the capacity of the new iteration of the open-ended working group to develop and adapt new legally

¹³ A/AC.291/6, para. 3.

binding rules that help to strengthen international security in the use of information and communications technologies.

In addition, the next open-ended working group, to be established after 2025, must be equipped with the capacity to address the challenges that arise from the considerable digital divide between Member States, a divide that makes it difficult to define global strategies aimed at strengthening international security in the use of information and communications technologies.

Lastly, there is broad support for the extensive efforts made by the Chair of the open-ended working group to achieve consensus in all the group's activities, and the Bolivarian Republic of Venezuela reiterates its willingness to continue to participate in and support this process.

Replies received from intergovernmental organizations

European Union

[Original: English]
[29 April 2024]

Cyberspace, and in particular the global, open Internet, has become one of the backbones of our societies. It offers a platform that drives connectivity and economic growth. The European Union and its member States support a global, open, stable and secure cyberspace grounded in the rule of law, human rights, fundamental freedoms and democratic values that bring social, economic and political development globally.

The international community recognizes that existing international law, including the Charter of the United Nations in its entirety – is applicable to State conduct in cyberspace and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.

The consensus recommendations of the 2010, 2013, 2015 and 2021 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, the consensus recommendation of the 2021 Open-ended Working Group on Developments in the Field of Information and Communications in the Context of International Security and the 2022 and 2023 consensus annual progress reports of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 have developed and consolidated a framework for responsible behaviour of States in cyberspace. The framework comprises the application of international law to cyberspace, voluntary norms of responsible State behaviour, confidence-building measures and capacity-building.

The European Union and its member States reaffirm our commitment to act in accordance with these existing agreements, and our commitment to act in accordance with international law, including the Charter in its entirety, as well as the norms of responsible State behaviour in cyberspace. We are committed to promoting and progressing cyber peace and stability through discussions and in forums such as the current open-ended working group.

Against this background, and consistent with our support to the work of the open-ended working group, the European Union was not in a position to support resolution [78/237](#), entitled “Developments in the field of information and telecommunications in the context of international security”, adopted by the General Assembly on 22 December 2023.

The European Union considers that the resolution could have better represented the fragile consensus achieved in the open-ended working group, its preceding processes and previous consensus resolutions.

Principally, the resolution fails to reference the cumulative and evolving framework for responsible State behaviour in the use of ICTs – a framework that is the result of over 20 years of negotiations and that has repeatedly been endorsed by consensus by the General Assembly.

Instead, it highlights, notably in preambular paragraph 16 and paragraph 5, selected substantive proposals supported by a small group of States, which the European Union fears may hamper the incremental and consensus-based approach through which the open-ended working group has been able to make progress over the past years.

The European Union and its member States consider the implementation of the United Nations framework of responsible State behaviour in the use of ICT to be of utmost importance in ensuring an open, secure, stable, accessible and peaceful ICT environment, and we are concerned to see that this resolution relies on non-consensual text that could lead to reinterpreting the open-ended working group's work and existing consensual documents.

The European Union remains fully committed to finding common ground on advancing consensus in the current open-ended working group, as well as to collective efforts to design an inclusive, permanent and action-oriented mechanism for regular institutional dialogue after the conclusion of the current open-ended working group.

Regarding requests pursuant to paragraph 8 of the resolution

Much progress has been made on the discussion of a future mechanism after the conclusion of the open-ended working group 2021–2025. The report of the Secretary-General (A/78/76), mandated by the General Assembly in its resolution 77/37, included observations and conclusions on the scope, structure, principles, content, preparatory work and modalities for establishment of the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. In addition, the open-ended working group 2021–2025 agreed on common elements for a future mechanism for regular institutional dialogue in its 2023 annual progress report. Lastly, the Chair of the open-ended working group 2021–2025 has proposed further common elements in a discussion paper, drawing from delegations' proposals and discussions from the open-ended working group's sixth substantive session.

Taking into account the progress made in identifying common elements for a future mechanism, the European Union will further express its views on a future mechanism for regular institutional dialogue.

Advancement of international security and stability in cyberspace, and enhancement of understanding on and the implementation of the United Nations framework for responsible State behaviour in cyberspace, should remain priorities for the regular institutional dialogue on these matters under the auspices of the United Nations.

Responding to the call to establish a permanent, inclusive, transparent institutional dialogue, with broad participation, under the auspices of the United Nations, as articulated in the 2021 Open-Ended Working Group on Developments in the Field of Information and Communications in the Context of International Security and Group of Governmental Experts reports, the programme of action, a proposal

initiated by a cross-regional group of countries,¹ represents an opportunity to put forward a permanent structure for regular institutional dialogue at the United Nations level and therefore allow the international community to focus its discussions on substance rather than having recurring debates on future processes. In this context, the programme could become the evolving mechanism for future cooperation within the General Assembly's First Committee.

To this end, the collective focus should be on seeking to strike a balance between two equally important aspects of our work – implementation of the established framework for responsible State behaviour in the use of ICTs in the context of international security, and the further development of the framework. The development of the framework stems from, inter alia, the lessons learned during the implementation of the existing commitments.

The mechanism should be inclusive, action-oriented and provide a platform for detailed discussions and exchanges, facilitate capacity-building and allow for the further development of the normative framework and its updating in accordance with the ongoing developments in the ICT environment on the basis of consensus.

It should also allow for the formal participation of and regular consultations with relevant stakeholders, including the private sector, academia and civil society, so they can consider and provide their unique perspectives and expertise on relevant issues. This will further focus efforts on supporting States in promoting the implementation of the framework for responsible State behaviour and of needs-driven capacity-building to increase cyberresilience both nationally and globally.

The programme of action should be based on the normative framework as contained in the successive Group of Governmental Experts and open-ended working group consensus reports and resulting commitments and actions. The future mechanism should convene periodic review conferences every several years (for example, every three or four years) to review the framework for responsible State behaviour, to update the framework as necessary and to provide strategic direction for the mechanism's work.

The programme of action could hold annual formal sessions, which could collate the work of open-ended detailed discussions to be convened throughout the year. The annual formal sessions could decide on the creation of open-ended technical meetings, working groups or workstreams to focus on specific priority issues to advance through the programme.

Participation in the technical workstreams should be voluntary and open to all States. The set-up of workstreams, including the participation of stakeholders, and the frequency of meetings should be decided at the annual meetings or review conferences. These meetings should be geared towards the development of an outcome document containing operational conclusions grounded in lessons learned from the implementation of the framework for responsible State behaviour, in a cycle of continuous improvement.

The programme of action could also enhance regional engagement through cooperation with regional organizations to leverage relevant existing initiatives and build on existing capacity-building structures and platforms. These collective efforts would help countries articulate and receive needs-based capacity-building. While emphasizing the primary responsibility of States for the maintenance of international peace and security and their central role in the programme of action, exchange and

¹ See <https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf>.

collaboration with stakeholders should be enhanced by providing a venue for inclusive and meaningful participation.

On the preparatory work and the establishment of the programme of action, intersessional meetings and dedicated sessions of the open-ended working group should be organized in 2024 and 2025 to continue elaborating the different aspects of the programme of action, including the budgetary implications involving the permanent mechanism and the identification of the relevant actors within the United Nations to carry out these functions. Outcomes of these sessions should be reflected in the respective annual progress reports of the open-ended working group. The programme of action should be operational upon the conclusion of the open-ended working group 2021–2025.
