United Nations A/78/76

General Assembly

Distr.: General
18 April 2023
English
Original: English/French/Russian/
Spanish

Seventy-eighth session
Item 97 of the preliminary list*
Developments in the field of information and telecommunications in the context of international security

Programme of action to advance responsible State behaviour in the use of information and communications technologies 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 77/37, without prejudice to their individual positions. It consolidates States' views 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.

* A/78/50.

23-07300 (E) 230523 290623

Contents

I. Introduction

1. In paragraph 3 of its resolution 77/37, the General Assembly requested the Secretary-General to seek the views of Member States on the scope, structure and content for a programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security, and the preparatory work and modalities for its establishment, including at an international conference, taking into account Assembly resolution 76/19, the 2010,[1] 2013,[2] 2015,[3] and 2021[4] consensus 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,[5] 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,[6] the views and contributions submitted by Member States in the framework of the open-ended working group 2021–2025 and the regional consultations held in accordance with paragraph 4 of Assembly resolution 77/37, and to submit a report based on those views to the Assembly at its seventy-eighth session and for further discussion between Member States in the meetings of the open-ended working group 2021–2025. The present report is submitted pursuant to that request.

2. On 14 December 2022, the Office for Disarmament Affairs of the Secretariat circulated a note verbale to all Member States in which their attention was drawn to paragraph 3 of General Assembly resolution 77/37 and their views were sought on the matter. An extension of the deadline for submission of views was subsequently communicated through a note verbale dated 3 March 2023. The views received by 14 April 2023 are reproduced in the annex to this report. Views received after that date have been posted to the Meetings Place of the Office for Disarmament Affairs.[7]

3. Sections III, IV, V and VI of the present report provide a consolidated summary of elements received from Member States, without prejudice to their individual positions. Section VII sets out the observations and conclusions of the Secretary-General.

II. Background

4. In its resolution 77/37, the General Assembly welcomed the proposal to establish a United Nations programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. In the same resolution, the Assembly underlined the complementarity of the proposal for the programme of action with the work of the ongoing open-ended working group on security of and in the use of information and communications technologies 2021–2025 and reaffirmed that any future mechanism for regular institutional dialogue under the auspices of the United Nations on information and communications technologies security should be an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus-driven and results-based.

[1] A/65/201.
[2] A/68/98.
[3] A/70/174.
[4] A/76/135.
[5] A/75/816.
[6] A/77/275.
[7] See https://meetings.unoda.org/ga-c1/general-assembly-first-committee-seventy-eighth-session-2023.

5. In General Assembly resolution 77/37, the programme of action was described as a permanent, inclusive, action-oriented mechanism with several functions, including to:

(a) Discuss existing and potential threats;

(b) 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;

(c) Discuss, and further develop if appropriate, the framework;

(d) Promote engagement and cooperation with relevant stakeholders;

(e) Periodically review the progress made in the implementation of the programme of action as well as the programme's future work.

6. The proposal for a programme of action was first introduced by a group of co-sponsors in December 2020 under the auspices of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, whose sessions were held between 2019 and 2021, under the theme "Regular institutional dialogue".[8] A concept note on the organizational aspects of a programme of action was shared along with a text proposal for inclusion in the final report of the Open-ended Working Group (see table below).[9]

7. Following its initial introduction in December 2020, the proposal for the programme of action has been addressed in subsequent intergovernmental processes. States have agreed to continue exploring that proposal under the auspices of the open-ended working group on security of and in the use of information and communications technologies 2021–2025. Many States have presented various proposals and reflections regarding the programme of action during discussions on the agenda item "Regular institutional dialogue".

Consensus language related to the proposal for a programme of action

Document symbol	*Document title*	*Paragraph/section*
A/75/816	Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security	Paragraph 77
A/77/275	Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, annex entitled " Progress report on the discussions of the working group on agenda item 5"	Section G, paragraph 18 (b) Section G, Recommended next steps, paragraph 2

[8] Argentina, Canada, Colombia, Ecuador, Egypt, El Salvador, Gabon, Georgia, Iceland, Japan, Lebanon, Montenegro, Morocco, North Macedonia, Norway, Republic of Korea, Republic of Moldova, Singapore, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland and the European Union and member States of the European Union (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, France, Finland, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden).

[9] See https://front.un-arm.org/wp-content/uploads/2020/12/sponsors-oewg-concept-note-final-12-2-2020.pdf.

III. Scope, structure and principles

Scope

8. In their submissions, many States underscored the importance of securing the peace, security and stability of the information and communications technologies environment and noted that the overall purpose of any regular institutional dialogue dedicated to the use of information and communications technologies by States in the context of international security is to contribute to this objective. As discussions on the proposal for the programme of action have been held under the auspices of the First Committee of the General Assembly, many States emphasized that the scope of the programme of action should be centred on the maintenance of international peace and security by preserving an open, stable, secure, accessible and peaceful information and communications technologies environment. Several States noted that a programme of action could provide an overarching framework for cybersecurity initiatives. A few States referenced the specific objectives of cooperation, stability and resilience in this context. A number of States emphasized the role of the programme of action in preventing conflict and promoting the use of information and communications technologies for peaceful purposes.

9. Many States noted that the primary objective of the programme of action should be to support the practical implementation of the framework for responsible State behaviour in the use of information and communications technologies, as endorsed by the General Assembly by consensus in its decision 75/564 of 28 April 2021. Several States referred to that framework as "evolving and cumulative", noting that the programme of action should provide for the future development of the framework, especially in the face of new threats and challenges which may arise in cyberspace. In referring to the framework, several States described its content as a combination of norms of responsible State behaviour, applicability of international law to the use of information and communications technologies by States, confidence-building measures and capacity-building.

10. In reference to implementation of the normative framework, a number of States underscored that capacity-building, including financial and technical assistance, should be a fundamental component of the scope of the programme of action and should support States' ability to implement their commitments. A few States noted that the programme of action should enhance synergies with other relevant efforts, including those related to digital development.

11. The view was expressed that a mechanism for regular institutional dialogue on information and communications technologies security should incorporate the formulation of a legally binding instrument which complements applicable international law and effectively addresses growing threats. In this regard, some States expressed scepticism that a politically binding programme of action would contribute to accountability for implementation of the normative framework. It was noted that without legally binding provisions, the programme of action could discourage the possible formulation of a future legally binding instrument. Reference was made to other proposals for regular institutional dialogue presented in the context of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, including a United Nations convention on ensuring international information security.

Structure

12. States noted the critical importance of conducting discussions of State use of information and communications technologies in the context of international security under the auspices of the United Nations. In this regard, there was general agreement

that any discussion of future regular institutional dialogue must be conducted within the United Nations. Several States noted that the First Committee of the General Assembly was the most appropriate forum for taking forward such discussions.

13. Several States called for the programme of action to be anchored in a political declaration to be agreed by the General Assembly, through which, inter alia, (a) States' commitment to the framework for responsible State behaviour, as affirmed in previously agreed consensus reports and resolutions, could be reaffirmed; and (b) a permanent institutional mechanism for advancing implementation of the framework, further developing the framework, as appropriate, and fostering multi-stakeholder cooperation in relevant areas could be established.

Principles

14. Many States recalled the conclusion of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security that future regular institutional dialogue should take place through an action-oriented process with specific objectives, building on previous outcomes, which is inclusive, transparent, consensus-driven and results-based. In their submissions, many States underscored that these principles should underpin the programme of action.

15. Many States emphasized the critical importance of consensus decision-making. A number of States noted, in particular, that the programme of action must adopt its decisions on substantive issues by consensus. In allowing for the possibility of updating the normative framework through the programme of action framework, several States underscored that such decisions must be made on the basis of consensus. In this context, several States supported the application of the principles of flexibility and adaptability in allowing the framework to respond to new challenges in the future.

16. Other principles identified by States in their submissions included, inter alia, permanence, neutrality, legitimacy, sustainability, incrementalism, continuity and stability. Regarding permanence, some States noted that the permanence of a programme of action structure would provide for institutional stability and save the General Assembly time and resources in negotiating new mandates.

17. Many States saw multi-stakeholder engagement as an important principle in the elaboration of a programme of action. Several States recalled that, while it was the exclusive right of States to negotiate outcomes and make decisions, exchange with relevant stakeholders, including regional and subregional organizations, civil society, the private sector and academia, was valuable. Those States called for participation modalities that are inclusive. The view was expressed that the intergovernmental nature of the programme of action should be preserved. Others noted that collaboration with regional and subregional organizations, including by leveraging their expertise, should be undertaken with a view to avoiding duplication.

18. A few States noted the importance of creating an enabling environment to narrow the digital divide, including the gender digital divide. There was a call for promoting the effective and meaningful participation and leadership of women in relevant decision-making processes related to security of information and communications technologies.

IV. Content, preparatory work and modalities for establishment

Content

19. In their submissions, States reflected variously on the content that would promote, refine and implement common understandings and cooperative measures in the use of information and communications technologies by States in the context of international security.

20. States offered a range of proposals for the inclusion of specific content in the programme of action, including actions and commitments aimed at practical implementation of the normative framework. The range of offerings included proposals for a "labelling system" for endorsing and promoting activities in line with the objectives of the programme of action on capacity-building, development of a procedure for submission of requests for international assistance, a fellowship programme, a cross-regional partnering mechanism and a dedicated trust fund. Regarding the last-mentioned proposal, several States reflected on examples provided by existing mechanisms under the United Nations in the area of arms control, such as the United Nations Trust Facility Supporting Cooperation on Arms Regulation and the Saving Lives Entity fund. States noted other existing funding structures such as the World Bank Cybersecurity Multi-Donor Trust Fund and those at the regional and subregional levels.

Preparatory work

21. States recalled the importance of the work of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 and its critical role in supporting discussions on the elaboration of any future regular institutional dialogue. Many States underscored the important role of the open-ended working group in further elaboration of the proposal for a programme of action. A number of States underscored that initiation of the creation of the programme of action should occur only after the conclusion of the mandate of the open-ended working group and that the creation of the programme of action should be decided by consensus and under the auspices of the open-ended working group.

22. Several States expressed concern over the creation of parallel tracks which would draw excessively on limited resources and present difficulties for delegations, particularly smaller delegations from developing countries. In this regard, a number of States stated that further discussion of the programme of action proposal should be carried out exclusively within the open-ended working group, which provides the appropriate mandate for considering all proposals by States, given its inclusive nature and consensus-based decision-making. The view was expressed that the programme of action should not predetermine the decision of States on a future institutional dialogue mechanism on information and communications technologies security within the United Nations and that the programme of action proposal, along with all other proposals of States, must be discussed within the open-ended working group in accordance with its mandate as set out in General Assembly resolution 75/240.

23. Some States noted that the views and contributions of States presented under the auspices of the open-ended working group regarding the programme of action, as well as the present report of the Secretary-General submitted pursuant to resolution 77/37, should represent the basis for establishing the scope, structure and content of the programme of action. In this regard, many States called for further dedicated discussions in the meetings of the open-ended working group on the elaboration of the programme of action proposal, including dedicated sessions in 2024 and 2025 and the possibility of convening additional intersessional meetings.

Modalities for establishment

24. Many States recalled the reference in resolution 77/37 to the possibility of holding an international conference in support of the establishment of the programme of action. A number of States welcomed the convening of such a conference after the conclusion of the work of the current open-ended working group in 2025. A suggestion was made to convene the international conference immediately following the last session of the open-ended working group in 2025, with regular follow-up meetings on the programme of action to begin in 2026. The view was expressed that the international conference should be convened no later than August 2024. It was noted that a decision on the international conference would depend on the views and assessments of Member States, supported by the present report, regarding whether such a conference should be deemed necessary.

25. In their submissions, States reflected on the role of an international conference, including its adoption of a founding programme of action document on the basis of the preparatory work undertaken under the auspices of the open-ended working group on security of and in the use of information and communications technologies 2021–2025. Several States called for the international conference to provide for the participation of stakeholders and make decisions on the basis of consensus, at least on matters of substance.

26. A number of States supported the anchoring of the programme of action in a political declaration which could be adopted by the international conference and subsequently endorsed by the General Assembly

V. Functions

27. In their submissions, States identified various functions and activities under a future programme of action, including those related to exchange of information, inter alia, on existing and potential threats and how to address them; practical exercises and exchanges between computer emergency response teams; and discussions on international law, capacity-building and confidence-building measures.

28. A number of States referenced the need for the programme of action to identify gaps in the existing normative framework and consider actionable recommendations to support implementation efforts. The view was expressed that, in responding to gaps and challenges, States could consider new norms, rules and principles, as well as legally binding obligations, to advance the implementation of the agreed framework.

29. In the area of international law, several States stated that the programme of action could offer an inclusive framework for further discussion on applicability of international law to the use of information and communications technologies by States and deepen common understandings on this topic, including through a dedicated workstream. In this context, some States encouraged the presentation of national positions on how international law applies to cyberspace.

30. Regarding the exchange of information, including national experiences, the proposal was made for States to undertake a self-assessment with a view to sharing good practices. In this regard, several States noted existing tools for conducting such a voluntary assessment of progress in implementation such as the national survey of implementation of United Nations recommendations on responsible use of ICTs by States in the context of international security, available on the United Nations Institute for Disarmament Research Cyber Policy Portal.[10]

[10] https://nationalcybersurvey.cyberpolicyportal.org/.

31. Many States emphasized that capacity-building should represent a central programme of action function. A number of States recalled the consensus guidelines for capacity-building agreed in the report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.

32. Several States noted the value of leveraging existing efforts implemented by regional organizations and the United Nations Institute for Disarmament Research and other multi-stakeholder efforts such as those undertaken through the Global Forum on Cyber Expertise. The value of stakeholder engagement in the area of capacity-building was emphasized and the possibility of matching needs with resources was noted. One State proposed a practical mechanism to facilitate capacity-building through a four-step cycle of (a) developing a set of areas of capacity-building; (b) conducting a self-assessment of needs; (c) matching needs with resources; and (d) enabling a feedback loop.

33. The role of the programme of action in building trust and confidence, including through concrete confidence-building measures, was highlighted. In this regard, some States recalled the decision of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 to establish an intergovernmental global points-of-contact directory, which could play a role in the development of additional confidence-building measures.

34. Recalling the principles of flexibility and adaptability, several States noted the role of the programme of action in facilitating common understanding of existing and potential threats and how to address them. Some States noted the importance of the exchange of information on these matters, including on vulnerabilities and protection of critical infrastructure, including in the context of health care and medical services. Moreover, in considering emerging threats, several States noted that the programme of action should allow for further development of the framework, if appropriate, and on the basis of consensus.

VI. Follow-up mechanism and implementation

35. In their submissions, many States reflected on the format, frequency and focus of a follow-up mechanism for the programme of action. Many States supported formal meetings to discuss implementation and evolution of the programme of action framework. Some supported annual meetings, while others noted the possibility of biennial meetings. Other States expressed flexibility regarding the frequency of such meetings. With regard to location, several States supported the holding of follow-up meetings in New York, with a few noting the possibility of holding meetings at alternative locations such as Geneva. Many States underscored the importance of taking all decisions at these follow-up meetings on the basis of consensus and the importance of utilizing formal follow-up meetings as a means to consider implementation efforts.

36. A number of States reflected on the possibility of review conferences. Proposed frequencies ranged from every third or fourth year to every six years. A number of States indicated that the review conference would be the appropriate forum for considering potential adaptation of the programme of action framework in view of emerging threats. Several States noted that the review conferences would serve as a mechanism for identifying priorities and workstreams for the interim period, including the possible development of a programme of work.

37. In support of intersessional work, a number of States called for the creation of technical workstreams, working groups on specific topics and other forms of

intersessional consultative meetings. In this regard, several States underscored that the decisions on the creation of such working groups should be made at plenary follow-up meetings, including review conferences. The view was expressed that technical working groups could be convened in a hybrid or virtual format to allow for the broadest participation of experts. Suggested topics of focus for potential working groups included applicability of international law, implementation of specific norms of responsible State behaviour and the elaboration of new norms, rules and principles, including legally binding obligations or instruments, as appropriate. It was also suggested that the working groups could address thematic topics such as critical infrastructure protection.

38. Many States noted the value of a voluntary reporting mechanism and how it could support implementation of the programme of action and related capacity-building efforts. Several States recalled the national survey of implementation of United Nations recommendations on responsible use of ICTs by States in the context of international security as a relevant tool in this regard. Some States expressed interest in discussion on a standardized template for reporting. It was suggested that annual reporting be conducted using a survey format, which should be agreed by consensus, and that this would be user-friendly and carried out through an online platform. Some States noted that such voluntary reporting could support the identification of implementation priorities and map capacity-building needs.

39. A number of States noted that the Office for Disarmament Affairs would be the most appropriate entity to serve as secretariat for the programme of action. A few States noted the potential role of the United Nations Institute for Disarmament Research in supporting implementation of the programme of action, including through relevant research activities.

40. In reflecting on the follow-up and implementation mechanism for the programme of action, many States noted the value of inclusive participation of non-governmental stakeholders, including civil society, the private sector, academia and the technical community, and called for specific modalities for their participation. Several States referenced the ability of stakeholders to attend programme of action follow-up meetings and make written and oral contributions. Some States referenced specific examples of stakeholder modalities, including those agreed in the framework of the Open-ended Working Group on Ageing, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes and the group of governmental experts of the High Contracting Parties to 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 related to emerging technologies in the area of lethal autonomous weapons systems. The view was expressed that the modalities agreed for the open-ended working group on security of and in the use of information and communications technologies 2021–2025 should form the basis for participation modalities related to the programme of action.

VII. Observations and conclusions of the Secretary-General

41. A peaceful, stable and secure information and communications technologies environment where human rights and fundamental freedoms are respected and protected is paramount. The international community is facing extraordinary challenges in achieving this objective. Over the last several decades, there has been a vast increase in the scale, scope and frequency of the malicious use of information and communications technologies. There is broad recognition that, in addition to malicious use of those technologies by non-State actors, a number of States are

developing information and communications technologies capabilities for military purposes. The urgency of strengthening the safety and security of the information and communications technologies environment, including enhancing the protection of civilians from malicious activity, has grown exponentially. Malicious information and communications technologies-related incidents impacting infrastructure providing services to the public and critical to the functioning of society, including energy and the health-care sector, have been well documented.

42. The information and communications technologies environment is not a lawless space. The rule of law exists in the digital sphere just as it does in the physical world. States have affirmed that international law, in particular the Charter of the United Nations, applies to State use of information and communications technologies. As a result of dedicated work undertaken under the auspices of the General Assembly over the last two decades, all States have agreed to be guided in their use of information and communications technologies by specific norms of responsible State behaviour. This normative framework, underpinned by a universal affirmation of the applicability of international law and a commitment to confidence-building and capacity-building, represents a significant milestone in international cooperation towards an open, secure, stable, accessible and peaceful information and communications technologies environment. This progress has been hard won and must serve as a baseline for all future multilateral work in this area.

43. In times like these, we must recognize the critical importance of common norms, rules and principles for safeguarding the peace and security of the information and communications technologies environment and redouble efforts to implement them. The consideration of proposals for action-oriented mechanisms for advancing implementation of the universally endorsed normative framework for responsible State behaviour and for supporting State capacities to implement it is most welcome. In this regard, 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.

44. States continue to reaffirm that regular institutional dialogue under United Nations auspices supports the shared objectives of strengthening international peace, stability and prevention of conflict in the information and communications technologies environment. They have concluded that in light of the scope of threats emanating from malicious use of information and communications technologies, there is an urgent need to enhance common understanding, build confidence and intensify international cooperation. States have also concluded that such regular institutional dialogue on these matters should be inclusive, transparent, consensus-driven and results-based. Given the dynamic nature of information and communications technologies and the rapidly changing digital environment, flexibility and adaptability remain important factors to consider.

45. While the progress made thus far is laudable, we must remain vigilant in ensuring that multilateral agreements in this area are fit for purpose in the face of new threats and challenges. It is through this lens that all proposals for United Nations mechanisms to advance the peace and security of the information and communications technologies environment should be viewed.

46. There is broad agreement that consensus decision-making and inclusivity, in particular, are critical elements of regular institutional dialogue in this area. The consensus nature of multilateral discussions on information and communications technologies security must be retained. To ensure maximum inclusivity, States must heed the concerns of delegations, particularly smaller delegations from developing countries, that parallel tracks on the same issues cause overburdening and a drain on limited resources. Moreover, given the unique nature of information and

communications technologies and the particular role of non-governmental stakeholders in supporting implementation of agreed norms, inclusivity must extend to appropriate participation of and contributions by relevant stakeholders, bearing in mind the exclusive right of States in decision-making.

47. For the programme of action, and all other proposals made by States, the process of consultations and agreement will be an essential factor in determining the programme of action's level of acceptance and, by extension, its implementation and long-term success. In this regard, the open-ended working group on security of and in the use of information and communications technologies 2021–2025, given its role and universal and consensus-based character, remains the most appropriate forum for continuing to elaborate on and unpack the potential programme of action framework both substantively and procedurally. There is broad agreement that the open-ended working group should play a key role in further work on this proposal and that its current mandate, set to conclude in 2025, could facilitate additional exchanges on the proposal.

48. While all States agree on the need for regular institutional dialogue under United Nations auspices, not all States view the programme of action proposal as the only or the most appropriate mechanism capable of serving this purpose. **It is therefore 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 present 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. Procedural questions, including budgetary requirements, should also be considered. In addition to discussions under the agenda item "Regular institutional dialogue", a dedicated intersessional meeting on the programme of action proposal could be convened in both 2024 and 2025 to ensure that all positions are heard. In considering the programme of action proposal, it is imperative that States continue to work towards consensus. The active participation of the whole of the United Nations membership is essential to its success.**

Annex

Replies received

Albania

[Original: English]
[14 April 2023]

Contribution of the Government of Albania to the report of the Secretary-General on the programme of action towards implementing the framework and building resilience in line with the United Nations General Assembly Resolution 77/37

First and foremost, Albania believes that the United Nations should have an effective instrument to successfully maintain peace and stability in cyberspace; hence, Albania expresses its full support for establishing a programme of action.

The Government of Albania recognizes the importance of international cooperation and collaboration to address cybersecurity challenges effectively. In this regard, we believe that the programme of action will provide a framework for international cooperation and dialogue on cybersecurity, including the exchange of best practices, the development and implementation of existing norms and principles and the strengthening of capacities and capabilities.

At a time when technological advances are dramatically impacting international peace and security and the potential for misuse by States or non-State actors is significantly growing, the programme of action, as a permanent mechanism, could be instrumental in bringing resilience and stability to cyberspace.

Albania is committed to supporting the establishment of the programme of action and to actively participating in its work. We will therefore address our expectations on how the programme of action could support the implementation of the framework, and support States' capacities and efforts to build resilience based on five key principles:

- **Facilitate the exchange of best practices:** we expect that the programme of action will provide a platform for States to share their experiences and best practices in implementing the framework. This can help States to learn from one another, identify good practices and implement those good practices in their cybersecurity ecosystem.
- **Support capacity-building:** the programme of action should support States in building their capacities to respond to cyberthreats and cyberattacks. This can include training programmes, technical assistance and other forms of support to help States to enhance their capabilities to prevent, detect and respond to cyberincidents.
- **Facilitate and encourage the implementation of existing international law and norms of responsible State behaviour in cyberspace:** the programme of action should facilitate the implementation of agreed norms and principles for responsible State behaviour in cyberspace, with follow-ups and periodic discussions. This can help in creating a common understanding of what is acceptable behaviour in cyberspace and what is not, which can help to prevent cyberconflicts and promote stability.
- **Encourage information sharing:** the programme of action should encourage States to share information about cyberthreats and attacks, including indicators of compromise, malware samples and other technical information. This can help

to improve situational awareness and enable States to respond more effectively to cyberincidents.

- **Facilitate cooperation and inclusiveness:** the programme of action should facilitate cooperation among States, the private sector, academia and non-governmental actors in building resilience against cyberthreats. This can include initiatives to promote the adoption of best practices and standards, joint exercises and simulations and other forms of collaboration, in order to benefit from the expertise and resources of each actor.

In summary, our expectations of the programme of action as a future forum for regular institutional dialogue are that it would provide a valuable platform for States to exchange best practices, build capacities, develop norms and principles, share information and facilitate cooperation and inclusiveness. By doing so, the programme of action would contribute to strengthening States' resilience against cyberthreats and to the overall goal of maintaining peace and stability in cyberspace.

We reiterate the firm position of Albania for a global, open, free, stable and secure cyberspace where international law, including respect for human rights and fundamental freedoms, fully applies and for social, political and economic development.

We believe that multilateral efforts are important in continuing the dialogue among Member States and, with respect to the modalities for the establishment of a programme of action, we intend to continue our efforts, by working with other Member States to consolidate a consensus in favour of this proposal and move towards the possible creation of the programme of action when the open-ended working group on security of and in the use of information and communications technologies 2021–2025 concludes its work in 2025.

Australia

[Original: English]
[12 April 2023]

Australia welcomes the opportunity, in response to the invitation in General Assembly resolution 77/37, to provide its views on the scope, structure and content of 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 preparatory work and modalities for its establishment. This submission builds upon the research paper[1] submitted by Australia to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications 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.

[1] Available at https://front.un-arm.org/wp-content/uploads/2020/12/australian-research-paper-revised-december-2020-version-2-oewg-regular-institutional-dialogue.pdf.

Scope

States have recognized that there is "an urgent need to continue to enhance common understandings, build confidence and intensify international cooperation" and have also recognized "the utility of exploring mechanisms dedicated to following-up on the implementation of the agreed norms and rules as well as the development of further ones" (see A/75/816).

Under the auspices of the First Committee, the scope of the programme of action should inherently focus on existing and emerging threats in cyberspace that have the potential to affect international peace, security or stability and on measures to address them. The overall objective of the programme of action should be to contribute to the maintenance of international peace and security by promoting and preserving an open, secure, stable, accessible, peaceful and interoperable cyberspace.

Mandate

Key to the scope of the programme of action will be a clear and effective mandate. This mandate must take, as its foundation, the agreed framework and provide appropriate flexibility for the programme of action to build upon and further develop the framework.

To this effect, the mandate of the programme of action should provide a clear basis to promote, refine and implement common understandings and cooperative measures to respond to current and emerging cyberthreats in the context of international security, including with respect to how international law applies to State behaviour in cyberspace, non-binding norms of responsible State behaviour, measures to build trust and confidence between States, and targeted, coordinated capacity-building to implement the framework. The mandate should provide a periodic opportunity to assess whether additional actions are necessary to respond to the rapidly evolving cyberenvironment.

Structure and Content

Political Declaration

The programme of action could be based upon a political declaration setting out the commitments of States and providing a mechanism that could be endorsed by a General Assembly resolution. The political declaration should:

- endorse and reaffirm States' political commitment to the framework (including the application of existing international law in cyberspace) as agreed in successive Group of Governmental Experts reports[2] and the report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.[3]
- 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 Group of Governmental Experts and the Working Group.
- establish a permanent institutional mechanism to advance the 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

[2] See A/65/201, A/68/98, A/70/174 and A/76/135.
[3] A/AC.290/2021/CRP.2.

that the General Assembly, by consensus, endorses a report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, 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 the international community agrees to discuss and address;
- clearly foster and encourage engagement with relevant members of the multi-stakeholder community in relevant areas.

Australia proposes that States could affirm their commitment to a political declaration at a high-level event at the first review conference of the programme of action. The declaration should also be able to be updated via consensus and set the agenda for the next round of meetings. In addition, Australia recognizes the key role of the working group in the establishment of the future mechanism and suggests that it play a role in the discussion, development, negotiation and adoption of a political declaration for the programme of action and notes that any political declaration should be agreed by consensus by all countries.

Yearly meetings, review conference and technical meetings

Australia remains flexible on the frequency and type of meetings that might be convened under the programme of action. For example, the programme of action could hold annual formal sessions, which could collate the work of technical workstreams convened throughout the year. Review conferences could be held every several years (for example, every three or four years) to review and update the political declaration and resulting commitments and actions. The annual formal sessions could decide on the creation of working groups or workstreams to focus on the pressing issues to advance through the programme of action and adopt decisions and recommendations by consensus. This should be based upon the work conducted by technical workstreams, which should be inclusive, encourage the participation of experts and be dedicated to specific issues set out in the political declaration. As a starting point, the first cycle or session of the programme of action could include such topics as the framework's protections for critical infrastructure against malicious cyberactivity, the protection of health-care and medical services from malicious cyberactivity or the application of international law to hypothetical examples of types of malicious cyberactivity. As technology advances, threats evolve and proliferate and challenges to implementation remain. Therefore, the programme of action should provide a vehicle to increase agility in the face of such change.

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).

Implementation

To ensure that programme of action activities are evidence-based and data-driven, the programme of action should emphasize support for 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/). We also propose that the programme of action allow for regular consultation with relevant stakeholders.

Preparatory work and establishment

The working group plays a key role in the elaboration and preparatory work of the programme of action. The programme of action should build on the hard-fought consensus gains and cumulative discussions of the past six Groups of Governmental Experts and the inaugural and current 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. The programme of action should begin only at the conclusion of the current working group.

Conclusion

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.

We look 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.

Austria

[Original: English]
[13 April 2023]

Austria strongly supports the establishment of a programme of action to advance responsible State behaviour in the use of information and communications technologies (ICT) in the context of international security. In accordance with paragraph 3 of General Assembly resolution 77/37, Austria would like to highlight the importance of the following points with a view to the scope, structure and content of the programme of action:

1. As a First Committee mechanism, the scope of the programme of action should be matters related to the use of ICT in the context of international peace and security. Its overarching objective would be to contribute to the maintenance of international peace and security by preserving an open, stable, secure, accessible and peaceful ICT environment based on respect for international law and human rights. In our view, the establishment of a programme of action as a permanent mechanism would be the most suitable vehicle for achieving this objective.

2. The implementation of the framework of responsible State behaviour, by providing and regularly updating sets of actionable recommendations for national implementation efforts, should be at the centre of the work of the programme of action. As technologies further develop, the programme of action should address new threats and challenges as they arise by further developing the framework, if appropriate, or by supporting States in adjusting their response to new threats and challenges.

3. A key priority of the programme of action should be to support capacity-building efforts in relation to the implementation of the framework (including by

seeking to take advantage of existing efforts and initiatives) and to enhance multi-stakeholder cooperation in this area as well as coordination with other relevant initiatives.

4. Furthermore, the programme of action should advance exchanges on the implementation of specific aspects of the framework (a specific norm or topic, e.g. the establishment of a national computer emergency response team, or the protection of critical infrastructure). Regular briefings could also be organized with other organizations (e.g. the International Telecommunication Union, the World Bank Group or the Cybersecurity Multi-donor Trust Fund) to take into account the activities conducted within their mandates.

5. While emphasizing the primary responsibility of States for the maintenance of international peace and security and their central role in the programme of action, collaboration with civil society, the private sector, academia and the technical community is essential for States in implementing their commitments under the framework. Modalities for the proceedings of programme of action meetings should therefore enable all relevant stakeholders to attend formal sessions, deliver statements and provide inputs, as is the case in other First Committee processes in which their expertise is useful, such as the Meeting of Experts on Lethal Autonomous Weapons Systems of the Convention on Certain Conventional Weapons.

6. Austria stresses the importance of States' political commitment to the framework for responsible State behaviour in cyberspace and also stresses that the programme of action should be based on a political document reaffirming the normative framework as contained in the 2021 final reports of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security and of the open-ended working group on developments in the field of information and telecommunications in the context of international security.

Belgium

[Original: English]
[14 April 2023]

Further to General Assembly resolution 77/37, communication ODA/2023-001/Programme of Action ICT security of 14 December 2022 and the extension of the deadline to 14 April 2023, Belgium has the honour to share its views on a programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security.

Belgium would like to share the following:

1. Rationale

Since 2003, a series of working groups have consolidated a framework for responsible State behaviour in the use of information and communications technologies (the acquis), which was endorsed by the General Assembly in consensus resolutions 70/237 and 76/19 and reaffirmed in various documents, including those of the working group. The establishment of a "regular institutional dialogue" was also discussed. As to the normative framework, it has been noted that this framework is cumulative and evolving: new norms could be developed over time.

The added value of a programme of action would be to provide a permanent and inclusive institutional mechanism to support and follow up on the implementation of agreed norms. It should be an action-oriented mechanism.

2. Scope and objectives

The scope of the programme of action would be matters related to the use of information and communications technology (ICT) in the context of international security (First Committee mechanism). The overarching objective of the programme of action would be to contribute to preserving international peace and security and preserving an open, stable, secure, accessible and peaceful ICT environment. The programme of action would therefore specifically be aimed at fostering cooperation, stability and global resilience.

The programme of action should be based on several key principles:

(a) The programme of action should provide a permanent institutional structure to deal with cybermatters, which are now a well-established item under the First Committee;

(b) The programme of action should clearly reaffirm the established framework for responsible State behaviour as the basis for its future work, for example, via a founding political document which would recall the relevance of that framework;

(c) The programme of action should offer a flexible structure which would allow for the broad participation of States and would make it possible to deal with new challenges as they emerge. For example, the programme of action could hold annual or biannual plenary meetings that are open to all States and that would make decisions (on, for example, implementation or the further development of norms) based on the work done in the intersessional period by technical working groups (some of which could take place in New York and others in Geneva). Plenary meetings would be able to decide on the creation of new working groups to address new issues;

(d) The programme of action should allow for the possibility to update the framework on the basis of consensus, for example, via regular plenary meetings/ review conferences which could re-examine the framework and decide to further develop it if appropriate (the work of these review conferences could be prepared in the intersessional period by dedicated working groups and the plenary meetings);

(e) The programme of action should place a strong emphasis on support for implementation efforts, including via regular voluntary reporting of such efforts, which would enable a mapping of the most urgent needs and challenges, actionable recommendations updated on a rolling basis to guide States in their implementation efforts and support for capacity-building activities,

(f) The programme of action should ensure that support for capacity-building within the programme of action relates to the mandate of the First Committee, is relevant to the implementation of the framework and takes into account existing initiatives in this domain. Coordination with capacity-building activities undertaken in other venues (such as the International Telecommunication Union) could be explored, bearing in mind the need for each forum to act within the scope of its own mandate;

(g) The programme of action should ensure inclusivity, both for States and for the stakeholder community. Regarding stakeholders, the programme of action should clearly reaffirm that States bear primary responsibility in matters of international security (and therefore should retain the decision-making power), but its modalities should allow stakeholders to attend formal meetings, make statements and submit written inputs.

3. Legal basis and functioning

(a) Inspiration for an institutional framework could be found in the structure of the Arms Trade Treaty, the 1997 Convention on the Prohibition of the Use,

Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction and the Convention on Cluster Munitions.

(b) The programme of action could be based on a political document which would reaffirm States' political commitment to the framework for responsible State behaviour, as affirmed in relevant reports and resolutions.

(c) Such a document would establish a permanent institutional mechanism to:

(i) Review and advance the implementation of this framework (including by supporting States' capacities to do so): the programme of action would notably encourage regular voluntary reporting of national implementation efforts by creating its own reporting system or by promoting existing mechanisms (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). This reporting would serve as a basis to identify priorities in the area of norms implementation and to map needs in terms of capacity-building. Programme of action yearly meetings would deliver actionable recommendations about the national implementation efforts. Working groups could be created to support these efforts.

(ii) Support tailored capacity-building efforts to address the needs and challenges identified by States in relation to the implementation of the framework. It should also aim to foster the exchange of best practices and transfer of expertise, as appropriate. The programme of action should seek the cooperation of the multi-stakeholder community in this area. The programme of action would also seek to leverage existing efforts and initiatives. A labelling system could be developed to endorse activities in line with the objectives. Other organizations could be invited to share their views (such as the International Telecommunication Union and the World Bank Cybersecurity Multi-Donor Trust Fund).

(iii) Further develop the framework as appropriate to address new threats and further enhance security in cyberspace. This development could be through yearly meetings and/or review conferences to the programme of action, which would allow the adoption of new norms on the basis of consensus.

(iv) Foster multi-stakeholder cooperation in relevant areas: it has been confirmed that strengthening of cooperation (when appropriate) with civil society, the private sector, academia and the technical community is valuable. The programme of action should draft modalities to enable stakeholders to attend formal sessions, deliver statements and provide inputs. A model exists, with the Convention on Certain Conventional Weapons. Other examples exist within the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and the Convention on Cluster Munitions.

The institutional structure would be the following:

(a) Regular meetings: these meetings could be held on a yearly basis (or at any optimal periodicity). These meetings could (i) discuss existing and emerging threats; (ii) consider the implementation of norms, rules and principles; (iii) discuss further how international law applies to the use of ICT and identify potential gaps; (iv) discuss the implementation of confidence-building measures; (v) identify priorities for capacity-building, also on the basis of voluntary reporting; and (vi) identify further actions needed and determine the programme of work for intersessional meetings. Yearly conferences could decide by consensus to create technical workstreams, open to all States and relevant stakeholders, that are focused on specific items. Participation by technical and legal experts would be encouraged;

(b) Intersessional meetings: these meetings would advance the programme of work agreed upon by yearly meetings. Their work could be structured in technical workstreams focused on specific items, in accordance with the priorities and areas of work identified in the yearly meetings;

(c) Review conferences: these conferences could be held every four years (or another periodicity) to consider whether the framework should be updated and to further develop it if relevant. A dedicated workstream may be created to deepen discussions on how international law applies to the use of ICTs and to assess whether gaps exist in the framework that may call for its further development.

4. Preparation and establishment

(a) Preparation: on the basis of General Assembly resolution 77/37, the elaboration of the programme of action could be organized via intersessional meetings and dedicated sessions of the working group in 2024 and 2025.

(b) Establishment: General Assembly resolution 77/37 noted an "international conference" as an option to establish the programme of action (as was done, for example, for the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects). If States decide it, such an international conference could be convened in 2025 to adopt the founding document of the programme of action, on the basis of the preparatory work done in the open-ended working group on the security of and in the use of information and communications technologies 2021–2025.

(c) This international conference should make decisions on the basis of consensus, at least on matters of substance. It should provide for participation by relevant stakeholders.

Canada

[Original: English]
[14 April 2023]

Context

The digital domain has, in recent years, shown negative trends that could potentially undermine international security and stability. These trends include the growing use of information and communications technologies (ICTs) for malicious purposes.

It is therefore imperative to address these potential threats by establishing a permanent basis on which to build and maintain international peace, security, cooperation and trust in the ICT environment, specifically through a programme of action on cyberissues.

A programme of action can be a key contributing factor as a permanent and inclusive venue within which States Members of the United Nations can specifically address, and further elaborate on, shared commitments to promote peace, protect the acquis of responsible behaviour and avoid conflict in cyberspace. The support of Canada for a programme of action also entails further development in transforming societies and economies and expanding opportunities for cooperation in the ICT environment.

In particular, Canada stresses that any new permanent mechanism is not intended to compete with what has come before it, nor with what currently exists, but rather represents the next evolution in United Nations cyberdiscussions, building on discussions and agreements to date.

Canada recalls its support of the previous 2021 consensus report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, and, in particular, the report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, which recommended that States consider proposals to advance practical work to implement our existing commitments.

Canada further recalls the substantive aspects of the mandate of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, along with General Assembly resolution 73/27, which welcomed the effective work of the 2010, 2013 and 2015 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, as relevant and guiding outcome documents to form the basis of the programme of action.

Objectives

The establishment of a United Nations programme of action on cyberissues to advance responsible State behaviour in the use of ICTs in the context of international security will support States' objectives in the following ways:

- Allow for the continuation of previous consensus work in the Group of Governmental Experts and Working Group to consider, implement and advance responsible State behaviour in cyberspace and further build upon this work.
- Provide for genuine stakeholder participation.
- Create a single, dedicated permanent forum for cyber, which will not require renewed iterations, under the auspices of the First Committee, where States bear primary responsibility in matters of international security.
- Ensure an inclusive body, in that it accommodates the interests of all United Nations States.
- Offer an action-oriented forum, in that it addresses the implementation of responsible State behaviour in cyberspace, seeks to advance confidence-building and promotes capacity-building to enhance States' abilities to implement the norms of responsible behaviour and international law.
- Address the needs of States to raise political awareness of cybersecurity issues domestically, anchored through a high-level conference and/or political declaration.
- Provide a forum for ongoing discussions around the future of the framework and its continued development in the face of emerging technologies and threats.

Scope and mandate

As a stable and permanent mechanism, the programme of action would provide States with the flexibility to both maintain the existing framework and develop it further as it evolves to address emerging and future threats.

With respect to threats, the programme of action could provide a platform for not only identifying potential threats, but also for agreeing on solutions and putting in place measures to mitigate those risks.

The programme of action could also build on existing work being done to operationalize the normative framework, for example the 11 agreed and General Assembly-endorsed Group of Governmental Experts norms, by making use of 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) and the norms implementation checklist of Singapore and the Office for Disarmament Affairs. For example, an early priority could be to encourage States to define, in a national capacity, what they consider to be critical infrastructure, which was an area of focus in the previous consensus report of the Group of Governmental Experts.

Moreover, the full inclusion of relevant stakeholders in a programme of action could help make progress on norm implementation and support States by promoting or assisting in regular self-reporting. The programme of action could build on implementation surveys already in existence in order to allow States to measure progress, as the implementation of norms will be a continuous process.

While norms are part of the international cybersecurity framework, greater understanding of how international law applies to cyberspace is equally important. With limited consensus or understanding of how it applies, the programme of action can encourage States to articulate their positions on international law. These can be collected, disseminated and discussed in order to build further common understandings in this area.

The programme of action could cement itself as a cooperative, multi-stakeholder model to help facilitate engagement with stakeholders, who in turn can assist in national and regional implementation efforts. The inclusion of relevant stakeholders in a dedicated forum would lend legitimacy and can shape an instrument that will reflect lived realities and address real threats.

A programme of action could establish regional engagement through cooperation with regional organizations to facilitate coordinated initiatives. The Office for Disarmament Affairs, through existing resources and voluntary contributions, should continue to collaborate with relevant regional organizations, such as the African Union, the European Union, the Organization of American States, the Organization for Security and Cooperation in Europe, the Pacific Islands Forum and the Regional Forum of the Association of Southeast Asian Nations, to convene further series of consultations. These would allow member States of these organizations to share views on emerging threats, norms, best practices, the application of international law, capacity-building and confidence-building measures once the programme of action is established in 2025 and afterwards.

The programme of action would provide a permanent mechanism for administering and evolving a directory of points of contact at the policy and technical levels. This directory, which is currently being finalized in the working group, could also eventually expand to include, on a voluntary basis, the contact information of other stakeholders in order to support more rapid crisis management when cyberincidents occur.

A programme of action should leverage existing investments in capacity-building and technical assistance as essential ingredients for the implementation of the objectives listed above, as well as to facilitate cooperation among States. This would allow it to serve as an overarching confidence-building measure in the field of ICT security.

The programme of action, based on needs identified by States themselves, would serve as a convening platform to match capacity-building need and resources. Provisions of concrete support for capacity-building will assist States' abilities to implement agreed norms, rules and principles. As a function, the programme of action could also integrate existing tools for States and stakeholders to share relevant capacity-building proposals, such as the UNIDIR Cyber Policy Portal.

As an action-oriented mechanism, the programme of action could cooperate with and leverage other capacity-building efforts underway through the Global Forum

on Cyber Expertise or through UNIDIR. These collective efforts would help countries articulate and receive needed capacity-building.

Structure

As set out in the previous paper[4] by Canada on a programme of action, important lessons can be learned from the set-up of other programmes of action and from a number of recommendations on how to make the programme of action a consultative and inclusive process. The establishment of a United Nations programme of action should, in the view of Canada, be structured and developed in the manner laid out below.

It is important to note that, once established, the programme of action will not act as a treaty process, but as a political mechanism – intended to work by unanimous consent – for encouraging voluntary cooperation on promoting responsible State behaviour in cyberspace.

The Office for Disarmament Affairs can serve as the secretariat of the international conference and can act as the secretariat of the programme of action. In addition to preparing the annual meetings and review conferences, the Office would also be in charge of administering the global point of contact directory.

Periodic reviews on the progress made in the implementation of the programme of action, as well as the programme's future work priorities, should be undertaken on a biannual basis. This should be done in order to keep pace with the speed of cyberdevelopments.

As a permanent process, the programme of action should not focus only on producing reports and outcomes. Instead, it must show sustained and measurable progress. A programme of action on cyberissues could fill the current accountability gap between existing norms and actual practice by solidifying commitments and introducing or leveraging existing reporting or review mechanisms. It will be crucial to incentivize reporting practices by making use of the information they contain or by offering opportunities to discuss them, such as in mandated meetings.

A minimum of two thematic meetings a year should take place in order to focus on areas to help drive collaboration and advance cyberissues.

Proposed working groups could address emerging threats, norms and best practices, the application of international law, capacity-building and confidence-building measures.

Representatives in these working groups could meet at least once a year to track their progress on implementing the programme of action and recalibrate efforts as needed. These meetings should be geared towards an outcome document containing conclusions that, if unanimously agreed, are politically (though not legally) binding for all participants in the programme of action.

Decisions on substantive issues should be adopted by consensus.

Proposed next steps

The report of the Secretary-General containing recommendations to the General Assembly should be presented with a view to a decision being made by the Assembly at its seventy-eighth session on the structure and content of the programme of action and the preparatory work for its establishment.

[4] Available at https://documents.unoda.org/wp-content/uploads/2022/07/OEWG-Portal-Cover-Letter-Submission-Cyber-PoA-Research-paper.pdf.

No later than August 2024, an international conference should be convened. It should include relevant international and regional organizations, as well as relevant non-governmental organizations, civil society organizations, academic institutions, the private sector and the technical community.

The purpose of the international conference would not be to duplicate the work of the working group. Rather, it would focus specifically on the modalities and substance of a programme of action, including the finalizing and adoption of a political declaration. This declaration would elaborate the key elements of a programme of action, a programme of future work and a set of priorities for the work of the programme of action, in accordance with the scope of the programme of action, as mandated in General Assembly resolution 77/37.

The programme of action would not begin to meet until the end of the working group 2021–2025 and would take the final report of the working group, should it be agreed by consensus, into account in its work. The sessions that take place in the programme of action, once it is established, will also take into account the consensus reports contained in documents A/65/201, A/68/98, A/70/174, A/75/816 and A/76/135, the 2023 annual progress report of the working group and any future annual progress reports.

Modalities

Given the nature of the cybersecurity field and the diffuse ownership of key cyberinfrastructure and services, stakeholders will have an important role to play in implementing a programme of action on cyberissues.

In consultation with the Office for Disarmament Affairs, a list of representatives of other relevant non-governmental organizations, civil society organizations, academic institutions and the private sector, including those with expertise in the field of cybersecurity, will be drawn and presented for consideration of who may participate in the preparatory sessions, the international conference and the sessions of the programme of action.

The stakeholder modalities of the programme of action should be based on 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 order to enable the broadest possible level of participation from civil society, the private sector and other relevant stakeholders.

The programme of action should aim to be gender-sensitive and inclusive, and, as a future instrument, should find ways to reinforce human-centric approaches to international peace and security in cyberspace.

Chile

[Original: English]
[14 April 2023]

Scope

The scope of the programme of action would be matters related to the use of information and communications technologies (ICTs) in the context of international security. The programme of action would be aimed at advancing responsible State behaviour in the use of ICTs and strengthening international security and stability in the cyberdomain through actionable proposals and enhanced support for tailored capacity-building efforts.

The programme of action should seek in particular to (a) achieve cooperation, in terms of reducing tensions, preventing conflicts and promoting the use of ICTs for peaceful purposes through a cooperative approach in dealing with cyberthreats, as well as inclusive dialogue among States and with relevant stakeholders; and (b) advance stability in cyberspace by supporting the implementation, and further development, if appropriate, of the framework for responsible State behaviour based on international law, including international humanitarian law and human rights, norms of responsible State behaviour, confidence-building measures and capacity-building.

The programme of action should support relevant capacity-building activities related to the implementation of the framework, taking into account and building on existing initiatives in this field. In that sense, the programme of action should be inclusive of both States and non-governmental stakeholders.

Structure and content

The programme of action could be based on a political document that would recall existing and emerging threats to international security related to the malicious uses of ICTs, building notably on the threat assessments contained in reports of the Group of Governmental Experts and the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, and reaffirm States' commitment to the framework for responsible State behaviour, agreed in successive reports of the Group of Governmental Experts and the 2021 report of the Working Group, 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 and future consensus outcomes of the current working group will add to this framework, which is cumulative and evolving. The political document would also establish a permanent institutional mechanism to advance the implementation of this framework (including by supporting States' capacities to do so), further develop the framework as appropriate and foster multi-stakeholder cooperation in relevant areas.

The programme of action could hold yearly formal meetings (with review conferences), with technical working groups meeting in the intersessional period (the technical working groups would be inclusive and enable the broad participation of all States that wish to join). The yearly meetings would adopt decisions and recommendations by consensus, based on the work conducted in the intersessional period by technical working groups dedicated to specific issues. The programme of action would encourage voluntary reporting of national implementation efforts, and programme of action meetings would be able to adopt, and regularly update, actionable recommendations for national implementation efforts. The programme of action would support capacity-building efforts in relation to the implementation of the framework and seek to enhance multi-stakeholder cooperation in this area and coordination with other relevant initiatives.

Preparatory work and modalities for the establishment of a programme of action

With respect to the preparatory work and modalities for the establishment of a programme of action, intersessional meetings and dedicated sessions of the working group should be organized in 2024 and 2025 to continue elaborating the different aspects of the programme of action. An international conference could be convened in 2025 or 2026 to adopt the founding document of the programme of action, based on the preparatory work done, including in the working group. This international conference should provide for participation by relevant stakeholders.

Colombia

[Original: Spanish]
[14 April 2023]

I have the honour to refer to General Assembly resolution 77/37, entitled "Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security." Pursuant to paragraph 3 of the aforementioned resolution, the point of view of Colombia on the scope, structure and content of the programme of action is set out below.

Scope

In accordance with General Assembly resolution 77/37, the purpose of the programme of action would be to establish a United Nations programme of action to advance responsible State behaviour in the use of information and communications technology (ICT) in the context of international security.

The programme of action would be voluntary in nature and based on States' political commitments. It would be:

(a) Permanent: with an indefinite term, but having periodic review mechanisms;

(b) Inclusive: the participation of all States and relevant multiple stakeholders would be ensured;

(c) Transparent: it would support the implementation and strengthening of confidence-building measures, and allow States to report on their related actions;

(d) Flexible: its content and implementing actions could be updated, bearing in mind the evolving nature of cyberspace and growing threats and challenges;

(e) Action-oriented: it would enable the identification and implementation of actions aimed at promoting responsible behaviour at the national, regional and global levels.

Content

The programme of action could bring together, in a single document, the recommendations of the Open-ended Working Group and the previous work of the Group of Governmental Experts, which the United Nations had agreed upon and endorsed.

In this regard, the programme of action should serve to advance and build on the work already done in these forums, and actions should be set out therein with reference to the framework for responsible State behaviour in the use of ICT (each action should correspond to a norm of responsible behaviour).

The issues addressed in the programme of action would be based on the themes dealt with by the Open-ended Working Group, set out in General Assembly resolution 75/240, and the provisions of General Assembly resolution 77/37. It is particularly important to monitor compliance with agreed norms, rules and principles, and to allow for the development of future regulatory frameworks, in the light of the changing and evolving nature of cyberspace.

In addition, it is essential that the programme of action include capacity-building exercises to assist States in their efforts to address existing and emerging challenges in the area of ICT. This is important as capacity-building, and assistance and cooperation to that end, are fundamental to enabling States to engage in responsible behaviour in cyberspace and to addressing the challenges that have been

identified. With respect to those two aspects, the programme of action should be sufficiently flexible as to allow for the incorporation in its content of issues that are identified as it develops.

With a view to the effective implementation of the programme of action, a follow-up mechanism should also be established thereunder to review achievements and challenges. Such a mechanism would also serve as a platform for sharing best practices and recommendations on application at the national and regional levels. As such, it would undoubtedly play a key role in capacity-building and cooperation, which must be a fundamental pillar of the programme of action.

Structure

In terms of structure, national, regional and global actions that are coherent and properly coordinated can be set out in the programme of action. The implementation of national provisions is most important, since these determine how effectively a State can properly apply the norms of responsible behaviour and address potential threats arising from the malicious use of ICT.

Annual reports could be prepared as a means of monitoring national-level actions, as well as achievements and challenges related to their implementation. These would preferably take the format of a survey, which would facilitate completion by States and allow information to be systematized and analysed in a simple, practical and timely manner.

In order to develop the actions to be embodied in the programme of action at the national and regional levels, a diagnosis of capacity-building needs, supply, common challenges and good practices could be prepared so that the programme responds to the multiplicity of realities faced by participating States.

The programme of action could be integrated with and provide follow up to the capacity-building action plan for the establishment of the global directory of points of contact, thus creating synergies and avoiding duplication of effort.

With respect to organizational functioning, a review and follow-up mechanism would be established under the programme of action, whereby States would hold periodic meetings to review the programme and its implementation (including achievements and challenges) and, if necessary, update and adjust its content.

As part of the programme of action, Member States could form technical working groups to discuss the issues that it would address and the measures that would advance its implementation. In this way the instrument would be guided by constructive institutional dialogue, while remaining operational and action-oriented.

Civil society and various stakeholders could participate in an advisory capacity in the technical working groups, sharing their valuable knowledge and different perspectives. Civil society also has a fundamental role in capacity-building, the identification of existing and potential threats and, of course, in the practical application of the norms of responsible behaviour in the use of ICT.

Bearing in mind that the programme of action would be based on the work of the Open-ended Working Groups, as well as the reports of the group of governmental experts, the sessions of the Working Group which are to take place through 2025 are the ideal multilateral space for further developing its content.

Cuba

[Original: Spanish]
[24 March 2023]

Developments in information and communications technology (ICT) are having an increasing impact in all areas of society.

Significant risks arise from the misuse of ICT and media platforms, including social media and radio broadcasts. These risks include the use of such platforms for interventionism, through the promotion of hate speech, incitement to violence, subversion, destabilization, the dissemination of fake news and the misrepresentation of reality for political purposes; the proliferation of cyberattacks; and the growing militarization of cyberspace.

We reject the use of ICT with the aim of turning cyberspace into a military theatre of operations, and the attempts, in that context, to legitimize the punitive unilateral use of force, including the application of unilateral coercive measures, and even military actions.

Our country promotes, as a fundamental principle of international relations in the realm of cybersecurity, the joint cooperation of States to prevent and address the covert and illegal use, by individuals, organizations and States, of the ICT systems of other nations, and to prevent cyberspace from becoming a military theatre of operations.

There is a need for the General Assembly to adopt, without further delay, 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 through international cooperation.

However, we believe that, no matter how well intentioned, the proposal to establish a programme of action to advance responsible State behaviour in the use of ICT in the context of international security – as long as the focus is only on non-binding commitments – would have the harmful effect of further reducing the likelihood of adopting legally binding obligations, which Cuba considers the only truly effective way to ensure responsible State behaviour in cyberspace.

The mandate of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 includes reviewing proposals made by States. Any cybersecurity initiative, including a programme of action, should be discussed in this forum.

It is the responsibility of this Group to recommend the most appropriate courses of future action, on the basis of consensus decisions by Member States. We do not support the establishment of parallel, duplicate or substitute mechanisms, but rather mechanisms that result from the work of the Open-ended Working Group.

The proposal to establish a programme of action would require further discussion among States in the Open-ended Working Group. The results of the discussion in the Open-ended Working Group, and the recommendations that the Group will submit to the General Assembly, should not be prejudged.

We strongly support the objective of ensuring responsible State behaviour in the use of ICT in the context of international security, but we do not support the establishment of mechanisms that are parallel to, or substitutes for, the Open-ended Working Group. It is our responsibility to make proper use of the limited financial resources at our disposal and to avoid the proliferation of parallel processes and

meetings, with the attendant difficulties in ensuring participation, which particularly affect the smallest delegations, those of developing countries.

The role of the Open-ended Working Group to engage in regular institutional dialogue on ICT security and use should be respected and preserved. We advocate the continuation of the work in this format, so that it can yield results that all States agree upon.

With respect to its scope, elements that do not meet with consensus must not be included, as they would jeopardize any future outcome.

A possible programme of action should include practical measures for international cooperation, which is a priority for developing countries. We reject the imposition of unilateral coercive measures that hinder assistance, cooperation and technology transfer.

We would like to draw attention to the participation of regional organizations in the development of this initiative. While we recognize the contribution they can make, we would not be able to accept proposals made by exclusive regional organizations which do not represent all the countries of a region. The intergovernmental nature of the process must remain paramount.

Czechia

[Original: English]
[14 April 2023]

Czechia appreciates discussions on cybersecurity within the First Committee. It especially values the progress made in this area by both the working group and the Group of Governmental Experts, whose aim is to contribute to the strengthening of a stable and peaceful information and communications technology (ICT) environment and thus to international peace and security. As part of the work of these groups, a whole range of ICT issues were identified that States need to address in an international security context.

Based on our analysis of the work of the Group of Governmental Experts and the Working Group to date, we believe that the proposed programme of action represents an appropriate way of systematically addressing discussions on the use of ICTs in the international context and efficiently continuing our work started in the format of the Governmental Group of Experts and the Working Group. Moreover, a permanent and inclusive United Nations body would allow the international community to set more ambitious goals, support their implementation worldwide and periodically monitor their progress. Therefore, Czechia supports the proposal to establish the programme of action and is one of its main co-sponsors.

In this context, we would like to contribute to the discussion regarding the scope, structure and content of the programme of action with the following points:

Stability

In our opinion, the programme of action would bring institutional stability to the international debate regarding ICTs. The programme of action would represent a permanent institutional framework underpinning all cyber-related debates within the United Nations.

- Periodically recurring discussions about the establishment of a new working group dedicated to the use of ICTs would thus be avoided.

- At the same time, the risk of polarization and fragmentation of the ICTs discussion, as witnessed in the past, due to the unfortunate parallel existence of the Group of Governmental Experts and the Working Group, would be eliminated.

Inclusiveness, public-private cooperation

States are the ones who bear the main responsibility for international security. Only they can take decisions. Participation in the programme of action should therefore be open to all States. Decisions within the programme of action framework should be based on consensus.

In addition, Czechia supports the opening of programme of action discussions to stakeholders as well. Stakeholders should be allowed to access programme of action working groups, make statements and submit written inputs.

- Engaging the private sector, academia and civil society would bring valuable expertise on matters such as threat assessment, norms implementation including measurement of progress made, etc.
- Private sector could also contribute to cybercapacity-building efforts.

Implementation of normative framework

Czechia believes that States should prioritize the implementation of the existing normative framework (endorsed by General Assembly resolution 76/19, adopted by consensus) rather than replacing it by a new instrument. The programme of action should thus place a strong focus on supporting the implementation of existing international law and norms of responsible State behaviour.

However, given the unique nature of ICTs, it may be necessary to develop new norms in the future. Therefore, the programme of action should be established as a flexible instrument that can address both the implementation of the existing norms and the potential development of new norms in the future.

Deepen understanding of how international law applies to cyberspace

Norms are but one part of the international cybersecurity framework that States need to comply with. As was stated in final reports of the Group of Governmental Experts and the first Working Group, as well as in the annual progress report of the current working group, international law is applicable and essential to maintaining peace, security and stability in the ICT environment. The programme of action should therefore build on this and could serve as a platform to further develop a common understanding of how international law applies to cyberspace.

- The programme of action should encourage States to present their positions on how international law applies to cyberspace and build a common understanding in this area.
- The programme of action could also leverage existing multi-stakeholder processes in this area to organize discussions on specific topics as a part of its mandate that could contribute to the practical application of a theoretical framework.

Support for cybercapacity-building

For Czechia, cybercapacity-building is a major priority since it helps to improve our collective global resilience against malicious cyberactivities. In other words, we recognize the important function that cybercapacity-building plays in global development, consequently also empowering all States to effectively participate in both technical and policy discussions on cybersecurity in global forums.

- The programme of action would be an important platform for the exchange of views and ideas on cybercapacity-building and would promote relevant activities to support States in implementing the normative framework.
- The programme of action would structure cybercapacity-building initiatives by coordinating donor efforts and mapping the needs of recipient countries.
- Establishing the programme of action also gives us the possibility to explore the creation of a dedicated multi-donor fund, which could support activities dedicated to the promotion of the framework for responsible State behaviour.
- Coordination with cybercapacity-building activities undertaken in other venues such as the International Telecommunication Union could be explored.

Structure

With regard to the specific modalities, Czechia favours the idea of annual or biennial 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 decision to establish or terminate a working group would be taken in plenary by consensus.
- Working groups would be open to all Member States and to stakeholders.
- Working groups established for different issues would not meet in parallel, to ensure broad participation and engagement.
- Working groups would be required to submit their progress reports.
- Working groups would not have to be held in New York only, but also – depending on the specific topic – in Geneva, for example.

Establishment

Last but not least, we would like to highlight that the programme of action would in no way duplicate the work of the current open-ended working group on security of and in the use of information and communications technologies 2021–2025.

- The programme of action would be established after the end of the current working group in 2025 and would continuously build on the work of the working group.
- It would be the current working group within which States would lead a discussion on the final form of the programme of action, including all the necessary modalities. Dedicated sessions of the working group should be organized in 2024 and 2025 to continue elaborating the different aspects of the programme of action, including its founding document.
- Regarding the establishment of the programme of action itself: according to Czechia, a feasible way is indicated in General Assembly resolution 77/37 on the establishment of the programme of action, namely, through an international conference, with the assumption that it would adopt the founding document prepared by the working group.

Denmark

[Original: English]
[13 April 2023]

Since 2003, several United Nations working groups discussed the establishment of a "regular institutional dialogue" on issues of information and communications technologies (ICTs) and international security.

This institutional dialogue should focus on supporting the implementation of the normative framework, as was also made clear by the 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".[5]

The programme of action would provide a permanent and institutional mechanism for follow-up on the implementation of agreed norms, provide and regularly update recommendations and support or promote capacity-building projects of relevance. At the same time, the programme of action would be flexible and allow further development of the framework, if appropriate.

The scope of the programme of action would be issues related to the use of ICTs in the context of international security. The primary objective would be to contribute to international peace and security by preserving an open, free, stable, secure, accessible and peaceful ICT environment.

The programme of action could be based on a political document which would

(a) reaffirm the commitment of States to the framework for responsible State behaviour;

(b) establish a permanent institutional mechanism to advance implementation of this framework and seek multi-stakeholder cooperation, as relevant.

The programme of action could hold formal meetings once a year and allow for technical working groups to meet in the intersessional period.

The yearly meetings would adopt decisions and recommendations by consensus, on the basis of the work conducted in the intersessional period by technical working groups dedicated to specific issues.

The programme of action would allow States to voluntarily report on the national implementation of the framework for responsible State behaviour through new or existing mechanisms to identify priorities for norms implementation.

At the meetings of the programme of action, it would be possible to adopt and update recommendations for national implementation efforts. Working groups could be created with a view to advancing implementation of specific aspects of the framework.

The programme of action would support capacity-building related to the implementation of the framework and seek to enhance multi-stakeholder cooperation and coordination with other relevant initiatives.

The value of collaboration with stakeholders such as civil society, the private sector, academia and the technical community was emphasized by the Working Group, which concluded that stakeholders themselves "have a responsibility to use ICTs in a manner that does not endanger peace and security".[6] Private stakeholders

[5] A/75/816, para. 74.
[6] Ibid., para. 10.

also contribute to capacity-building efforts, and cooperation with stakeholders can be essential for States in order to implement their commitments under the framework.

Modalities for the meetings of the programme of action and working groups should consequently enable stakeholders to attend formal sessions, deliver statements and provide their valuable input.

On the preparatory work and the establishment of the programme of action, intersessional meetings and dedicated sessions of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 should be organized in 2024 and 2025 to continue elaborating the different aspects of the programme of action.

Furthermore, General Assembly resolution 77/37 included the option of an international conference to establish the programme of action. A conference could be convened in 2025 or 2026 to adopt the founding document of the programme of action on the basis of the preparatory work done up to this point, including in the working group. Participation by relevant stakeholders should be provided for at this conference.

Ecuador

[Original: Spanish]
[14 April 2023]

Ecuador values and supports the recommendations and conclusions of the groups of experts and the open-ended working groups, which are also reflected in the resolutions of the General Assembly on developments in and use of information and telecommunications in the context of international security.

Ecuador believes that a regular institutional dialogue should be established to address issues related to the use of information and communications technology (ICT) in the context of international security, and that such a dialogue should be action-oriented, inclusive, transparent and results-based and build on the previous discussions of the groups of experts and working groups on the topic.

In this context, Ecuador considers that the establishment of a programme of action would provide a permanent and institutional mechanism to follow up on the implementation of existing voluntary norms. It would serve to provide and periodically update relevant recommendations on responsible State behaviour; promote relevant international cooperation projects, capacity-building and confidence-building measures; and study the development of new norms and a potential legally binding instrument on the subject, if appropriate.

Similarly, Ecuador considers that the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 can be the primary forum for further consideration and development of the programme of action, with a view to its future establishment.

With the programme of action, we are seeking to contribute to the maintenance of international peace and security by preserving an open, stable, safe, accessible and peaceful digital environment conducive to bridging digital and gender divides, and to take measures to address emerging threats and challenges in cyberspace through dialogue and consensus among States, as well as with relevant stakeholders.

Ecuador firmly believes that States bear the primary responsibility for the maintenance of international peace and security and, therefore, they must retain a central role under the programme of action by being responsible for decision-making and the negotiation of outcome documents. However, Ecuador values and encourages the participation and input, where appropriate, of civil society, the private sector,

academia and the technical community in these deliberations. These actors play a fundamental role in ensuring that the use of ICT does not jeopardize global peace and security.

As a follow-up mechanism, the programme of action should be reviewed on an ongoing basis at annual meetings. New technical working groups could also be created at such meetings to address emerging issues or new priorities.

We value the work already undertaken to establish norms of responsible behaviour; we are not starting from scratch. At the same time, we do not see the programme of action as an end in itself, but as a milestone that will facilitate further progress towards a more robust international cybersecurity architecture.

Egypt

[Original: English]
[11 April 2023]

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 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 the 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 on Developments in the Field of Information and Telecommunications in the Context of International Security, as well as those of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security,[7] thereby establishing a cumulative and evolving framework for responsible State behaviour in the use of information and communications technologies, elaborated by these processes.

3. Member States have been called upon to be guided in their use of ICT by the 2010, 2013, 2015 and 2021 reports of the Governmental Groups of Experts and the 2021 report of the Working Group. Moreover, this 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 of 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. The proposed programme of action aims at building on the acquis and the existing framework that has been endorsed by the General Assembly by consensus.

6. The proposed programme of action does not in any way undermine the deliberations of the ongoing open-ended working group on security of and in the use of information and communications technologies 2021–2025, as it would be established following the conclusion of the mandate of the working group in 2025. In addition, it would avoid any duplication of efforts or the creation of parallel tracks. It

[7] See A/65/201, A/68/98, A/70/174, A/75/816 and A/76/135.

would represent a one-stop shop under the auspices of the United Nations, addressing issues related to the 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 by focusing on following up on the implementation of the framework with an action-oriented approach.

II. Objectives and scope of the programme of action

7. To serve as a regular institutional dialogue platform that would allow the participation of all States in a permanent, inclusive, transparent, action-oriented, results-based and consensus-driven process that builds on the existing framework through following up on the latter's implementation, identifying the gaps, tailoring capacity-building programmes and promoting international cooperation and transparency.

8. To function as an action-oriented platform under the auspices of the United Nations that is aimed at:

(a) Periodically assessing the implementation of the agreed framework by Member States through reviewing their voluntary national implementation reports, which could follow an agreed harmonized reporting template.

(b) 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, including through new norms, rules and principles, as well as legally binding obligations, thereby advancing the implementation of the agreed framework.

(c) Taking practical steps to promote international cooperation and periodically assessing whether additional actions are needed to respond to current and emerging challenges, taking into account the rapidly evolving ICT environment.

(d) Elaborating concrete guidance to support Member States in their implementation of the agreed norms, rules and principles.

(e) Exchanging information on best practices that can be implemented at the national, regional and international levels (including the legislative and administrative frameworks and measures taken towards protecting critical infrastructure).

(f) Facilitating direct communication between national focal points through a dedicated global directory (which could benefit from or rely on the establishment of the points of contact directory on security in the use of ICTs (if decided by States)).

(g) Creating a portal for States that contains modules on facilitating communications among national focal points, including on incident reporting, repository of documents and assistance mapping (the Indian cyberportal proposal). Moreover, the portal would, as appropriate, allow engagement with relevant stakeholders for the sharing of their relevant positions and proposals.

(h) 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 under the programme of action could be envisaged, including the possibility of relying on existing or new instruments, such as the World Bank Cybersecurity Multi-donor Trust Fund.

(i) Preventing conflicts arising from the use of ICTs and seeking the settlement of relevant disputes by peaceful means.

(j) Promoting the use of ICTs for peaceful purposes.

(k) Coordinating with other relevant regional initiatives as appropriate.

III. The establishment of the programme of action

9. The views and contributions submitted by Member States in the framework of the ongoing working group on the programme of action proposal and the report of the Secretary-General pursuant to General Assembly resolution 77/37, as well as the relevant possible recommendations contained in the reports of the working group, shall represent the basis for the establishment of the programme of action in terms of its scope, structure and modalities.

10. States should continue its active participation in the ongoing working group established pursuant to General Assembly resolution 75/240 with a view to reaching consensus reports, including recommendations on the establishment of the programme of action.

11. The programme of action should be further elaborated and developed within the current 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.

12. The programme of action would be established after the conclusion of the current working group's mandate in 2025 through a consensual General Assembly resolution based on inclusive and transparent consultations and preparations. The option of convening a dedicated conference on the establishment of the programme of action depends on the views of Member States and the assessment of the Secretary-General on whether such a conference is deemed necessary. Member States may agree within the ongoing working group to establish the programme of action, including its suggested modalities, through a political declaration that could be endorsed in a General Assembly resolution.

IV. Structure and possible modalities

Periodic meetings

13. The 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 programme of action, 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.

14. The programme of action 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.

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

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

Reports

17. Under the programme of action, 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.

18. 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

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

Secretariat

20. The Office for Disarmament Affairs should provide secretariat services for the programme of action.

Participation of stakeholders

21. The programme of action is an intergovernmental process in which negotiation and decision-making are exclusive prerogatives of Member States.

22. The programme of action will be committed to engaging with the relevant stakeholders in a systematic, sustained and substantive manner.

23. Relevant non-governmental organizations in consultative status with the Economic and Social Council in accordance with its resolution 1996/31 would inform the secretariat of their interest in participating in the work of the programme of action.

24. Other interested non-governmental organizations relevant and competent to the scope and purpose of the programme of action 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 programme of action. These organizations would accordingly be invited to participate, on a non-objection basis, as observers in the formal sessions of the programme of action.

25. 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.

26. Where there is an objection to a non-governmental organization, the objecting Member State will make known its objection to the Chair of the programme of action 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.

27. The Chair will organize informal consultative meetings with stakeholders during the intersessional period.

28. The programme of action may facilitate coordination with the relevant regional and subregional initiatives, including through their possible participation and contributions.

El Salvador

[Original: Spanish]
[15 April 2023]

Introduction

It is increasingly interesting to witness the growing importance that most States Members of the United Nations are attaching to what happens in cyberspace, which must be seen against the backdrop of the responsibilities and rights of States under international law and the Charter of the United Nations.[8]

The increasing reliance on information and communications technology (ICT), and the capabilities that can be developed in cyberspace, can influence the internal affairs of other States and seriously threaten peace and security.

It is important for all States Members of the United Nations to understand that what happens in cyberspace affects the processes of building and maintaining international peace and security; this knowledge will make them better prepared to address challenges, overcome obstacles and capitalize on opportunities.

Since work on this issue has been ongoing at the United Nations for some 25 years, and is evolving and cumulative, it is vital that future progress be based on the consensus outcomes that resulted from the reports of the groups of governmental experts and of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security[9] and the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025,[10] without prejudice to the outcomes reached by the Working Group whose mandate is due to end in 2025.

The reports of the 2010, 2013, 2015 and 2021 groups of governmental experts[11] provide the foundation for the framework of norms, rules and principles for responsible State behaviour in cyberspace.

Advances in discussions and States' shared understanding will increase adherence to consensus-based rules on the basis of political commitments, while progress continues towards the next natural stage in the development of the law, which is the establishment of legally binding norms to regulate State behaviour in cyberspace.

Objectives and scope

General

The programme of action should be consolidated as a regular action-oriented mechanism to monitor developments in ICT in the context of international security through the preservation of an open, stable, secure, accessible, affordable and peaceful ICT environment. Decision-making with regard to substantive matters should be consensus-based, in keeping with the practice that has been developed throughout this process.

Specific

It should serve as an institutional framework that can address the urgent needs of the international community in terms of international cooperation and assistance,

[8] See A/68/98, para. 19.
[9] See A/75/816.
[10] See General Assembly resolution 75/240, the mandate extends to 2025.
[11] See A/65/201, A/68/98, A/70/174 and A/76/135, respectively.

including financial and technical assistance, on more favourable terms, to support and facilitate national, regional and international efforts related to threats in the field of information security.

It should advance a shared understanding of the implementation of the existing framework for responsible State behaviour in cyberspace, which is based on the applicability of international law, actual and potential emerging threats, measures to build confidence in cyberspace and capacity-building.

It should create an enabling environment to further progress in reducing digital divides, particularly the gender digital divide, build digital resilience and maintain a human-centric approach.[12]

Structure

The programme of action could be based on a policy document endorsed by the General Assembly, with the objective of creating a permanent institutional mechanism. The provision of resources and technical expertise should be planned to promote the implementation of the programme of action.

To support the functioning of the mechanism, the United Nations Office for Disarmament Affairs should act as its secretariat.

Establishment

The national opinions and contributions of Member States, which are collated in the report of the Secretary-General pursuant to General Assembly resolution 77/37[13] and the consensus outcomes of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 should serve as the basis for defining the scope, structure and content of the programme of action.

Active involvement in the regular institutional dialogue of the Open-ended Working Group (2021–2025) can generate input to inform the establishment of the programme of action, which could be endorsed as an outcome of the Working Group, if such a decision is reached by consensus.

This process requires a vision to prevent duplication of effort.

In addition, broad informal consultations with Member States can serve to elicit additional input from those States which do not submit national opinions, by providing another forum for them to express their ideas, priorities and interests with respect to the establishment of the programme of action.

The establishment of points of contact to enable States to liaise on implementation-related matters would be useful for the operationalization of the programme of action. Once it is established, synergies with the global directory of points of contact initiative, part of the confidence-building measures of the Open-ended Working Group (2021–2025), could be considered.

The possibility of convening an international conference to review progress and implementation four years after the establishment of the programme of action may be considered.

Meetings of the States parties should be convened twice a year to consider the implementation of the programme of action at the national, regional and international levels. However, the focus should be on reviewing the implementation of practical

[12] General Assembly resolution 77/37.

[13] Ibid., para. 3.

measures, to avoid renegotiation of recurrent instruments, which serve declarative purposes. The programme of action should have a practical focus, based on strengthening capacity.

The convening of working groups during the intersessional period to assess progress in specific areas may be considered.

The creation of ongoing cybersecurity awareness-building programmes can be considered, as a cross-cutting objective of the programme of action.

Frequency of meetings

In order to advance in the implementation of the programme of action and verify compliance with the actions required thereunder, it would be appropriate to convene:

- State party review meetings every two years, with a practical focus.
- State party review conferences every four years, depending on the outcomes of the first review conference.

The above is suggested with a view to allowing sufficient time between sessions for delegations to prepare, and not overloading the agenda in the light of other, existing processes related to international security. Analysis should be carried out later to decide in which years the cycle of meetings should begin, with a view to ensuring that they do not coincide with other, already mandated, disarmament and international security processes.

The main objective of the follow-up meetings should be to update, if applicable, the practical national and regional implementation measures being taken under the programme of action.

Reports to the programme of action

Voluntary reporting will be encouraged under the programme of action; such reporting can be based on existing mechanisms, such as the survey on the implementation of the regulations on responsible behaviour of States in cyberspace of the United Nations Institute for Disarmament Research.

Additional reporting instruments should be chosen taking into account the need to avoid “reporting fatigue”, and complementarities with other existing instruments should be sought.

If new reporting tools are agreed by consensus, these should be user-friendly and accessible via an online platform, so that all delegations can create reports from which data are generated that serve to evaluate progress towards the objectives of the programme of action, as well as approaches to emerging needs in the ICT environment.

Participation of other stakeholders

As States bear the primary responsibility for the maintenance of international peace and security, the negotiation process will remain intergovernmental in nature.

However, in view of the private nature of the infrastructure of the Internet and the role that other relevant organizations play in the design and development of technological advances, it is important to take on board the contributions of civil society, non-governmental organizations, academia and industry. Such contributions should be made through a clear and defined mechanism under the programme of action, which should be agreed by consensus and taking into account the views of all Member States regarding the terms of participation of other stakeholders.

Estonia

[Original: English]
[14 April 2023]

As mandated by General Assembly resolution 77/37, Estonia would like to submit a national position on the programme of action

Over recent years, threats in the use of information and communications technologies (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 working group. Estonia would like to share the following remarks on the establishment of a regular institutional dialogue in the format of the programme of action. We believe that the programme of action would serve as a useful vehicle for continuing discussion to advance responsible State behaviour in the use of ICTs and thereby contribute to reducing tensions, preventing conflict and promoting their peaceful use.

1. **The programme of action should be based on the existing acquis and the framework of 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 Group 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 point 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 the 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 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 programme of action via an international conference, as proposed in General Assembly resolution 77/37. We would also like to underline that the programme of action mechanism should be founded on the principle of consensus. Estonia believes that the proposed programme of action framework would remove the need for the General 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 working group in an inclusive manner.** We welcome the increasing interest of Member States in contributing to various topics which are focused upon during the ongoing debates in the working group sessions. The current working group discussions 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. The programme of action should also include clear and transparent modalities for the substantial involvement of the multi-stakeholder community in order to further benefit from their expertise and knowledge.

4. **The format of the programme of action should allow for focused discussions.** Estonia suggests that the elements of the programme of action mechanism could be based on focused discussion held, for example, in working groups open to all interested participants, on subjects including, but not limited to, threats, capacity-building, confidence-building, norms and international law. Another option could be focusing these working groups on more thematic topics, such as critical infrastructure protection. With an increasing number of Member States reflecting their views, and in the light of an evolving threat landscape, the programme of action would allow for a more flexible yet focused format for continuing these discussions. Equally, we would like to underline that the design of the programme of action framework should also take into account the challenges regarding the limited capacities of small States and therefore be built on reasonable expectations regarding the projected workload. In that regard, we support the idea of annual conferences broadly addressing the State use of ICTs, supplemented with more focused working groups.

5. **The programme of action should offer an inclusive framework for 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. International law is currently evolving and Member States would benefit from a deepened understanding of and shared views on how existing rules apply, as well as 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.

6. **The programme of action should be action-oriented, with a strong focus on capacity-building.** An integral part of the future discussions should be the implementation of the agreed-upon framework of responsible State behaviour. This can be supported by a practical and transparent approach to mapping as well as through responding to the need for and requests for capacity-building. The programme of action should take stock of existing capacity-building initiatives in a well-coordinated and complementary manner. For example, design of the programme of action should take note of existing mapping exercises and resources, such as the Cybil Portal and the CyberNet mapping of the cybercapacity-building projects of European Union member States.

Finland

[Original: English]
[13 April 2023]

I. Introduction: general rationale for the programme of action

Finland shares the concern of many Member States over malicious and harmful cyberoperations that pose a threat to international peace and security.

Finland welcomes the progress made by the previous and current working groups and the Groups of Governmental Experts through producing important assessments and recommendations, and, in particular, by affirming the applicability of international law to cyberspace and elaborating a framework for responsible State behaviour in the use of information and communications technologies, endorsed by the General Assembly by consensus in resolutions 70/237 and 76/19, namely.

As captured in the final report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Member States have "concluded that any future mechanism for regular institutional dialogue under the auspices of the United Nations should be an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven and results-based".[14] States have also underlined the "utility of exploring mechanisms dedicated to following up on the implementation of the agreed norms".[15] The programme of action should therefore place a strong focus on supporting and following up on the implementation of the existing normative framework for responsible State behaviour in the use of ICTs.

Meanwhile, States have also observed that the normative framework is "cumulative and evolving" in nature, and that additional norms could be developed over time if any gaps in the existing framework are identified. Finland does not see any need for a new international binding instrument on the topic. However, while supporting the implementation of the existing agreed framework, the programme of action should allow for the potential further development of said framework, especially as new threats and challenges may arise.

In this context, the establishment of a programme of action would provide a permanent and institutional mechanism for follow-up on the implementation of the existing framework by providing and regularly updating sets of actionable recommendations and supporting or promoting relevant capacity-building projects. Meanwhile, the programme of action would be flexible, to enable the further development of the framework, if appropriate.

II. Scope and objectives

The overarching objective of the programme of action would be to contribute to the maintenance of international peace and security by preserving an open, stable, secure, accessible and peaceful ICT environment.

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

- Cooperation: to reduce tensions, prevent conflicts and promote the use of ICTs for peaceful purposes through a cooperative approach in dealing with cyberthreats and through inclusive dialogue among States and with relevant

[14] See A/75/816, para. 74.
[15] Ibid., para. 73.

stakeholders, including civil society, the private sector, academia, and the technical community.

- Stability: to advance stability in cyberspace by supporting the implementation and further development, if appropriate, of the framework for responsible State behaviour, based on international law, including international humanitarian law and human rights, norms of responsible State behaviour, confidence-building measures and capacity-building.
- Resilience: to contribute to the reduction of digital divides, especially the gender digital divide, and the strengthening of global resilience in relation to the implementation of the framework for responsible State behaviour.

III. Structure and content

The programme of action would serve as a permanent platform for regular institutional dialogue that would be inclusive of all States and relevant multi-stakeholders and would operate in a transparent and results-based manner through a consensus-driven process.

The establishment of the programme of action could reaffirm the political commitment of Member States to the framework for responsible State behaviour, provide a platform for the promotion of the implementation of this framework, further develop the framework if needed and foster multi-stakeholder cooperation.

The structure of the programme of action could be informed by other relevant examples, such as the Arms Trade Treaty, and hold yearly meetings to review the work of technical working groups that meet during the intersessional period.

The yearly meetings would adopt decisions and recommendations by consensus, on the basis of the work conducted in the intersessional period by technical working groups dedicated to specific issues, such as specific norms and the implementation of those norms and discussions regarding how international law applies to the use of ICTs.

The programme of action and its technical working groups would be inclusive and enable the broad participation of all States that wish to join. Participation from relevant governmental experts would be encouraged. Participation by relevant stakeholders would also be possible and encouraged (see below for modalities).

Yearly programme of action meetings could create new technical working groups to address emerging issues or new priorities.

Advancing the implementation of the framework

The programme of action would encourage voluntary reporting of national implementation efforts, either by creating its own reporting system or by promoting existing mechanisms, including 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. This reporting would serve as a basis for identifying priorities in the area of norms implementation and would map needs in terms of capacity-building.

The programme of action could adopt, and regularly update, actionable recommendations for national implementation efforts.

The programme of action would support capacity-building efforts in relation to the implementation of the framework and seek to enhance multi-stakeholder cooperation in this area and coordination with other relevant initiatives. Moreover, the programme of action would be a platform for the sharing of lessons learned and

experiences in capacity-building support, support for the mobilization of resources and the pairing of available resources with demand for capacity-building assistance.

The programme of action should also provide opportunities for strengthening complementarity between existing actors, processes and mechanisms, including at the international and regional levels, and should hold focused discussions with relevant representatives from relevant organizations.

Developing the framework, if appropriate

Yearly meetings or review conferences could adopt new norms, on the basis of consensus, if appropriate.

Multi-stakeholder involvement

"States bear primary responsibility for the maintenance of international peace and security"[16] and would therefore have the central and decision-making roles in the programme of action.

Meanwhile, the value of further strengthening collaboration with civil society, the private sector, academia and the technical community is critical for advancing responsible State behaviour in cyberspace. Previous working groups have repeatedly emphasized strengthening multi-stakeholder collaboration,[17] both because cooperation with these stakeholders is essential for States in implementing their commitments under the framework and because stakeholders themselves "have a responsibility to use ICTs in a manner that does not endanger peace and security".[18] Multi-stakeholders can also contribute to capacity-building efforts.

Modalities for the proceedings of programme of action meetings and working groups should therefore enable stakeholders to attend formal sessions, deliver statements and provide inputs, as is the case in other First Committee processes, such as the Meeting of Experts on Lethal Autonomous Weapons Systems of the Convention on Certain Conventional Weapons, where their expertise has proven to be useful.

IV. Preparatory work and modalities for the establishment of a programme of action

Preparatory work

The final reports of the Working Group and the Groups of Governmental Experts have recommended that the programme of action should be further elaborated, including at the process of the open-ended working group on security of and in the use of information and communications technologies 2021–2025. The annual progress report of the current working group also calls for focused discussions on the programme of action.

General Assembly resolution 77/37 also foresees that the Secretary-General's report on the programme of action should be submitted to the General Assembly and serve as a basis for further discussion within the working group.

Therefore, intersessional meetings and dedicated sessions of the working group should be organized in 2024 and 2025 for the continued elaboration of the different aspects of the programme of action, for the drafting of its founding document, and so on.

[16] Ibid., para. 10.
[17] Ibid., para. 22.
[18] Ibid., para. 10.

Establishment

General Assembly resolution 77/37 noted an "international conference" as an option for establishing the programme of action, as was done, for example, for the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects.

Such an international conference could be convened in 2025 or 2026 to adopt the founding document of the programme of action, on the basis of the preparatory work done, including in the working group.

This international conference should provide for participation by relevant stakeholders accredited with modalities close to those adopted in General Assembly resolution 75/282.

France

[Original: French]
[12 April 2023]

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, they have consolidated a framework for responsible State behaviour in the use of ICT, which the General Assembly has approved by consensus in several resolutions.[19]

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".[20] States also emphasized the "utility of exploring mechanisms dedicated to following up on the implementation of the agreed norms and rules".[21]

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.[22] 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.

[19] See General Assembly resolutions 70/237 and 76/19.
[20] A/75/816, annex I, para. 74.
[21] A/75/816, annex I, para. 73.
[22] General Assembly resolution 76/19, tenth preambular paragraph.

In this context, the establishment of 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.

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.

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.[23] 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 potential 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;[24]

(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 meetings, which could be held on an 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:

[23] 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 Open-ended Working Group 2021–2025. It should be borne in mind that the future consensus outcomes of the current Group will enrich this cumulative and evolving framework.

[24] See General Assembly resolution 77/37, second preambular paragraph.

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

Intersessional meetings would advance the work programme agreed upon at the annual meetings. These meetings could be structured around specific workstreams, in line with the priorities and areas of work identified at the annual meetings.

Review conferences 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 the 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, technical workstreams 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, a dedicated workstream could be established at the annual meeting. Work under the workstream would be carried out at the intersessional meetings of the programme of action, and any conclusions would be submitted to the next annual 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.[25] Initiatives or projects funded by this instrument should be in line with terms of

[25] https://disarmament.unoda.org/unscar/.

reference, which could be defined at the first meeting of the programme of action (promoting adherence to the framework, adhering to the guiding 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 (e.g. through the adoption of new norms) 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"[26] 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.[27] 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".[28] 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 Conventional Weapons Which May Be Deemed to Be Excessively Injurious or

[26] A/75/816, annex I, para. 10.
[27] A/75/816, annex I, para. 22.
[28] A/75/816, annex I, para. 10.

to Have Indiscriminate Effects.[29] 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 Open-ended Working Group 2021–2025 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 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 Open-ended Working Group 2021–2025. The Open-ended Working Group 2021–2025 also called for focused discussions on the programme of action in its 2022 progress report.

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 Open-ended Working Group 2021–2025. Many States have insisted that the Open-ended Working Group should be the primary forum for the development of the programme of action with a view to its future establishment.

Therefore, intersessional meetings and dedicated sessions of the Open-ended Working Group 2021–2025 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 potential establishment of the programme of action, including the option of a dedicated conference.

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 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). If States so decide, such an international conference could be convened in 2025 to adopt the founding document of the programme of action, on the basis of the preparatory work done by the Open-ended Working Group 2021–2025.

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).

[29] See rule 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).

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 programme of action.

Germany

[Original: English]
[31 March 2023]

A. Underlying principles of the programme of action

Germany supports the establishment of a programme of action as an action-oriented, permanent 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 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 working group after completion of its mandate.

Parallel processes or double structures need to be avoided, as this would exceed the capacity of many States to participate meaningfully. 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 working group with the ambition of finding consensus on the substance and modalities of the programme of action, which should be endorsed by all Member States 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:

- Cybercapacity-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 and leveraging synergies with mechanisms in other forums.
- Confidence-building measures, including the effective use of the future 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 shall constitute the permanent platform for advancing recurring items by facilitating 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 potential development of the international framework of responsible State behaviour in cyberspace shall 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 in order to address those areas where national implementation is lagging behind.

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 cybercapacity-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 to be established by the current working group. Beyond being a confidence-building measure in itself, the directory shall provide the basis for the implementation of other confidence-building measures, with the overall objective of reducing the risk of misunderstanding and conflict in cyberspace. By facilitating the implementation of dedicated confidence-building measures focusing, inter alia, on communication, particularly in times of crises, peer-to-peer exchange, the sharing of best practices, transparency measures, cooperation with the private sector or joint table-top exercises, the directory would constitute a central pillar of the programme of action, focusing on the implementation of the existing framework;

(c) 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;

(d) UNIDIR providing States with relevant monitoring and review instruments (e.g. norms implementation checklists) and conducting research activities related to the implementation of the framework;

(e) The possibility of additional meetings of technical workstreams in the intersessional period. Dedicated technical workstreams could focus, inter alia, on topics such as advancing cybercapacity-building, confidence-building measures, the application of international law and current and evolving 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, should take into account the capacities of States to participate meaningfully and should be decided by consensus at the annual meetings.

(f) Review conferences every four 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.

While States will retain the exclusive right to negotiate outcomes and make decisions within the programme of action, exchange with non-governmental stakeholders (multilateral and regional organizations, civil society, the private sector and academia) should be enhanced by providing opportunities for inclusive and meaningful 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 (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 annual meetings, review conferences and additional meetings of technical workstreams during the intersessional period. Furthermore, hybrid options of participation would 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 cybercapacity-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 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.

Italy

[Original: English]
[14 April 2023]

A. Introduction, motivations, scope and objectives

Italy is a staunch supporter of multilateralism and a strong advocate of United Nations processes and regular institutional dialogue on security of and in the use of information and communications technologies within the First Committee.

The work of the 2010, 2013, 2015 and 2021 Groups of Governmental Experts and that of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security have established the international framework that Italy has pledged to respect when adopting its posture on cyberspace. It has also contributed to shaping the national cyberarchitecture of Italy. Italy is committed to continuing to promote it at both the national and international levels.

As part of this vision, Italy actively participates in the current open-ended working group on security of and in the use of information and communications technologies 2021–2025, which will conclude its work in 2025, and supports the establishment of a programme of action as the best means of ensuring effective regular institutional dialogue, thus contributing to the further implementation of both the framework and the results of the current working group.

The programme of action should be a single permanent structure/platform/mechanism/forum for tackling cybersecurity issues at the global level, especially in the United Nations context. A lack of capacities at the national, regional and global levels is a challenge, and the programme of action should support national efforts to implement the normative framework and provide capacity-building to help bridge the digital divide.

As digitalization increases, so does the potential for instability in cyberspace. As we look towards the end of the mandate of the working group, it is high time to start discussions on the establishment of the programme of action in order to ensure that discussions continue beyond 2025 in a more structured and predictable manner.

B. Process

Duplication of efforts should be avoided; therefore, discussions on the goals, objectives, principles, structure, tasks, modalities and content of the programme of action should take place in the context of regular institutional dialogue within the current working group. References to the programme of action should be inserted in the upcoming annual progress report and the discussions on a 2024 and 2025 programme of work should begin at the earliest opportunity.

The report of the Secretary-General will be crucial for this process and – if needed – more time should be allowed for States to contribute, should the need arise. The possibility could also be considered of yearly technical resolutions to mark annual progress until 2025, when a political declaration to be agreed by the General Assembly should also be adopted. A specific conference could be convened in 2025, after the conclusion of the current working group, to advance the set-up of the programme of action and prepare the ground for the political declaration.

C. Principles, structure and content

For such an endeavour to succeed, and taking into account the speed at which information and communications technologies (ICTs) are evolving, the programme of

action needs to have sufficient flexibility in order to make it future-proof. Such characteristic should be reflected in the frequency at which its mechanisms are reviewed, as well as in the number of intersessional technical workstreams that could be established and/or terminated.

The working group has successfully brought the use of ICTs to the attention of the entire United Nations membership. Inclusivity should therefore be the cornerstone of the activities of the programme of action, both in terms of taking into account the capacities of all States and in terms of ensuring the participation of non-governmental entities in the debate. With respect to the former, cross-regional pairings, groupings and participation in the various workstreams should be encouraged and become one of the defining features of the programme of action. While the intergovernmental nature of the decision-making process of the programme of action is not in question, civil society and the private sector are essential players in cyberspace and a key ingredient of any successful regular institutional dialogue. Current working group arrangements are suboptimal and ways to improve the depth and frequency of multi-stakeholder consultations should be thoroughly explored, including by taking into account lessons learned from other processes.

Building upon the successes of past and present mechanisms and processes will be key to making the programme of action fit for purpose. The excellent work of the Office for Disarmament Affairs should continue as the secretariat of the programme of action. Similar words of appreciation are applicable to the United Nations Institute for Disarmament Research, which should continue to provide input in the context of the programme of action, not only in its capacity as a research institute, but also when applying its methodologies to analytical, monitoring and review capacities.

The work carried out by regional organizations in the field of cybersecurity is fundamental. This is becoming increasingly apparent with respect to current efforts to establish a global points of contact directory as a first enabling step towards increasing cooperation among States. Collaboration between the programme of action and regional and subregional organizations should be carefully considered in order to accelerate discussions on some topics, thus allowing for more time to dive deeper on other pressing issues. Mechanisms to avoid repetition of discussions and decisions that have already been taken at the regional level should be thoroughly explored in order to make the programme of action as action-oriented as possible.

Regularity and predictability of consultations among States and stakeholders are also key elements of a successful programme of action. One way of ensuring that could be to hold: (a) annual conferences in New York to discuss the implementation and possible evolution of the framework, as well as the work of technical workstreams; (b) a review conference focused on the assessment of the performance of the programme of action and its possible review every four years (with Geneva as a possible location); (c) technical/topic-specific workstreams, which would meet in a more regular/frequent manner, to be decided by consensus. In such formats, discussions could also take place in different geographic locations and/or in hybrid format, as long as recommendations stemming from such activities are validated on a yearly basis at least, during plenary meetings. Technical workstreams should primarily focus on the implementation of the acquis.

A biennial programme of work should provide visibility on the activities and topics to be tackled. It should be presented and approved at annual conferences, together with a report of the Chair on activities carried out the previous year. The Chair of the programme of action should be appointed for a three-year term of office with the possibility of a one-year extension. A six-month overlap in office with the incoming Chair would be advisable in order to ensure continuity of work and smooth transition arrangements.

The current lines of activity of the working group (existing and potential threats; international law; rules, norms and principles of responsible State behaviour; confidence-building measures; and capacity-building) should be continued within the programme of action, which should initially focus on implementing what has been consensually agreed in the past. Given the pace of technological developments and their implications, particular focus on threats is needed. An additional workstream dedicated to a voluntary peer review mechanism on the national implementation of the framework could be envisaged. Current reporting mechanisms/obligations could also be maintained with a view to developing more efficient and less time-consuming systems in the medium to long term. Finally, discussions on how international law applies in cyberspace are of crucial importance in order to further the understanding of States, influence their behaviour in cyberspace and increase the possibilities of mutual cooperation.

Cybercapacity-building support, which should constitute one of the most prominent features of the programme of action, should be provided upon request and on the basis of the principles outlined in document A/76/135. The programme of action could absorb any initiative currently being developed, provided that it helps to facilitate the analysis of cybercapacity-building offers, does not duplicate existing efforts, contributes to de-confliction and prevents "forum shopping". A dedicated funding mechanism should be explored, drawing on the experiences of existing instruments provided by regional organizations such as the European Union and/or specialized bodies, including the World Bank Cybersecurity Multi-donor Trust Fund or the Global Forum on Cyber Expertise.

Regarding participation in different workstreams and activities, mechanisms to ensure geographical balance and cross-regional collaboration should be promoted. One such mechanism could be a precondition that workstreams must be joined "in tandem", that is, a request to participate from a Member State must be submitted jointly with another Member State from a different geographic area. In addition, and conversely, a mediation support mechanism to assist Member States with resolving diametrically opposed positions should be explored. This could be provided by the United Nations or by developing a pool/roster of willing and able Member States. The initiative could constitute a spin-off of the confidence-building measures workstream.

Japan

[Original: English]
[14 April 2023]

1. Introduction

Japan supports the establishment of a programme of action to advance responsible State behaviour in cyberspace. 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 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 working group after completion of the latter's mandate. The programme of action will be established after the mandate of the ongoing 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.

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 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 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 programme of action on cyberissues, 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 efforts to implement the norms in each country.

The structure and modalities of the programme of action should include annual conferences to be held at the United Nations. The programme of action yearly conferences would be able to adopt, and regularly update, actionable recommendations for national implementation efforts. For example, a yearly conference 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, and so on.

To support further exchanges on this topic, the yearly conference may decide to create a dedicated workstreams that would take place in the intersessional meetings of the programme of action yearly conferences and that would submit their conclusions to the following yearly conference.

The global points of contact directory, to be established by the current 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 programme of action meetings, briefings could be delivered by representatives of other organizations (e.g. the 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 mechanisms (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 yearly programme of action conference 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.

4. Preparatory work and modalities for the establishment of a programme of action

Japan supports further focused discussions in the working group to further elaborate the programme of action.

Latvia

[Original: English]
[14 April 2023]

The framework of responsible State behaviour in the use of information and communications technologies (ICTs) for a long time – since 2003 – has been on the agenda of the First Committee and discussed at several working groups, which underscores the increasing importance of the responsible use of ICTs for maintaining international stability and security. As a means of advancing responsible State behaviour in the use of ICTs in a coherent and long-term approach, the establishment of a programme of action was proposed. General Assembly resolution 77/37 on the programme of action – a permanent, inclusive and action-oriented mechanism – received broad support from States. Therefore, further discussions on the scope, structure, content, preparatory work and modalities for the establishment of the programme of action should be conducted.

The establishment of the programme of action would create the first permanent institutional mechanism in the United Nations that would focus on the responsible use of ICTs in the context of international security. That would ensure institutional stability and regular dialogue on relevant issues, while at the same time preventing possible process fragmentation. All energy and resources should be focused on enhancing cooperation and trust among States, rather than on discussions regarding the modalities of a new mechanism every few years.

The idea to establish a "regular institutional dialogue" under the auspices of the United Nations is not new and has been discussed previously in the First Committee, as noted, for example, in the final report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.[30] The Working Group 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".[31] As noted in General Assembly resolution 77/37, the programme of action would "take into account the consensus outcomes adopted"[32] by the open-ended working group on security of and in the use of information and communications technologies 2021–2025.

Scope of the programme of action

The programme of action would be a permanent institutional mechanism in the First Committee and a platform for all States to participate in. The scope of the programme of action would be matters related to the use of ICTs in the context of international security. Its overarching objective would be to contribute to the strengthening of international peace and security and to promote conflict prevention.

Coordination and dialogue among States and with the relevant stakeholders can help to prevent conflicts, diminish misunderstandings and advance responsible State behaviour in the use of ICTs. As the cyberdomain has no borders and is ever-evolving, dialogue is therefore a vital element in dealing with existing and potential cyberthreats and challenges.

Stability and security in cyberspace would be advanced by supporting the implementation and further development, if appropriate,[33] of the framework for

[30] See A/75/816.
[31] Ibid., para. 74.
[32] General Assembly resolution 77/37, para. 2.
[33] General Assembly resolution 76/19, tenth preambular paragraph.

responsible State behaviour based on international law, including international humanitarian law and human rights, norms of responsible State behaviour, confidence-building measures and capacity-building activities.

In order to advance the implementation of the framework for responsible State behaviour, the programme of action would support relevant capacity-building activities. It is important to advance collective work on capacity-building, sharing our experience and best practices with States that need assistance in their efforts to build or strengthen their cyberdefences in order to improve global resilience against cyberthreats.

Structure and content of the programme of action

The programme of action, as a permanent institutional mechanism, would advance an implementation and further development, if appropriate, of the framework for responsible State behaviour. In order to achieve these objectives, the programme of action should support relevant capacity-building activities and encourage dialogue with stakeholders.

The programme of action could hold formal yearly meetings, and, between these meetings, work could be organized within technical working groups dedicated to specific issues related to the advancement of responsible State behaviour in the use of ICTs. For example, a technical working group could work to further enhance an understanding of how international law applies to the use of ICTs. The yearly meetings would adopt recommendations prepared by the technical working groups during the intersessional period.

These technical groups would be created and ended by a decision of the yearly meetings. The technical working groups would be inclusive and open to all States wishing to join, and efforts should be made to ensure that national experts could participate offline or online (hybrid format). Decisions made on the initial number of technical groups, the creation of additional technical groups and the frequency of their meetings should be made with consideration of all States' capacities and resources. Recommendations prepared by these technical groups should represent the views, interests and concerns of as many States as possible.

Coordination and dialogue with stakeholders – civil society, the private sector, academia and the technical community – would be encouraged, as their expertise in the ever-evolving cyberdomain is invaluable and their input is relevant in advancing responsible State behaviour and given that the stakeholders themselves "have a responsibility to use ICTs in a manner that does not endanger peace and security."[34]

Preparatory work and modalities for the establishment of the programme of action

We believe that the General Assembly has granted a strong mandate to proceed with the establishment of the programme of action. Further focused discussions on the scope, structure, content, preparatory work and modalities for the establishment of the programme of action are required. These discussions should be organized primarily within the open-ended working group on security of and in the use of information and communications technologies 2021–2025, as recommended in the final reports of the Working Group[35] and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.[36] Therefore, sufficient time should be dedicated to discussions on the

[34] See A/75/816, para. 10.
[35] Ibid., para. 77.
[36] See A/76/135, para. 97.

programme of action at the open-ended working group on security of and in the use of information and communications technologies 2021–2025 during remaining intersessional meetings and formal sessions. National contributions submitted pursuant to General Assembly resolution 77/37 should serve as a basis for further discussions on the development of the programme of action.

General Assembly resolution 77/37 noted an international conference[37] as an option for States to exchange views on the establishment of the programme of action. An international conference could be convened in 2025 or 2026 to adopt the founding document of the programme of action, building on the work and decisions made by consensus in the working group.

Monaco

[Original: French]
[14 April 2023]

The Principality of Monaco considers that discussions on how to reduce the risks of instability, escalation and damage to international security posed by the malicious use of information and communications technologies (ICTs) must continue within a single permanent institutional structure. This institutional structure would report to the First Committee of the General Assembly.

The increase in malicious activities in cyberspace, including attacks against critical State infrastructure, requires regular and sustained dialogue and cooperation. A programme of action to advance responsible State behaviour in the use of ICTs in the context of international security would be an appropriate platform for this. It would have the advantage of enabling regular exchanges in the short, medium and long term and of ensuring greater efficiency in its actions by avoiding discussions on launching working groups and their mandates and deliverables within the General Assembly.

The programme of action will need to provide some flexibility to ensure that its members are responsive to new challenges as they emerge, in a field in which technological developments are particularly rapid. It must also allow interested parties to discuss issues of interest on an ad hoc basis before reporting to a plenary body of the programme of action.

In order to build on the work done to date and to avoid duplication, it is essential that the programme of action take into account the work carried out under the auspices of the United Nations over the past 20 years or so by the various groups of governmental experts and working groups. Monaco therefore considers that the framework for responsible State behaviour must be the basis for this. The programme of action must be dynamic, allowing the framework to be updated and further developed as necessary on the basis of consensus.

Furthermore, given the importance of activities carried out by the private sector, which owns and operates many ICTs throughout the world, as well as the expertise and capacity of civil society organizations on these issues, the Government of Monaco sees only advantages in allowing all stakeholders to participate in the programme of action. While States should retain exclusive responsibility for the decision-making process, they could benefit from the contributions and experiences of various non-State entities. This would facilitate collaboration with non-State entities, including to prevent the development of malicious tools and improve the security of

[37] General Assembly resolution 77/37, para. 3.

the sector, and would contribute to the implementation of the framework for responsible State behaviour.

It is essential for the programme of action to be action-oriented, i.e. focused on the implementation of standards of responsible State behaviour. The voluntary submission of implementation reports would be especially useful to identify challenges and consider actions to address them. Moreover, exchanging good practices at the national, regional and international levels would help to guide States in their actions.

An action-oriented programme of action will thus promote international cooperation and strengthen the capacity of States, which is essential in this field. Existing initiatives will need to be promoted and their coordination strengthened.

Finally, the development of confidence-building measures and the strengthening of international cooperation will also be essential for the programme of action to be effective. All such initiatives, including the directory of points of contact and various proposals to enable specialized exchanges in these areas, should be encouraged.

Netherlands (Kingdom of the)

[Original: English]
[14 April 2023]

Introduction

The Netherlands continues to be deeply concerned by the growing risk to international security and stability, economic and social development and the safety and well-being of individuals posed by the malicious use of information and communications technologies (ICTs) by State and non-State actors. 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 ICTs in the context of international security, welcomed by the General Assembly in its resolution 77/37.

In accordance with paragraph 3 of that resolution, the present submission contains the views of the Netherlands on the desired scope, structure and content of the programme of action, as well as the preparatory work and modalities for its establishment. In particular, it proposes a practical mechanism to facilitate capacity-building within the programme of action.

Scope and objectives

The Netherlands, reaffirming paragraph 1 of General Assembly resolution 77/37, is of the view that the main scope of the programme of action should be (a) to support States' capacities and efforts to implement and advance commitments to be guided by the framework for responsible State behaviour; and (b) to discuss, and further develop, if appropriate, this framework, on the basis of consensus. While maintaining its focus

on matters related to international peace and security, the programme of action should also enhance synergies with other relevant efforts, including those related to cybercrime, connectivity, cybercapacity-building and digital development.

Structure

The Netherlands shares the view that the programme of action should be an inclusive, transparent, consensus-driven and results-based process. Its mandate 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 inclusive, open to participation by all Member States, permanent observers, intergovernmental and other organizations and specialized agencies. Furthermore, 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 regular meetings to adopt decisions and recommendations by consensus, as well as work undertaken in technical work groups, open to the participation of relevant stakeholders, dedicated to specific issues, including, inter alia, a study of how new and emerging technologies affect international peace and security in cyberspace.

Content

Facilitating capacity-building within the programme of action will bolster and streamline international cooperation to advance the worldwide implementation of the normative framework. The programme of action could also build synergies with existing capacity-building resources on a broader set of cyberrelated issues, such as connectivity, countering cybercrime and broader efforts to bridge the digital divide.

The Netherlands proposes a practical mechanism to facilitate capacity-building within the programme of action. The proposal is based on a four-step cycle of (1) developing a set of programme of action areas of capacity-building; (2) self-assessing and identifying needs; (3) matching needs with resources; and (4) a feedback loop.

Step 1: developing a set of programme of action "areas of capacity-building"

Under the programme of action, States could together develop a set of programme of action-endorsed "areas of capacity-building" that are instrumental to the implementation of the framework for responsible State behaviour. A similar approach has been taken with the areas of assistance identified with respect to the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects. The areas of capacity-building would build on the rich practical guidance for implementation provided in the consensus reports of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security and would be reviewed periodically to remain up-to-date. The areas of capacity-building would provide a common framework that translates the consensus outcomes to practical action on, for example, critical infrastructure protection, incident response, policies and strategies, computer emergency response teams, and so on. They should also be flexible to ensure they can be adapted to the diverse contexts and priorities of each State. In identifying the areas of capacity-building, States could draw from the work

undertaken by the United Nations Institute for Disarmament Research (UNIDIR) on a threat-based approach to unpacking cybercapabilities needs and the norms implementation checklist of Singapore and the Office for Disarmament Affairs, as well as tools developed by other stakeholders, such as the Cybersecurity Capacity Maturity Model for Nations developed by the University of Oxford.

Step 2: self-assessment and identification of needs

Based on the areas of capacity-building and the accompanying tool, States can voluntarily conduct a self-assessment to identify their cooperation and capacity-building needs and gaps. This would ensure national ownership and a needs-based approach to capacity-building. The UNIDIR national survey of implementation of United Nations recommendations on responsible use of ICTs by States in the context of international security provides a useful tool for undertaking such a self-assessment. States can then choose to share the outcomes of their self-assessment in the programme of action, for example at a technical working group.

Step 3: matching needs with resources

As a next step, the programme of action would provide a convening platform in order to match the identified capacity-building needs with resources. The programme of action would serve as a hub where providers of capacity-building could hold exchanges with States seeking capacity-building resources to address the capacity-gaps identified in the areas of capacity-building. Providers of capacity-building would be encouraged to make available resources dedicated to the areas of capacity-building, thereby helping to mobilize more resources for capacity-building with a common purpose. The secretariat could support States by maintaining an online overview of capacity-building needs and available resources. This overview would integrate existing tools, such as the Cybil Portal of the Global Forum on Cyber Expertise, as well as other potential United Nations portals or repositories proposed by several Member States in the working group. An easily accessible overview could also help States to find available resources for cybercapacity-building in areas adjacent to international security (e.g. cybercrime, digital development, connectivity, and so on). This includes capacity-building work undertaken by, among others, regional organizations, the International Telecommunication Union, INTERPOL, the United Nations Office on Drugs and Crime and the Global Forum on Cyber Expertise.

Capacity-building efforts as part of the programme of action framework should be undertaken in accordance with the principles for capacity building agreed in the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.

Step 4: feedback loop

After capacity-building needs have been identified and successfully matched with resources and capacity-building is underway, the programme of action platform would facilitate a feedback loop for reporting progress, sharing best practices and identifying areas where the normative framework could be further developed.

The preparatory work and modalities for the establishment of the programme of action

General Assembly resolution 77/37 provides an initial road map towards establishing the programme of action. Recalling the recommendations contained in the final reports of the Working Group and the Groups of Governmental Experts that the programme of action could be further elaborated in the open-ended working group on security of and in the use of information and communications technologies 2021–

2025, the Netherlands welcomes further discussions on the scope, structure and content of the programme of action within the working group and welcomes paragraph 2 of General Assembly resolution 77/37, which states that the "programme of action is to take into account the consensus outcomes adopted by the open-ended working group 2021–2025." In that regard, the Netherlands would encourage further intersessional and dedicated sessions of the working group to continue elaborating the programme of action. The Netherlands also welcomes the request of the General Assembly to the secretariat of the Office for Disarmament Affairs, contained in resolution 77/37, to convene a series of regional consultations to share views on the programme of action.

In 2025, after the conclusion of the working group, the Netherlands envisages an international conference, open to non-governmental stakeholders, that builds upon the preparatory work done, including in the working group, to be held to adopt the founding document.

New Zealand

[Original: English]
[12 April 2023]

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 establishment of a framework for responsible State behaviour in cyberspace that has been endorsed by the General Assembly and is based on four pillars:

- International law: all Member States agree that international law applies to the conduct of States 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. Aotearoa New Zealand believes that it is now time to build on this foundation and establish a permanent, regular, institutional cybersecurity dialogue at the United Nations. As a sponsor of General Assembly resolution 77/37, we support ongoing discussions on the establishment of a programme of action on cybersecurity and the further elaboration of its scope, structure, content, preparatory work and modalities, including during the regular institutional dialogue agenda item in the open-ended working group on security of and in the use of information and communications technologies 2021–2025.

4. We envisage a programme of action that is the "permanent home" of cybersecurity discussions at the United Nations at the conclusion of the current 2021–2025 working group, building on the proposal adopted in General Assembly resolution 77/37. In line with that proposal, we support the establishment of a programme of action that is:

(a) The 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 international law, ensuring that the programme of action builds on, and enhances, the foundational work of successive Groups of Governmental Experts and working groups to advance responsible State behaviour online;

(c) Inclusive of multi-stakeholder participation involving Governments (which bear responsibility for international peace and security in cyberspace), companies, civil society, technical experts, academics and other organizations that contribute to a free, open, secure and interoperable Internet. Aoteraoa 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 the implementation of the framework for responsible State behaviour and the promotion of capacity-building measures that support States in implementing the framework and mechanisms for accountability and monitoring;

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

North Macedonia

[Original: English]
[14 April 2023]

Submission of the Government of the Republic of North Macedonia to the report of the Secretary-General on the programme of action towards implementing the framework and building resilience in line with General Assembly resolution 77/37

The discussion on the principles related to the programme of action is crucial in enhancing our ability to address challenges and ensure a secure cyberspace.

Our view is that regional and global collaboration can significantly enhance the pace and effectiveness of State actors' efforts to improve their response capabilities.

In countries comparable to North Macedonia, where there is a lack of standards and resources for defence, individuals, businesses, and organizations are very susceptible to cyberthreats. Therefore, the programme of action should establish a permanent and unified institutional structure to address cyberissues. This structure should have a clear and well-defined mandate and sufficient resources in order to confront the constantly evolving landscape of threats.

Inter-organizational cooperation, including cross-regional collaboration among institutions that are dealing with the issue of their relevant structures involved in cybersecurity matters, should also be considered in order to strengthen coordination, which can add value in the further exchange of experiences, with the aim of building a coherent front that can address all emerging challenges.

To promote widespread involvement in this respect, the programme of action must provide a malleable framework that can be adjusted as required. One possible solution is for the programme of action to hold annual or biannual plenary sessions, which would be open to all Governments, whose decisions would be based on the efforts of specialized working groups during the intersessional period.

These plenary sessions could also establish task forces utilizing the knowledge of both States and pertinent stakeholders.

While the established framework for responsible State behaviour should serve as the basis for the work of the programme of action, there should also be room for updating the framework as necessary. One way to accomplish this is through periodic plenary meetings or review conferences, during which States can reassess the framework and decide to enhance it, if deemed necessary. To ensure the effectiveness of these reviews, dedicated working groups could inform the plenaries during the intersessional period.

A major priority for the programme of action should be to provide significant support for the implementation of its efforts. This level of support could come in the form of voluntary reporting on implementation efforts by participating States, which would help to identify the most pressing needs and challenges.

The programme of action should also provide updated, practical recommendations on a continual basis to guide States in their implementation efforts. In addition, it should offer support for capacity-building activities to further enable effective implementation.

We believe that the programme of action should be comprehensive and suitable for each country. One of the challenges is that the needs and capacities of different countries can vary significantly. Therefore, it is important that the programme of action be flexible enough to accommodate these differences and that it can be tailored to the specific needs and circumstances of each country. This could help to ensure that the implementation is feasible and effective in each context.

The programme of action must prioritize inclusivity, not only for participating States, but also for the stakeholder community. With regard to stakeholders, the programme of action should affirm that States hold the primary responsibility for matters related to international security and thus retain decision-making power. However, the programme of action should also provide modalities that enable all stakeholders to attend formal meetings, make statements and submit written inputs. This approach would ensure that the voices and perspectives of all relevant parties are considered while acknowledging the central role of States in matters of international security.

Norway

[Original: English]
[14 April 2023]

Norway supports the establishment of a programme of action to advance responsible State behaviour in the use of information and communications technologies (ICTs) in the context of international security. The proposal for its establishment was welcomed by the General Assembly in its resolution 77/37, which Norway sponsored.

Norway considers that establishing a programme of action is the best way to move forward in United Nations discussions and efforts on cybersecurity and responsible State behaviour in cyberspace. We believe that the programme of action should be a permanent structure for dealing with cybersecurity issues in the United Nations. This would allow for a stable structure in which we can focus on action-oriented activities and concrete progress, as well as continue the normative discussion. The programme of action should reaffirm and build on the consensus-based framework for responsible State behaviour achieved through years of discussions in the 2010, 2013, 2015 and 2021 Groups of Governmental Experts and

in the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. The programme of action should be inclusive, transparent, consensus-based, action-oriented and results-based.

We should have one structure in the United Nations both for regular dialogue and for implementation of the normative framework for responsible behaviour in the use of ICTs. The programme of action should be established by the time the open-ended working group on security of and in the use of information and communications technologies 2021–2025 concludes its mandate in 2025.

The consensus achieved on the normative framework should now be accompanied by action-oriented implementation and capacity-building. The programme of action could promote capacity-building activities to support States in implementing the normative framework. In the programme of action, Members States and relevant stakeholders could have focused discussions, round tables, briefings, voluntary reporting by States on implementation efforts, mapping of needs and exchange of knowledge, best practices and expertise. The programme of action could provide a better opportunity for tailored assistance to States in their efforts to maintain a free, open and secure cyberspace. The programme of action should consider existing initiatives and cooperation on cybersecurity within relevant organizations such as the Organization for Security and Cooperation in Europe and other regional organizations.

The programme of action should be organized in a way that allows for flexibility in terms of focus areas and practical efforts. This could allow States to address new threats and emerging technologies. The programme of action should focus both on the implementation of norms and continuation of the discussion on the further development of the normative framework. The framework of the structure of the programme of action should be subject to regular review, as necessary and appropriate, through regular meetings or review conferences.

The programme of action must be inclusive. All Member States must be able to participate. In addition, we need broad participation from non-governmental actors and other stakeholders, as they have important roles in maintaining a free, open and secure cyberspace. Regular consultations with the private sector, academia and non-governmental organizations would secure the necessary expertise and resources for both discussions and practical efforts. The inclusion of stakeholders does not challenge the role of States in international security.

Norway believes that enough time should be allocated within the format of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 for detailed discussions on the mandate, modalities and realization of a future programme of action. The working group should have a dedicated session to discuss the programme of action.

Pakistan

[Original: English]
[22 March 2023]

Pakistan maintains a consistent and clear position on the topic of regular institutional dialogue including the programme of action. We propose that the key principles that should be considered in the formulation of future platforms for discussions on information and communications technologies (ICTs) must include inclusivity, transparency, consensus-driven decision-making, multi-stakeholder participation, global collaboration and sustainability. Pakistan believes that the future institutional dialogue must also include in its mandate the topics of capacity-building,

norms-building and the application of international law in cyberspace, including discussion on the formulation of a legally binding instrument to regulate the behaviour of States in cyberspace. Furthermore, we hold the view that such dialogue should take place under the auspices of the United Nations.

It is essential to emphasize here that at this stage there is no need to create any parallel structure to the existing open-ended working group on security of and in the use of information and communications technologies 2021–2025. Pakistan firmly believes that the existing working group is the most appropriate forum for all discussions related to the terms of reference and mandate areas of any future platform, including the programme of action.

The decision of Pakistan to abstain from the resolution on the programme of action is driven by our belief that any mechanism or structure created after the existing working group concludes in 2025 must be built on a sustainable foundation and developed through a consensual process. Therefore, the existing working group provides an ideal platform for such discussion. We therefore advocate for a collaborative and all-inclusive approach for the programme of action, which would ensure its effectiveness and long-term sustainability.

In addition to this, we would like to announce the submission of a paper that sheds light, in detail, on the position of Pakistan on the application of international law in cyberspace, including other aspects of global cybersecurity. The paper may be accessed at https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf.

Philippines

[Original: English]
[10 April 2023]

A regular institutional dialogue that would facilitate a permanent forum for all Member States is needed now more than ever, given the evolving nature of information and communications technologies (ICTs) in the context of international peace and security.

The Philippines finds merit in the creation of a programme of action to advance responsible State behaviour in the use of ICTs in the context of international security. However, the Philippines is of the view that the creation of a permanent regular institutional dialogue should be decided by the open-ended working group on security of and in the use of information and communications technologies 2021–2025. Therefore, the Philippines was constrained to abstain on the adoption of General Assembly resolution 77/37 on the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security.

The Philippines is of the view that the working group is the most appropriate platform to discuss the scope, structure and content of the programme of action, given the inclusive, transparent and consensus-based mandate of the working group. According to the first annual progress report of the working group, adopted by consensus, the working group decided to convene intersessional meetings to advance and deepen discussions on specific proposals, including proposals on the establishment of a permanent regular institutional dialogue on security of and in the use of information and communications technologies. These meetings provide a venue at which Member States can hold an inclusive dialogue and find convergence on the future of the regular institutional dialogue.

The Philippines therefore reaffirms the principles contained in paragraph 74 of the 2021 consensus outcome document of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, that "any future mechanism for regular institutional dialogue under the auspices of the United Nations should be an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven and results-based."

Aside from these core principles, the Philippines maintains the view that any future dialogue should take into account the importance of narrowing the gender digital divide, promote the effective and meaningful participation and leadership of women in decision-making process and be gender-sensitive.

The Philippines also reaffirms the conclusion reached by the Working Group in paragraph 73 of its 2021 report that future dialogue should, inter alia, raise awareness, build trust and confidence and encourage further study and discussions on areas where no common understanding has yet emerged. The Philippines furthermore joins States in recognizing the utility of exploring mechanisms dedicated to following up on the implementation of the agreed norms and rules as well as the developments of further ones.

Therefore, the Philippines supports a future regular institutional dialogue that would advance responsible State behaviour in the use of ICTs in the context of international security, and would, inter alia:

- Provide capacity-building programmes that enable States to develop skills, human resources, policies and institutions in order to facilitate their genuine participation in discussions on ICTs in the context of international security and their ability to address vulnerabilities in their critical infrastructure. Capacity-building programmes should be anchored on the principles consensually agreed by all Member States in the outcome document of the Working Group (A/75/816), which contains a discussion of process and purpose, partnerships and people, including the integration of capacity-building efforts into the 2030 Agenda for Sustainable Development.
- Facilitate the understanding of existing and potential threats and how to address them.
- Provide concrete steps on how to implement existing rules and norms of responsible State behaviour and further discussion on other possible norms in view of the evolving threats related to ICTs that would facilitate a more transparent and predictable cyberspace and maintain peace in this area.
- Deepen understanding on the applicability of international law and, if gaps still exist, facilitate a core group discussion on how to address this issue through, for example, the possible development of a normative document or legally binding instrument that would satisfy the special characteristics of the ICT environment.
- Provide practical guide that States can use to facilitate information-sharing, table-top exercises and coordination in the field of ICTs in matters related to international peace and security.

The Philippines is of the view that the future regular institutional dialogue on ICTs in the context of international security should be decided by the open-ended working group on security of and in the use of information and communications technologies 2021–2025 and should not be launched or convened in parallel to the ongoing working group. Proliferation of discussions on this important matter that would adversely affect the participation of small delegations should be avoided, unless otherwise decided by consensus by the working group. Discussions on the

future dialogue should also take into account the 2021 and 2025 outcome documents of the working groups, the annual progress reports of the working group and the 2010, 2013, 2015 and 2021 reports of the Group of Governmental Experts.

Romania

[Original: English]
[14 April 2023]

In line with the previous work regarding the establishment of a "regular institutional dialogue" to address issues related to the use of information and communications technologies (ICTs) in the context of international security, the establishment of a programme of action would provide the First Committee with a permanent and institutional mechanism for following up on the implementation of agreed norms by providing sets of actionable recommendations and supporting or promoting relevant capacity-building projects. In the view of Romania, such a permanent, inclusive and action-oriented mechanism is urgently needed.

The scope of the programme of action should be related to the use of ICTs in the context of international security. The objective of the programme of action should be to contribute to the maintenance of international peace and security by preserving an open, stable, secure, accessible and peaceful ICT environment, in full alignment with the aquis of responsible State behaviour in cyberspace.

The programme of action could aim in particular to strengthen cooperation, advance stability in cyberspace and increase resilience. In this respect, reducing tensions, preventing conflicts, promoting a cooperative approach to cyberthreats and supporting the implementation of the framework for responsible State behaviour based on international law, including international humanitarian law and human rights, norms of responsible State behaviour, confidence-building measures and capacity-building, are but a few of the objectives to be achieved through an inclusive dialogue among States and with the relevant stakeholders.

At the basis of the political document of the programme of action should be the reaffirmation by States of their commitment to the framework for responsible State behaviour, the establishment of a permanent institutional mechanism to advance the implementation of this framework and the fostering of multi-stakeholder involvement, as appropriate.

In line with the recommendations of the reports of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and of the Groups of Governmental Experts regarding the elaboration of the programme of action, including in the process of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, as well as in line with General Assembly resolution 77/37, provisions regarding the report of the Secretary-General on the programme of action, intersessional meetings and dedicated sessions of the working group should be organized in 2024 and 2025 to continue elaborating the different aspects of the programme of action.

Romania is of the view that, in line with the option noted in General Assembly resolution 77/37, a conference for the establishment of the programme of action should be called at the earliest convenience.

Russian Federation

[Original: Russian]
[12 April 2023]

Pursuant to paragraph 3 of General Assembly resolution 77/37, the Russian Federation hereby submits its views on the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security.

It is our understanding that the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 is the first and only inclusive, open, transparent and truly democratic negotiating mechanism on international information security at the United Nations. The principle of consensus allows all States, without exception, to influence the decision-making process. The Group has proven its effectiveness and relevance in practice.

It is necessary for the negotiation process to evolve, based on the Working Group's experience. The detailed proposals of the Russian Federation in this regard are outlined in the concept paper on regular institutional dialogue (submitted during the fourth session of the Group, held in New York from 6 to 10 March 2023).

The programme of action should not prejudge the decision on a future negotiating mechanism on international information security at the United Nations. This initiative, alongside other national proposals, should be discussed in the Working Group, in line with its mandate as set out in General Assembly resolution 75/240. A period of three years, until 2025, is long enough to jointly develop an understanding of the format that will replace the current Group.

In terms of content, the programme of action remains poorly developed and its purpose is unclear. Discussions in the Working Group show that even the proponents of the programme do not have a common position on its main parameters; above all, on the decision-making procedure.

In its current form, the programme of action initiative cannot claim to be an independent and inclusive negotiating mechanism on international information security at the United Nations. It has no added value with respect to the Working Group, but rather duplicates key areas of its mandate (General Assembly resolutions 75/240 and 77/37, para. 1). At the same time, the agenda of the programme of action is much narrower than that of the existing Group and is limited to a discussion of the existing recommendations of the Working Group and the Group of Governmental Experts and the efforts of States to implement them.

Capacity-building, which is the focus in advancing the programme of action, is also an aspect of the Working Group's mandate. The Group has developed a list of universal principles for such activities (the 2021 report of the Working Group) and, in accordance with General Assembly resolution 77/36, is exchanging views on the specific needs and requirements of countries in this area and the mechanisms for addressing them, including funding.

Moreover, the authors of the programme of action, in an attempt to give it practical meaning, are appropriating proposals from States that are already being discussed within the Working Group. This includes the creation of a directory of points of contact and a permanent United Nations online portal on international information security. These initiatives will be implemented (once States reach a consensus) irrespective of the launch of the programme.

It is important to keep in mind that Western countries attach a very specific political meaning to the programme of action and are publicly promoting it to spite

Russia. They justify the need to launch the programme with unsubstantiated allegations of allegedly malicious cyberactivities by our country, including in the context of the special military operation in Ukraine (in particular, such arguments are voiced by French representatives at the Organization for Security and Cooperation in Europe). Such an anti-Russian message cannot serve as the basis for constructive engagement between States on issues of international information security. It is contrary to the spirit of the Charter of the United Nations and, in particular, its Article 1 on equality and friendly relations among nations. Under these circumstances, the programme of action can be expected to be used by Western countries, in line with the "rules-based order" concept promoted by the United States, to impose non-binding rules and standards to their advantage, instead of international law.

The Russian Federation believes that it is only after the existing voluntary rules of responsible behaviour are codified in a universal legally binding document that one can talk about the accountability of countries for their compliance. A growing number of States have spoken out in favour of an international legal regime on international information security at the United Nations. Whatever negotiating format is established at the conclusion of the Working Group should be aimed at developing an appropriate international instrument.

In this regard, Russia submitted a concept on a United Nations convention on ensuring international information security at the fourth session of the Working Group. Our initiative is the practical development of a long-standing discussion on this topic. It is based on the purposes and universally recognized principles of the Charter of the United Nations that unite the world community for the maintenance of international peace and security. It builds upon the recommendations of annual General Assembly resolutions on developments in the field of information and telecommunications in the context of international security, as well as the consensus reports of the 2021 Working Group and of the 2010, 2013, 2015 and 2021 groups of governmental experts. It also takes into account the initiatives of States outlined in the Chair's summary of the first Working Group. Such a convention should include mechanisms to monitor the implementation of its provisions by the parties, to make changes and adopt supplements, to exchange views on the implementation of the instrument, and to settle and peacefully resolve disputes.

We are convinced that the Working Group is the most appropriate forum to discuss this and other country proposals in the area of information and communications technology security. The Group serves the interest of the vast majority of Member States and therefore should not be replaced by the programme of action. Those elements of the programme that States find useful can either be integrated into the existing mechanism or into a future one.

Singapore

[Original: English]
[14 April 2023]

Singapore attaches great importance to the consensus language adopted thus far on the programme of action proposal. These consensus decisions are a good basis for further consideration of the programme of action. In this regard, the following elements from previous consensus reports of the working groups remain important:

- According to the report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, States note a variety of proposals for advancing responsible State behaviour in information and communications technologies (ICTs), which

would, inter alia, support the capacities of States in implementing commitments in their use of ICTs, in particular the programme of action. In considering these proposals, the concerns and interests of all States should be taken into account through equal State participation at the United Nations. In this regard, the programme of action should be further elaborated, including at the process 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.[38]

- In its first annual progress report, the open-ended working group on security of and in the use of information and communications technologies 2021–2025 stated that States, at the fourth and fifth sessions of the working group, are recommended to continue to engage in focused discussions within the framework of the working group to further elaborate the programme of action with a view towards its possible establishment as a mechanism to advance responsible State behaviour in the use of ICTs, which would, inter alia, support the capacities of States in implementing commitments in their use of ICTs. At these sessions, States will also engage in focused discussions on the relationship between the programme of action and the working group and on the scope, content and structure of a programme of action.[39]

As Member States engage in focused discussions within the framework of the working group to further elaborate the programme of action, and in the context of discussion on the future mechanism for regular institutional dialogue, Singapore is of the view that it is essential for this mechanism to be universal, inclusive, transparent, consensus-based, action-oriented and single-track in nature. The basic principles that should govern its scope, structure and content are as follows:

- Established and operated exclusively on the basis of consensus in order to preserve the fragile and hard-won consensus achieved by the international community over the course of successive previous Groups of Governmental Experts and working groups.
- Motivated by a vision of building upon the foundation provided by the work of successive previous Groups of Governmental Experts and working groups.
- Aimed at strengthening the cumulative and evolving framework for responsible State behaviour in the use of ICTs and at reinforcing the spirit of consensus underpinning this framework.

Slovenia

[Original: English]
[13 April 2023]

Slovenia perceives the programme of action on information and communications technology (ICT) security as an important instrument for securing peace and stability in cyberspace. It should additionally serve as an effective vehicle for securing an open and stable future development of cyberspace.

The programme of action could also provide a permanent structure for dealing with cyberissues in the First Committee and could submit substantive deliverables to the General Assembly on adoption and approval. The permanent structure of the programme of action would provide institutional stability and could spare the General Assembly discussions about the creation of open-ended working groups, which are,

[38] See A/75/816.
[39] See A/77/275.

by definition, time-limited. In any case, it could work in a complementary and coordinated fashion with other relevant United Nations processes, such as the open-ended working group on security of and in the use of information and communications technologies 2021–2025, established pursuant to resolution 75/240.

Slovenia strongly supports the principle of a transparent and inclusive multi-stakeholder approach and the participation of State and non-State actors in the various work of the programme of action.

Slovenia advocates that States should develop voluntary self-assessment and be ready to share best practices. The programme of action should support capacity-building and information-sharing with the aim being for all States to promote and implement the framework of responsible behaviour in cyberspace. Key areas for capacity-building should include, inter alia, incident response, the development of policies and strategies, the development of computer emergency response teams, the building of necessary cyberinfrastructure and the normative framework. The programme of action should also be flexible enough to allow States to address new threats and to further develop the normative framework, if necessary.

Sweden

[Original: English]
[14 April 2023]

Introduction

The First Committee has consolidated a framework for responsible State behaviour in the use of information and communications technologies (ICTs), endorsed by the General Assembly in consensus resolutions.[40] In the context of the framework, there have been discussions on the establishment of a regular institutional dialogue to address issues related to the use of ICTs in the context of international security. It has been underlined that such a dialogue should place a strong focus on supporting the implementation of the normative framework. In particular, the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security concluded that any 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".[41] In this context, the establishment of a programme of action would provide a permanent institutional mechanism which would follow up on the implementation of the agreed framework while also allowing for its further development, if appropriate.

Content

The programme of action could be based on a political document which would notably (a) reaffirm States' founding political commitment to the framework for responsible State behaviour, as affirmed in relevant reports and resolutions,[42] which would consider the consensus outcomes adopted in the Working Group, and

[40] See General Assembly resolutions 70/237 and 76/19.

[41] See A/75/816, para. 74.

[42] These would include 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 (A/75/816) 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 (A/77/275), bearing in mind that the future consensus outcomes of the current working group will add to this framework, which is cumulative and evolving.

(b) establish a permanent institutional mechanism to (i) advance implementation of this framework, including by supporting States' capacities to do so, (ii) further develop the framework as appropriate and (iii) foster multi-stakeholder cooperation in relevant areas.

Sweden notes that there are many aspects of how to advance the implementation of the framework. We align ourselves with the European Union input and the French proposal as presented at the Working Group in March 2023. To further advance the discussion, our submission focuses on the importance of applying a multi-stakeholder approach, the role of the private ICT sector and the need to promote public-private partnerships.

Multi-stakeholder involvement

Given that States bear primary responsibility for the maintenance of international peace and security,[43] the programme of action should seek to enhance multi-stakeholder engagement and cooperation for the benefit of an open, free, global, stable and secure cyberspace.

Today it may be difficult for governments to gather the means and capacity to fully understand and respond to the growing number of cyberrelated issues their countries are facing. Governments are increasingly relying on cooperation and collaboration with the private sector and other non-governmental actors to respond to threats and challenges and the public policy needs and concerns that stem from them. Meanwhile, the value of further strengthening collaboration, when appropriate, with civil society, the private sector, academia and the technical community was repeatedly emphasized by relevant First Committee working groups,[44] both because cooperation with these stakeholders can be essential for States in implementing their commitments under the framework and because stakeholders themselves "have a responsibility to use ICTs in a manner that does not endanger peace and security".[45] Private stakeholders can also bring valuable expertise to discussions and contribute to capacity-building efforts. Security in the digital era cannot be achieved by States alone and the multi-stakeholder approach must remain a fundamental part of our cooperation.

The role of the private ICT sector in defending and promoting human rights

The ICT sector has often been perceived as an ally of freedom of expression and human rights. Telephones and cellular technology connect people and businesses; the Internet opens a new world of information, education and entertainment for people and businesses, enabling exchanges, debates, arguments, discussions, negotiations and resolutions. The private sector provides the technologies that form the backbone of the Internet.

The private ICT sector is very diverse. It comprises purveyors of hardware – such as transmission towers, instruments and equipment, servers, cables and other infrastructure – as well as software and digital services, including the numerous technologies and standards that comprise the architecture of the Internet. This diversity makes it difficult to generalize about the sector and focus on a single set of issues. As with other industries, companies from all around the world are active in the ICT sector, making a geography-focused strategy less effective and a multilateral approach necessary.

[43] See A/75/816, para. 10.
[44] Ibid., para. 22.
[45] Ibid., para. 10.

The obligation of States to respect human rights also includes an obligation to protect individuals and groups of individuals against human rights abuses by third parties, including business enterprises. Their obligation to fulfil human rights means that States must take positive action to facilitate the enjoyment of basic human rights (Guiding Principles on Business and Human Rights, principle 1). The possibility of a gap between the expectations of users and civil society and the understanding by business of its responsibilities will always remain. There is a need for greater consensus politically and within the industry to work on this agenda.

Multi-stakeholder initiatives are the way forward

Governments and ICT companies need good guidance based on internationally accepted standards, norms and principles in order to respond to challenges. Sweden will continue to promote an open, free, global, stable and secure cyberspace where human rights, fundamental freedom and the rule of law fully apply in support of the social well-being, economic growth, prosperity and integrity of our free and democratic societies. Therefore, governments would benefit from working together and approaching problematic contexts jointly. The programme of action mechanism should be a platform for States to engage with multi-stakeholders, including the private sector, from all regions of the world. Working in partnerships can add valuable input.

Sweden supports an approach that is anchored in norms, rules and procedures and practices. However, such regimes are difficult to put in place in a constantly shifting environment. Overregulation may misalign with both existing and emerging security threats, and it can slow or undercut innovation and reduce the incentives for private sector participation. It can also misalign with other obligations and duties, including those aimed at minimizing harm to the public. The programme of action mechanism must seek to engage with the private sector on cybersecurity and resilience-related issues. In this regard, public-private partnerships and multi-stakeholder engagement should be underpinned by key principles such as transparency and accountability, notably when they are established to solve specific public policy problems.

Keeping the momentum and preparing for an international conference in 2025

Sweden supports additional focused discussions in the open-ended working group on security of and in the use of information and communications technologies 2021–2025 to further elaborate the programme of action and seek consensus on its establishment. Intersessional meetings and dedicated sessions of the working group should be organized in 2024 and 2025 to continue elaborating the different aspects of the programme of action, to draft its founding document, and so on.

Sweden supports further discussions on the precise modalities for the potential establishment of a programme of action, including the option of a dedicated international conference in 2025 to adopt the founding document of the programme of action on the basis of the preparatory work done, including in the working group (as noted in General Assembly resolution 77/37). It should provide for participation by relevant stakeholders (accredited with modalities close to those adopted in Assembly resolution 75/282).

Switzerland

[Original: English]
[14 April 2023]

I. Introduction

1. For more than 20 years, States have been discussing at the United Nations level existing and potential threats to international peace and security by States' use of information and communications technologies (ICTs) and how to address those threats. Those discussions, held in varying, time-limited formats, have, incrementally, made considerable progress. The consensus recommendations of the 2010, 2013, 2015 and 2021 Groups of Governmental Experts, the consensus recommendation of the 2021 Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the 2022 consensus annual progress report 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 for responsible behaviour of States in cyberspace comprises the application of international law to cyberspace, voluntary norms of responsible State behaviour, confidence-building measures and capacity-building.

2. Member States, through General Assembly resolutions 70/237 and 76/19, have agreed by consensus to be guided in their use of ICTs by the 2015 and 2021 reports of the Groups of Governmental Experts as well as the 2021 report of the Working Group, which outline the framework, affirming the so-called acquis.

3. The proposed programme of action builds firmly on this agreed framework and the acquis.

II. Scope and objective of the programme of action

4. The programme of action would contribute to the shared goal of an open, free, peaceful and secure cyberspace. It would provide a permanent structure for regular institutional dialogue at the United Nations level to support Member States in their national efforts to implement and operationalize the framework for responsible State behaviour in cyberspace.

5. It would be action-oriented, inclusive, transparent, consensus-driven and results-based.

6. Its action-oriented nature is a core element of the programme of action. The programme would assist States in putting in place cooperation and capacity-building activities adapted to their needs. It would provide a permanent platform for the exchange of knowledge, best practices and expertise, thereby contributing to building and strengthening trust and transparency.

7. The programme of action should also be flexible enough to allow States to address future threats. In this regard, it should regularly convene States to review the framework and to further develop the framework, as appropriate, on the basis of consensus.

III. Structure and content

8. An annual formal meeting would be held as part of the programme of action. States would be invited to conduct, on a voluntary basis, an assessment of their progress and challenges in implementing the framework. This could be done either by creating its own reporting system or by promoting existing mechanisms (such as the national survey of implementation of United Nations recommendations on

responsible use of ICTs by States in the context of international security[46]). Based on these assessments, the specific needs, positive lessons learned, challenges and priority areas could be identified. At the annual formal meeting, Member States would adopt decisions and recommendations by consensus. Also at the annual formal meeting, Member States would establish technical working groups by consensus.

9. During the intersessional period, technical working group meetings could be held, as established at the annual formal programme of action meeting. The findings and recommendations of those meetings would feed back into the annual formal meeting. The technical working groups would focus on priority areas as identified at the annual meeting. These technical areas could include operationalization of specific voluntary norms through the development of concrete guidance and exchange of best practices; advancing discussion and common understanding on how international law applies to cyberspace; presentation of concrete capacity-building needs; and provision of concrete support.

10. Regular exchanges with regional organizations as well as relevant international bodies such as the International Telecommunication Union should also be envisaged to share best practices and to support coordination with relevant international and regional initiatives. Where such exchanges already exist, the programme of action should build on corresponding experiences and structures, as appropriate.

11. On a regular basis (e.g. every 4–6 years), a review conference could be held to update the programme of action, as appropriate.

12. All decisions taken within the programme of action should be taken by consensus.

13. States bear the primary responsibility for the maintenance of international peace and security, including in cyberspace. At the same time, they are not the sole actors relevant to the achievement of this goal. This is especially true in cyberspace, where most of the infrastructure is owned and operated by private actors. Multi-stakeholders play an integral role in its operation and possess valuable insights and expertise beyond that of States. Actors from civil society, the private sector, academia and the technical community also have their respective roles and contributions to make, especially in supporting States in their implementation of their commitments under the framework for responsible behaviour of States in cyberspace. Moreover, their expertise is important for capacity-building efforts. It is essential for States to harness this knowledge and to benefit from a rich pool of ideas.

14. Decision-making and negotiation within the programme of action should remain the prerogative of Member States. In addition, the programme of action should allow for the broad and meaningful participation and contributions of the multi-stakeholder community in the annual formal meetings, review meetings and technical working group meetings. Modalities for the proceedings of programme of action meetings and working groups should therefore allow stakeholders to attend formal and informal sessions, deliver statements and provide oral and/or written inputs for consideration by Member States.

IV. Preparatory work and modalities for establishment of the programme of action

15. As recommended by the 2021 reports of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security and of the Working Group, the programme of action should be further elaborated, including at the process of the open-ended working group on security of and in the use of information and communications technologies 2021–2025.

[46] Available at https://nationalcybersurvey.cyberpolicyportal.org/.

Therefore, within the current working group process there should be dedicated sessions on the programme of action. Outcomes of these sessions should be reflected in the respective annual progress reports of the working group.

16. In addition, intersessional multi-stakeholder consultations should be held to gather their views and suggestions on the programme of action and its establishment.

17. Establishment of the programme of action should be based on a decision/resolution by the General Assembly on the basis of the preparatory work done, including in the working group. Member States may wish to hold a dedicated United Nations conference to establish the programme of action.

18. The programme of action should be operational after the conclusion of the working group.

Türkiye

[Original: English]
[14 March 2023]

- Carry out studies to reduce the difference in maturity level between countries with respect to cybersecurity and determining methodological methods.
- Utilize the criteria used in the International Telecommunication Union Global Cybersecurity Index, which is accepted as an important indicator in determining the maturity level of countries with respect to cybersecurity in order to achieve significant foresight for determining the potential growth areas of developing countries.
- Measure the maturity level of computer emergency response teams with respect to detection and intervention in order to determine the current situation and to increase their competencies.
- Increase the exchange of views among Member States in the process of harmonizing national rules and norms with international law and norms.
- Encourage cooperation between national incident response teams.
- Establish emergency communication channels and platforms that allow sharing of resources and information among Member States.
- Share best practices and experiences to better understand the rules, norms and principles.
- Organize international exercises to increase the cyberincident resilience and the response capacities of countries.
- Research national regulatory approaches for the security of emerging technologies and to prepare international guides for members.
- Make recommendations to close the gap among the cybercapacity-building needs of countries.
- Map regional progress in building necessary capacities.
- Carry out activities to increase the level of expertise of the personnel working in the fight against cybercrime.
- Include recommendations for the development, testing and implementation of local and international emergency response plans.

Ukraine

[Original: English]
[14 April 2023]

The development of joint and concrete measures to counter threats related to the use of information and communication technologies (ICTs) will contribute to responsible State behaviour in cyberspace.

The maintenance of international peace, security, cooperation and trust in the ICT environment is of utmost importance, especially in a context where a number of States are developing ICT capabilities for military purposes and the number of incidents related to the malicious use of ICTs by State and non-State actors continues to grow.

The programme of action should address the challenges and threats related to the increase of malicious activity in the field of the use of ICTs, which affects critical information infrastructure, infrastructure that provides basic services to the population, technical infrastructure necessary to ensure the general availability or integrity of the Internet, and the health-care sector.

Any activities, projects and initiatives related to the programme of action that duplicate those that are being implemented within the framework of the Organization for Security and Cooperation in Europe working group on confidence-building in the use of ICTs should be avoided.

Ukraine supported the consensual adoption of 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 (A/77/275) to further elaborate the programme of action, including within the working group process.

The programme of action may decide to convene one or two meetings of States per year, while the review conference could be held every 4 or 5 years. The programme of action may hold intersessional meetings and establish working groups to focus on specific agenda items.

The international conference on the establishment of the programme of action may be convened in 2025 after the expiry of the mandate of the working group.

The programme of action may envisage the possibility of presenting reports on national efforts on the implementation of rules, norms and principles, as well as convening regular meetings at the working level to focus on the implementation of such rules, norms and principles.

The programme of action may discuss the importance of cooperation among Member States in the field of the security of the use of ICTs, including through the establishment of platforms for the exchange of information on vulnerabilities and undocumented software functions and attack patterns, as well as the results of the evaluation of software and library security to prevent supply chain attacks.

The programme of action may envisage a procedure for the submission of requests for international assistance. The relevant mechanism exists within the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[14 April 2023]

Introduction

1. Over the past 30 years, Member States have developed a framework of responsible State behaviour in information and communications technologies in the context of international security, endorsed by the General Assembly in successive resolutions (resolutions 70/237, 76/19 and others).

2. The Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security concluded that future regular institutional dialogue should take place through an "action-oriented process with specific objectives, building on previous outcomes … [that is] inclusive, transparent, consensus driven and results-based".[47]

3. In 2022, the General Assembly, in its resolution 77/37, voted to welcome proposals for a programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. The United Kingdom strongly supports the creation of the programme of action as a permanent, inclusive, action-oriented mechanism for discussions on international peace and security in cyberspace.

4. This Programme of Action should also be developed with a particular focus on:

(a) **Inclusivity.** The programme of action should be shaped by, and open to participation from, all Member States. Modalities should allow for meaningful participation by non-governmental stakeholders. Establishing the programme of action as the single successor mechanism to the current open-ended working group on security of and in the use of information and communications technologies 2021–2025 will help States to efficiently allocate the resources to participate.

(b) **Legitimacy.** Member States have agreed a framework of responsible State behaviour in information and communications technologies (ICTs) in the context of international security. This should be our starting point. There is a clear role for the programme of action in supporting States to implement this consensus framework and in further clarifying how existing international law applies to cyberspace.

(c) **Flexibility.** This focus on implementation of the agreed framework would identify gaps for further elaboration. The structure of the programme of action should therefore be flexible enough to allow it to respond to such gaps as they are identified over time and to further develop the evolving framework, including in response to emerging threats.

Scope and objectives

5. The overall purpose of the programme of action should be to contribute to international peace and security through the preservation of a free, open, peaceful and secure cyberspace. It should do so by facilitating dialogue and cooperation between Member States on security of and in the use of information and communications technologies and by supporting the implementation and evolution of the framework.

6. The programme of action should be the single successor mechanism to the current working group in its discussion of security of and in the use of information and communications technologies. In doing so, it would provide:

[47] See A/75/816, para. 74.

- An opportunity for discussion of, and information-sharing on, cyberthreats (e.g. through discussion at annual meetings and in focused workstreams and through consideration of new mechanisms on threats, such as the portal proposed by India).
- A means of supporting States to identify the areas of capacity needed to improve their performance in the implementation of the framework (e.g. through voluntary reporting; stock-taking of existing capacity-building activities carried out by United Nations bodies; active participation of non-governmental stakeholders, including regional organizations, civil society and the private sector; engagement with the World Bank Cybersecurity Multi-donor Trust Fund and others).
- An inclusive process through which to elaborate the framework (e.g. through a workstream to consider how international law applies to cyberspace).
- A basis for the development of further confidence-building measures (e.g. by building on the points of contact directory, a permanent mechanism already under development in the current working group; discussion of further measures that would benefit from links to a permanent United Nations forum on international peace and security in cyberspace).

Structure and content

Political declaration

7. The programme of action should be initiated through a political declaration agreed at the political level through a high-level meeting or international conference. The framework should form the basis of this declaration, which should include agreement on actions to advance the implementation of commitments to responsible State behaviour in cyberspace; clarification of the application of international law in cyberspace; and the agreed scope and modalities for the programme of action.

8. Political-level agreement would provide an opportunity for States to publicly and visibly reaffirm their commitments at this stage in the evolution of the framework and could help States to secure political buy-in within their own systems.

9. Capacity-building is an important part of the framework and its value should be highlighted through the political declaration. The declaration should take account of the working group's principles on capacity-building and also the work of other United Nations and non-United Nations bodies, including the capacity-building principles set out in the Delhi communiqué of the Global Forum on Cyber Expertise.

Annual meeting

10. The programme of action should hold an annual formal meeting, which would provide an opportunity to:

- discuss and share information on new and emerging threats.
- review the implementation of the framework, including on the basis of voluntary reporting.
- share capacity-building opportunities and ensure briefings by relevant stakeholders.
- elaborate understandings of the framework, including on the application of international law.
- consider the recommendations of specific workstreams (which could be established through the annual meeting).

Review conferences

11. The programme of action should hold a review conference every four years. These conferences would allow the programme to take stock and to adapt, given the dynamic and evolving nature of threats to international peace and security in cyberspace.

Voluntary reporting

12. Implementation of the framework and support to capacity-building have been identified as important priorities for the programme of action. Voluntary reporting would support this effort. Existing surveys (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) and evolving mechanisms (such as the norms checklist proposed by Singapore) provide possible bases for a consistent approach through the programme of action.

Multistakeholder participation

13. Member States should have the exclusive right to negotiate outcomes and make decisions within the programme of action. However, non-government stakeholders provide valuable perspectives. They are often the first to be affected by cyberincidents and are essential to the response. They can also play an increased role in delivering capacity-building. Non-government stakeholders should therefore be able to participate meaningfully in all programme of action meetings, including through written and oral contributions. Stakeholder participation should be inclusive and diverse and regional participation should be encouraged. Stakeholder accreditation should be informed by transparency, with final decisions on accreditation being taken by all States, including through voting if consensus cannot be reached.

Preparatory work and modalities

14. The working group should play an important role in the further elaboration of the programme of action. Mindful of the resource constraints experienced by delegations, dedicated time to discuss and further elaborate the programme of action should be given within the formal and informal meetings of the current working group. Given the significance of the task, dedicated intersessional meetings are likely to be needed.

15. Member States should also not be precluded from developing proposals in additional conferences and bringing them to the working group and the General Assembly for consideration.

United States of America

[Original: English]
[14 April 2023]

Introduction

United Nations Member States have acknowledged that information and communications technologies (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 and the Open-ended Working Group

on Developments in the Field of Information and Telecommunications in the Context of International Security, States have coalesced around a framework for responsible State behaviour in the use of ICTs. This framework for enhancing international stability is comprised of the embrace of relevant international law, including the Charter of the United Nations, 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 articulated in the consensus report of the 2015 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, States have previously affirmed the need to establish regular institutional dialogue with broad participation under the auspices of the United Nations.[48] Building on that effort, the Working Group has since reaffirmed the need for States to pursue the establishment of a mechanism for future institutional dialogue.[49]

The consensus 2021 Working Group report recommended that a future United Nations mechanism on cyberissues should be inclusive, transparent, consensus-driven and results-based. The programme of action offers such a mechanism and provides an opportunity for States to create a permanent but flexible mechanism in the United Nations to advance the work of the framework to enhance peace and security in cyberspace and prevent conflict and harm to civilians caused by the use of ICTs. The programme of action should also be a permanent and action-oriented mechanism through which Member States can implement and advance the consensus framework.

Scope of the programme of action

General Assembly resolution 77/37 recalled the assessments and recommendations of the 2010, 2013, 2015 and 2021 groups of governmental experts, as well as those of the 2021 Working Group along with the first annual progress report of 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, and in particular "the cumulative and evolving framework for responsible State behaviour in the use of information and communications technologies elaborated by these processes", and called on Member States to be guided by those reports and the framework.[50] This framework, supported by those reports, is the foundation of the programme of action.

Member States should set the direction of the programme of action 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 would make it a durable resource for States in these efforts.

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

Non-State stakeholders should be an integral part of the programme of action process. The programme of action must have modalities for stakeholder participation that are as inclusive as possible to fully leverage these stakeholders' expertise.

[48] See A/70/174, para. 18.
[49] See A/75/816, paras. 70–74.
[50] See General Assembly resolution 77/37, preambular paras. 10 and 11.

Establishment of a programme of action

States' primary objective in establishing a future programme of action and its content should be to design an architecture that facilitates national implementation of the consensus framework, promotes cooperation among States on security in and of the use of ICTs and enables advancements to the framework over time as Member State consensus evolves.

To facilitate the creation of the programme of action in an expedient manner, the programme of action should be launched via an international conference[51] in 2025 following the conclusion of the working group. The outcome documents of that conference, which could include a political declaration, should form the substantive foundation of the programme of action and address modalities and rules of procedure for the programme of action mechanism. Regular programme of action meetings should start in 2026.

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

Structure

The programme of action should convene an annual meeting of States at which representatives would decide on thematic or issue-focused areas to be discussed in technical or informal working groups that would meet at a frequency established at the annual meeting or via the conference's outcome documents. The Office or the United Nations Institute for Disarmament Research could provide briefings summarizing national survey submissions and these meetings would also be opportunities for States to exchange views on:

- National experiences and best practices in implementing the framework
- Relevant capacity-building needs and resources
- Emerging issues and threats, including how the programme of action should address them.

In addition to an annual meeting and regular meetings of established technical or working groups, the programme of action could convene a review conference every three or four years to reaffirm the outcomes of the programme of action and consider whether changes to the content or structure of the programme of action are necessary. This regular review of the foundational documents of the programme of action would give States the flexibility to adapt the programme of action as circumstances evolve.

The programme of action would be launched in 2026 following the conclusion of the 2025 conference. Each year thereafter, via a resolution or decision, the First Committee would affirm the consensus outcomes of the annual meetings of the programme of action, including recommendations for timing and location of future meetings. The First Committee would also affirm the outcomes of review conferences when they occur.

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

[51] See General Assembly resolution 77/37, para. 3.

cooperation of States and confidence-building in the field of ICTs.[52] The United Nations has a key role in 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.

The primary capacity-building function of the programme of action should 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 in order to implement the framework to ensure that its efforts closely align with States' range of needs. In other words, it should aim to raise international awareness on the importance of cybercapacity-building to support the framework while also providing guidance and best practices that States could establish domestically/nationally to implement the framework.

The United States recognizes that many States still lack awareness on what the framework is and its importance. Many also lack the basic national-level cybersecurity capabilities needed to begin implementing the framework, including domestic needs 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 and cybersecurity standards. The programme of action should not duplicate or supersede such existing efforts. All of these efforts enhance States' national security posture and ultimately enable implementation of the framework but are outside of the mandate of the programme of action.

Multistakeholder participation

States should retain exclusive decision-making authority within the programme of action. Nonetheless, non-governmental stakeholders, to include civil society, academia and the private sector, play a positive role in multilateral forums by bringing expertise to formal discussions and contributing to capacity-building efforts. These groups should have an opportunity to actively participate in the programme of action as observers, without the right to vote.

For the programme of action to be as inclusive as possible of interested stakeholders, the modalities for objecting to stakeholder participation should be transparent and build upon existing gold-standard modalities. 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 a 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.[53]

With respect to the modalities of multi-stakeholder participation in formal sessions, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the use of Information and Communications Technologies for Criminal Purposes could serve as a model. Its modalities allow multi-stakeholder participation, including:

- attending any open formal session.

[52] Ibid., preambular paragraph 20.

[53] As articulated in section F of A/AC.278/2011/2.

- 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.[54]

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

Preparatory work

The United States acknowledges that establishing a programme of action will require significant effort from Member States. There should be continued dedicated discussions on the programme of action, including in the current working group, to enable a seamless launch of the programme of action following the conclusion of the current working group in 2025.

[54] See A/AC.291/6, para. 3.