CYBER CBMS IN ACTION

Working paper submitted by the open, informal, cross-regional group of the OEWG Confidence Builders in the name of the following OEWG participating states: Argentina, Australia, Brazil, Canada, Chile, Colombia, Czech Republic, Fiji, Germany, Israel, Republic of Korea, Mexico, The Netherlands, Singapore, Uruguay.

The 2023 Open-ended Working Group on security of and in the use of information and communications technologies decided to establish a global, inter-governmental, points of contact (POC) directory recognizing that the establishment and operationalization of the global POC directory is an important step forward in building confidence between States at the global level.

States further recognized in the 2023 Annual Progress Report that the global POC directory can facilitate the implementation of other CBMs at the global level that could help to promote an open, secure, stable, accessible, and peaceful ICT environment.

This working paper strives to further advance the elaboration of a first set of CBMs at the global level by drawing on already existing regional practice in the implementation of four CBMs drawn from the Final Report of the 2021 Open-ended Working Group and the first and second APRs of the OEWG which have been included in Annex B of the 2023 Annual Progress Report.

This paper is meant to give a more practical angle to the discussion in upcoming OEWG sessions and serve as encouragement for UN member states less familiar with CBM implementation so far.

Chile would like to share the following experience with the implementation of a regional CBM focusing on nominating a national Point of Contact as mentioned in CBM 1 b) of Annex B of the Annual Progress Report 2023:

Since 2018, Chile has nominated PoCs at the political and diplomatic level, as part of the mandate of cyber CBM 2 ("*Identify a national point of contact at the political level to discuss the implications of hemispheric cyber threats*") of the Organization of American States (OAS) and CBM 3 ("*Designate points of contact, if they do not currently exist, in the Ministries of Foreign Affairs with the purpose of facilitating work for cooperation and international dialogues on cybersecurity and cyberspace*"). Chile keeps updated that information at the OAS and it is available at the OAS Cyber CBMs Portal (https://www.oascybercbms.org/). The PoCs have contributed to the exchange of information, strengthening cooperation on capacity-building and technical assistance, coordinating policies and positions with other states on multilateral and regional processes, responding to queries and requirements from other states and international stakeholders, requesting information on cyber-attacks and strengthening bilateral relations, among others. At the technical level, Chile is part of the CSIRT America, which operates in the OAS.

Colombia would like to share the following experience with the implementation of a regional CBM focusing on communication checks in the form of "Ping" tests as mentioned in CBM 1 c) i) of Annex B of the Annual Progress Report 2023:

The Member States of the Inter-American Committee Against Terrorism (CICTE) of the OAS, in 2017 created the *Working Group on Cooperation and Confidence Building Measures in Cyberspace*, through resolution CICTE/RES.1/17, with the purpose of enhancing interstate cooperation, transparency, predictability, and stability online.

One of the first measures adopted by this Working Group was the identification of National Points of Contacts (PoCs) at the political level to discuss the implications of hemispheric cyber threats. This initiative was followed by the establishment of CBMs PoCs in Ministries of Foreign Affairs, with the main purpose of strengthening cooperation on cyber diplomacy and facilitating international dialogue.

In order to confirm that the Cyber CBMs PoCs are active and able to respond in a timely manner through this communication channel, the CICTE/OAS Secretariat has been conducting regular “ping tests”. The last test was carried out during the Fourth Session of the OEWG, on March 9, 2023. According to the information provided by the Secretariat, all 22 PoCs from OAS Member States responded to this test, which shows its relevance, applicability**,** and success. Colombia has nominated its CBMs PoCs and has successfully participated in these tests.

Germany would like to share the following experience with the implementation of a regional CBM focusing on voluntary information-sharing, including in the event of an urgent or significant ICT incident, facilitated through the global POC directory as mentioned in CBM 1 c) ii) of Annex B of the Annual Progress Report 2023:

Starting in May 2022 Germany has shared information on major cyber incidents with participating states of the Organisation for Security and Cooperation in Europe (OSCE) based on CBM eight – „Nomination of national focal points to raise concerns and communicate through“ – of the OSCE. CBM eight is the most widely accepted CBM of the OSCE having been adopted by 56 of the 57 OSCE participating states.

Germany chose to share information via this platform in order to contribute to the implementation of related OSCE CBMs, namely CBM two on facilitating cooperation, CBM five on using the OSCE as a platform for dialogue, CBM seven on information exchange on national updates, CBM fifteen on enhancing protection of critical infrastructure and CBM sixteen on reporting vulnerabilities.

The overarching objective of sharing information via the OSCE CBM platform was to activate a channel for information sharing on major cyber incidents at a time of heightened geopolitical tensions in the OSCE area – a channel, which might contribute to de-escalation in the event of significant malicious crossborder cyber activity.

Germany has repeatedly informed OSCE participating states about major cyber incidents since, also using the confidential designated *OSCE Communication Network* based on OSCE CBM thirteen. Germany has also used this network to

inform about mitigation measures put in place in response to the respective cyber incidents.

Uruguay would like to share the following experience regarding the implementation of a regional CBM focused on the nomination of a national Point of Contact as mentioned in CBM 1 b) of Annex B of the Annual Progress Report 2023:

Since 2018, Uruguay has nominated at the Organization of American States (OAS) a PoC at the technical level, as stated in CBM 1 and 2. Uruguay keeps such information updated at the OAS and it is available on the OAS Cyber CBMs Portal (https://www.oascybercbms.org/).

Our cooperation has been carried out by sharing experience at both strategic and technical levels. At the technical level, Uruguay is part of the CSIRT America, which operates in the OAS. Within this framework, Uruguay is working towards sharing indicators of compromise (IoC). At the strategic level, Uruguay has received several delegations from countries in the region. During those visits Uruguay shared the country's experience in digital government and cybersecurity in particular.

In addition, Uruguay is a member of various regional and international groups such as Digital Nations, GFCE, RedGealc and LAC4. In all these organizations, Uruguay promotes the exchange of good practices and experiences.

Singapore would like to share the following experience within the Association of Southeast Asian Nations (ASEAN) with the implementation of a regional CBM focusing on mechanisms for regular cross-regional exchanges of lessons and good practices on CBMs, taking into account differences in regional contexts and the structures of relevant organizations as mentioned in CBM 2 b) of Annex B of the Annual Progress Report 2023:

ASEAN sees CERT to CERT cooperation and exchanges as an important confidence building measure in the region. It is taking steps to strengthen regional CERT to CERT cooperation and capacity building initiatives to enhance the region’s collective cybersecurity. In 2021, the ASEAN Digital Ministers’ Meeting welcomed the proposal for the establishment of an *ASEAN Regional CERT Information Exchange Mechanism*. Earlier this year, the *Operational Framework for an ASEAN Regional CERT* was endorsed, and members are now deliberating on the funding model for this initiative.

Singapore is working with other ASEAN Member States in establishing an ASEAN Regional CERT, which aims to promote and facilitate information sharing related to cyber incident response to complement the operational mandate exercised by individual national CERTs in each ASEAN Member State. The CERT-CERT exchanges will further complement the ASEAN Cyber POCs Directory established in 2020 through a proposal spearheaded by Malaysia and Australia as part of the CBMs effort in the ASEAN Regional Forum. Nomination of POCs to the directory occurs on a voluntary basis and is updated and ping-tested biannually.

Besides CERT to CERT cooperation, there is also regular dialogue among ASEAN Member States on cybersecurity issues through a variety of platforms including the annual ASEAN Ministerial Conference on Cybersecurity, the ASEAN Cybersecurity

Coordinating Committee, and the ASEAN Network Security Action Council. These platforms and peer-learning opportunities built into cyber capacity building programmes delivered at the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) allow ASEAN members to exchange perspectives on the rapidly changing cyber landscapes, as well as to discuss newly evolving threats, including continuing the coordinated ASEAN approach to address common threats.

These mechanisms, such as CERT to CERT cooperation and regular dialogue, help to foster regular exchange of lessons and good practices at the regional level, while taking into account differences in national contexts.

Australia would like to share the following experience with the implementation of a regional CBM focusing on sharing information, on a voluntary basis, including concept papers, national strategies, policies and programmes and information on transparency measures, as mentioned in CBM 3 of Annex B of the Annual Progress Report 2023:

On 22 November 2023, the Australian Government released its new 2023-2030 Cyber Security Strategy. The Strategy is a road map to improving our resilience and strengthening our response to cyber security threats, and sets the agenda for Australia's cyber security policy to 2030, including our international ambitions of advocating for rules, norms and standards that are consistent with our shared interests and values.

Australia's 2016 Cyber Security Strategy, 2016 Defence White Paper, 2017 Foreign Policy White Paper, 2017 International Cyber Engagement Strategy and its 2019 Progress Report and 2021 International Cyber and Critical Tech Engagement Strategy are all examples of Australian transparency measures as they clearly explain our goals, visions and planned actions.

Australia has also committed to periodically publishing its position on the application of international law to state conduct in cyberspace (most recently in 2021). By publishing these views, Australia seeks to promote common understanding, increase predictability, foster trust and reduces the risk of miscommunication during times of conflict.

Czechia would like to share the following experience with the implementation of a regional CBM focusing on sharing concept papers, national strategies, policies and programmes, as well as information on ICT institutions and structures with relevance to international security as mentioned in CBM 3 c) of Annex B of the Annual Progress Report 2023:

Czechia publishes all relevant national cybersecurity documents (inter alia national strategies, policies, legislation, or information about institutional frameworks) on the website of the National Cyber and Information Security Agency (NÚKIB). The majority of these documents are translated into English in order to facilitate information sharing with international partners.

In addition, Czechia shares relevant national cybersecurity documents within the regional groups that Czechia is part of, namely in the OSCE. The OSCE has developed a platform with restricted access reserved for the exclusive use by

participating states. Within this platform, Czechia voluntarily shares and regularly updates relevant information such as the act on cybersecurity, national strategy and its action plan, institutional establishment, and other important information regarding cybersecurity. Czechia is convinced that the Global PoC Directory and its portal could play a very similar role for UN member states in the future.

The Netherlands would like to share the following experience within the OSCE with the implementation of a regional CBM focusing on the development and implementation of CBMs, including on the potential development of additional CBMs as mentioned in CBM 4 c) of Annex B of the Annual Progress Report 2023:

The OSCE adopted its first set of Cyber CBMs in 2013.The first set of CBMs consisted of eleven transparency measures. The eleven CBMs encompassed various aspects, including the exchange of information on (inter)national cyber threats, incidents, national cyber agencies (including contact details), strategies, measures, and programs. This also involved public-private cooperation, best practices, and opportunities for consultation to mitigate risks of misperception and miscommunication. The second set of OSCE CBMs was adopted in 2016 and consisted of five co-operative measures. The five CBMs covered elements such as the protection of critical infrastructure, strengthening mutual cooperation, and exchanging information through seminars, roundtables, and workshops.

The implementation of the CBMs is actively promoted by sharing national updates within the OSCE Informal Working Group on Cyber. This ongoing exchange, which includes best practices and lessons learned, supports all participating States in their implementation efforts. Furthermore, through the *adopt-a-CBM initiative*, almost all participating States have actively engaged in the implementation of a specific CBM. For example, with the OSCE Secretariat and a number of States, the Netherlands is involved in the further implementation of CBM16 ("*Coordinated Vulnerability Disclosure*") through e-learning modules, policy papers and the organization of workshops to enhance national capacities and cybersecurity skills.

Mexico would like to share the following experience within the OAS with the implementation of a regional CBM focusing on the development and implementation of CBMs, including on the potential development of additional CBMs as mentioned in CBM 4 c) of Annex B of the Annual Progress Report 2023:

Within the framework of the OAS, Mexico has promoted, together with the member states, the regional implementation of CBMs, as well as the norms and principles adopted by the UN, relying on cyber-diplomacy and multilateralism as ideal tools for conflict prevention and the peaceful and responsible use of ICTs.

The Working Group on Cooperation and Confidence-Building Measures focused on studying what additional CBMs would be needed to strengthen security, including greater agility in responding to cyber incidents. In 2022 this effort led to the adoption of five new regional CBMs related to the gender dimension and the substantive participation of women in decision-making processes, the study of the application of international law to cyberspace, the systematic reporting of progress in the implementation of norms, multistakeholder participation, and the development of cyber-risk schemes.

Similarly, as referred to previously in the document, the Group adopted recommendations to continue work on the optimal functioning of the OAS CBMs portal and the PoCs portal, capacity building among PoCs by the Inter-American Juridical Committee and the International Committee of the Red Cross as well as on cyber diplomacy and International Humanitarian Law, greater collaboration with UNODA and UNIDIR. The Group also issued a recommendation to study how the Inter-American Committee against Terrorism could act as a "first responder" in the event of a serious cyber incident.

Canada would like to share the following experiences within the OAS and the OSCE with the implementation of a regional CBM focusing on the development and implementation of CBMs, including on the potential development of additional CBMs as mentioned in CBM 4 c) of Annex B of the Annual Progress Report 2023:

Canada strongly supports the set of 16 Cyber CBMs adopted by the OSCE's participating States. This year, we celebrate the tenth anniversary of OSCE cyber/ICT security confidence-building measures. We praise the efforts undertaken across the OSCE area on the implementation of these measures and the lessons learned in this process. In this context, Canada is championing OSCE's CBM 4, which states that "*Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure and reliable Internet*". To this end, we encourage further discussion on sharing national measures, best practices and lessons learned in implementing initiatives to promote an open, secure, reliable and interoperable Internet.

In the context of the Organization of American States (OAS), Canada has been actively supporting the development of CBMs by the OAS Inter-American Committee Against Terrorism (CICTE). The development of CBMs has allowed OAS member states to enhance interstate cooperation, transparency, predictability and stability online. Recently, Canada, along with other regional partners, has promoted the development of additional CBMs at the OAS, on the following topics: Gender, International Law, implementation of the 11 non-binding voluntary norms and stakeholder participation.

Annex B of the 2023 Annual Progress Report of the OEWG:
Initial List of Voluntary Global CBMs

CBM 1. Nominate national Points of Contact to the global POC directory, and operationalize and utilize the global POC directory

a) States agree to establish, building on work already done at the regional level, a global, intergovernmental, points of contact directory. At the fourth and fifth sessions of the OEWG, States to engage in further focused discussions on the development of such a directory, on a consensus basis, as well as engage in discussions on initiatives for related capacity-building, taking into account available best practices such as regional and sub-regional experiences where appropriate.
[First APR of the OEWG, CBM section, Recommended Next Steps, paragraph 2]

b) States, which have not yet done so, consider nominating a national Point of Contact, inter alia, at the technical, policy and diplomatic levels, taking into account differentiated capacities. States are also encouraged to continue to consider the modalities of establishing a directory of such Points of Contact at the global level.
[2021 OEWG report, paragraph 51]

c) States are encouraged to operationalize and utilize the global POC directory in the following ways:

i) Communication checks in the form of "Ping" tests;
ii) Voluntary information-sharing, including in the event of an urgent or significant ICT incident, facilitated through the global POC directory;
iii) Tabletop exercises to simulate practical aspects of participating in a POC directory; and
iv) Regular in-person or virtual meetings of POCs to share practical information and experiences on the operationalization and utilization of the POC directory on a voluntary basis.
v) Utilize the POC directory to establish communication between POCs, in accordance with the modalities of the POC directory.

CBM 2. Continue exchanging views and undertaking bilateral, sub-regional, regional, cross-regional and multilateral dialogue and consultations between States.

a) States concluded that the dialogue within the Open-ended Working Group was in itself a CBM, as it stimulates an open and transparent exchange of views on perceptions of threats and vulnerabilities, responsible behaviour of States and other actors and good practices, thereby ultimately supporting the collective development and implementation of the framework for responsible State behavior in their use of ICTs.
[2021 OEWG report, A/75/816, paragraph 43]

b) States explore mechanisms for regular cross-regional exchanges of lessons and good practices on CBMs, taking into account differences in regional contexts and the structures of relevant organizations.
[2021 OEWG report, A/75/816, paragraph 52]

c) States continue to consider CBMs at the bilateral, regional, and multilateral levels and encourage opportunities for the cooperative exercise of CBMs.
[2021 OEWG report, paragraph 53]

d) States continued to emphasize that the OEWG itself served as a CBM.
[First APR of the OEWG, paragraph 16(e)]

CBM 3. Share information, on a voluntary basis, such as national ICT concept papers, national strategies, policies and programmes, legislation and best practices, on a voluntary basis

a) States, on a voluntary basis, continue to inform the Secretary-General of their views and assessments and to include additional information on lessons learned and good practice related to relevant CBMs at the bilateral, regional or multilateral level. **[2021 OEWG report, paragraph 48]**
b) States voluntarily engage in transparency measures by sharing relevant information and lessons in their chosen format and fora, as appropriate, including through the Cyber Policy Portal of the United Nations Institute for Disarmament Research. **[2021 OEWG report, paragraph 50]**
c) States are encouraged to continue, on a voluntary basis, to share concept papers, national strategies, policies and programmes, as well as information on ICT institutions and structures with relevance to international security, including through the report of the Secretary-General on developments in the field of information and communication technologies in the context of international security as well as the UNIDIR Cyber Policy Portal as appropriate. **[First APR of the OEWG, CBM section, Recommended Next Steps, paragraph 5]**
CBM 4. Encourage opportunities for the cooperative development and exercise of CBMs
a) States voluntarily identify and consider CBMs appropriate to their specific contexts, and cooperate with other States on their implementation. **[2021 OEWG report, paragraph 49]**
b) States continue to consider CBMs at the bilateral, regional and multilateral levels and encourage opportunities for the cooperative exercise of CBMs. **[2021 OEWG report, paragraph 53]**
c) States continue exchanging views at the OEWG on the development and implementation of CBMs, including on the potential development of additional CBMs. **[First APR of the OEWG, CBM section, Recommended Next Steps, paragraph 1]**