MEMORANDUM OF UNDERSTANDING
ON COOPERATION IN CYBERSECURITY
BETWEEN
THE GOVERNMENT OF THE REPUBLIC OF CHILE
AND
THE GOVERNMENT OF THE REPUBLIC OF ESTONIA

The Government of the Republic of Chile and the Government of the Republic of Estonia, hereinafter referred to as "the Participants";

ACKNOWLEDGING the importance of cyberspace and its positive impact on the economic and social development of countries, as well as the increasing use by the States of information and communication technologies (ICT), networks, information systems and related technology, integrated to the Internet global network;

CONSIDERING that the threats to cyberspace security, particularly cyberattacks promoted by other States, and increasing threats by third parties endanger the critical infrastructure of countries, their economic development and the welfare of people;

CONVINCED THAT the common purpose of Chile and Estonia is to promote a free, open, safe, reliable, resilient cyberspace which fosters innovation and can be used as a tool for economic and social development of both countries and the promotion of human rights;

RESOLVED TO expand and strengthen bilateral coordination and cooperation between Chile and Estonia, promoting joint initiatives in the field of cyberspace and cybersecurity, as well as the exchange of good practices, development and implementation of domestic strategies, responses to cyberspace incidents, drafting of laws, protocols, exchange of information, personnel, education and training, development of domestic capacities, institutional agreements, among others.

HAVE ACCEPTED THE FOLLOWING:

CLAUSE 1
Objective

This Memorandum of Understanding is aimed at providing reciprocal cooperation on cybersecurity matters of common interest to both Participants and promoting coordination between them.

CLAUSE 2
Binational Working Group on Cyberspace and Cybersecurity

To accomplish the objective in Clause 1 above, the Participants may establish a Binational Working Group on Cyberspace and Cybersecurity.

The Binational Working Group will have the following duties:

(a) To prepare political and strategic policies for coordination and cooperation between both Participants;

(b) To establish an annual work plan and set priorities on cybersecurity and cyberspace cooperation matters;

(c) To analyse and discuss the current and future status of cybersecurity policies at a global, regional, multilateral and bilateral level;

(d) To identify and propose specific cooperation measures;

(e) To facilitate and supervise cooperation work in all areas, as well as agreements and initiatives to be established between both Participants;

(f) To invite representatives from the private sector, civil society and academic world to participate in cooperation activities;

(g) Other duties as may be agreed upon by the Participants within the framework of this Memorandum of Understanding.

The Binational Working Group will be presided by such authorities as may be determined by the Participants and will hold meetings in person or by videoconference, as frequently as agreed upon by the Participants.

CLAUSE 3
Coordination and cooperation

In furtherance of the objectives in Clause 1 above, the Participants may develop coordination and cooperation initiatives and actions in the following areas:

(a) To promote joint work in international agencies and fora on cyberspace and cybersecurity by supporting and actively participating in initiatives and coordinating positions by both countries;

(b) To agree upon common positions and actions at a global level;

(c) To promote and strengthen work and cooperation in the combat against cybercrime by national agencies of both countries, supporting negotiation and adoption of international agreements on the matter;

(d) To promote the adoption of measures to increase cyberspace confidence and reliability, at a global, regional and bilateral level;

(e) To foster the establishment of bilateral information channels, detection and response;

(f) To promote the conclusion of agreements with governments, the private sector, civil society and universities;

(g) To promote cooperation in the development of cybersecurity, cyber-intelligence and cybercrime combat policies and strategies;

(h) To promote and develop cooperation in education, training, upskilling and creation of national capacities;

(i) To foster cybersecurity promotion and dissemination activities.

The Participants will appoint persons of contact (POC) to facilitate, monitor and review the implementation of this Memorandum.

The Participants may invite other institutions, including from private sector and non-governmental sector, or other levels of government, to participate in the work and assign them responsibility for the implementation of particular activities.

The effective implementation may include, *inter alia*, evaluation, pre-qualification and nomination of suitable private companies or other institutions or experts from their respective countries to implement as well as partner and collaborate in development projects both countries.

CLAUSE 4
Cooperation methods and forms

Cooperation between the Participants may be provided in the following ways:

(a) Exchanging information, to the exclusion of issues on information marked as confidential, according to the Participants' relevant laws on the protection of personal data and confidentiality of information. Each Participant will protect the information exchanged by the relevant law enforcement agencies or entities against non-authorized access and disclosure. Exchanged information, according to the provisions of this Memorandum, may not be remitted to a third party without the written consent of the other Participant;

(b) Developing training, programs;

(c) Cooperating and providing information between national CSIRTs or CERTs;

(d) Establishing official channels for the exchange of information on cybersecurity threats and incidents affecting critical infrastructure and/or key resources of both States in such areas;

(e) Appointing national focal points, which will coordinate the preparation of plans of action and education, upskilling implement proposals contained in this document;

(f) Participating in technical cooperation and training programs on cybersecurity and protection of critical infrastructure of the Participants as well as training programs, research, conferences and other activities on the matter;

(g) Exchanging publications, papers, academic material and forensic information in case of similar cyberattacks having affected or threatened to affect any agency in either State;

(h) Exchanging information to prevent, mitigate or neutralize threats or cyberattacks that may be originated in Chile or Estonia against assets located in each State, whether public or private, even to strengthen criminal prosecution and related extraditions;

(i) Jointly assessing – with due observance to their internal laws and regulations – the feasibility of generating a computer mechanism to consult criminal and police information with a view to improving the prevention and punishment of transnational crimes;

(j) Fostering political and technical coordination in multilateral instances connected with cybersecurity matters;

(k) Promoting the granting of scholarships for student, professor and technical staff exchange in order to carry out internships, research and development activities in cybersecurity;

(l) Cooperating in other areas, to be determined by mutual agreement, on cybersecurity, to the extent that legal or contractual duties by either Participant are not adversely affected;

(m) Any other cooperation form the Participants may agree upon.

CLAUSE 5
Financial Considerations

The implementation of cooperation actions under this Memorandum of Understanding will be subject to the availability of financial and human resources by each Participant.

Expenses to be incurred to implement this Memorandum of Understanding will be conditioned upon the annual availability of funds by the Participants, according to their respective laws and regulations.

CLAUSE 6
Nature of the instrument

The Participants leave on record that this Memorandum of Understanding is not legally binding and does not give rise to rights or obligations; it is a political and technical undertaking by both Participants to explore mutual cooperation ways on the matter.

The cooperation mechanisms, projects and activities to be developed or implemented within the framework of this document will be laid down by separate instruments to be negotiated by the Participants where deemed appropriate.

CLAUSE 7
Change or amendment

Any change or amendment to be made as a result of the development or implementation of this Memorandum of Understanding will be agreed upon by mutual consent of the Participants. Amendments will become effective in accordance with Clause 9.

CLAUSE 8
Settlement of disputes

Any dispute that may arise about the implementation and/or interpretation of this Memorandum of Understanding will be settled by the Participants on the basis of good faith and by deploying, to such effect, their best efforts.

CLAUSE 9
Effectiveness, duration and termination

This Memorandum of Understanding will become effective on the date of signing and will have an indefinite duration. Either Participant may terminate this Memorandum of Understanding at any time, by sending a written notice to the other Participant at least six (6) months in advance.

The termination of this Memorandum of Association will not affect any ongoing projects and initiatives agreed upon during its life, unless otherwise agreed upon by the Participants.

SIGNED at Santiago, Chile, on this 16 January, 2020, in two counterparts, in the English language.

FOR THE GOVERNMENT OF THE REPUBLIC OF CHILE

FOR THE GOVERNMENT OF THE REPUBLIC OF ESTONIA