MEMORANDUM OF UNDERSTANDING
ON COOPERATION IN CYBERSECURITY
BETWEEN
THE GOVERNMENT OF THE REPUBLIC OF CHILE
AND THE GOVERNMENT OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND

The Government of the Republic of Chile and the Government of the United Kingdom of Great Britain and Northern Ireland hereinafter referred to as "the governments or 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 conducted 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 Chile and the United Kingdom common purpose is to promote a free, open, peaceful and secure cyberspace, where rights apply online as they do offline, and respond and deter those who threaten democracy;

RESOLVED TO expand and strengthen bilateral coordination and cooperation between Chile and the United Kingdom, promoting joint initiatives in the field of cybersecurity/defence, as well as the exchange of best practices, development and implementation of domestic strategies, responses to cyberspace incidents, drafting of laws, protocols, exchange of information, personnel, development of domestic capacities, institutional arrangements or understanding, among others.

HAVE DECIDED AS FOLLOWS:

ONE

Purpose

This Memorandum of Understanding is aimed at providing reciprocal cooperation on cybersecurity/defence matters of common interest to both governments or participants and promoting coordination between them.

TWO

Binational Working Group on Cyberspace and Cybersecurity

To accomplish the object in ONE above, the governments or participants may establish a Binational Working Group on cyberspace and cybersecurity/defence.

The Binational Working Group may decide the following:

(a) To prepare political and strategic policies for coordination and cooperation between both governments or participants;

(b) To establish an annual work plan and set priorities on cybersecurity/defence, 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 arrangement or understanding and initiatives to be established between both governments or participants;

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

(g) To promote the responsible state behaviour in cyberspace, in line with the 2010, 2013 and 2015 report recommendations of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of

International Security (A/65/201, A/68/98, A/70/174).

(h) Other duties as may be accepted, approved or decided upon by the within the framework of this Memorandum of Understanding.

The Binational Working Group may decide to be presided by such authorities as determined by the governments or participants and will or decide to hold meetings in person or by videoconference, as frequently as decided upon.

THREE

Nature of Cooperation

In furtherance of the object in ONE above, the governments or 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, cybersecurity/defence, by supporting and actively participating in initiatives and coordinating positions by both countries;

(b) To promote and strengthen work and cooperation to combat cybercrime by national agencies of both countries, and to support international collaboration to tackle this threat;

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

(d) To promote the conclusion of arrangements or understandings with governments, the private sector, civil society and universities;

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

(f) To exchange information, to the exclusion of issues on information marked as confidential, in accordance with the governments or participants' relevant laws on the protection of personal data and confidentiality of information. Each Party will or decide to protect the information exchanged by the relevant 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 Party, except where required by law.

(g) To cooperate and provide information between national CSIRTs or CERTs. Establishing official relations between both States, mainly focused on the exchange of information on cybersecurity/defence and incidents affecting critical infrastructure and/or key resources of both States in such areas.

(h) To participate in technical cooperation and training programs on cybersecurity/defence and protection of critical infrastructure of the governments or participants as well as training programs, research, conferences and other activities on the matter;

FOUR

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 Party.

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

FIVE

Nature of the instrument

The governments or participants leave on record that this Memorandum of Understanding is not legally binding and does not give rise to benefits or commitments; it is just a political and technical arrangement or understanding by both governments or 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 be laid down by separate instruments to be negotiated where deemed appropriate.

SIX

Change or amendment

Any change or amendment to be made as a result of the development or implementation of this Memorandum of Understanding will or decide be agreed upon by mutual consent of the governments or participants. Amendments will become effective in accordance with paragraph EIGHT

SEVEN

Settlement of disputes

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

EIGHT

Effectiveness, duration and termination

This Memorandum of Understanding will become effective on the date of signature indicated herein and will remain in effect for a period of five (5) years thereafter, unless terminated by either Party giving at least one (1) month's prior notice in writing to the other Party.

The termination of this Memorandum of Understanding will not affect any ongoing projects and initiatives accepted, approved or decided upon during its life, unless otherwise accepted, approved or decided upon by the governments or participants.

SIGNED in London, United Kingdom, on 10 September 2019, in duplicate, in the English language.

For the Government of the
Republic of Chile

For the Government of the
United Kingdom of Great Britain and
Northern Ireland