130th ASSEMBLY OF THE INTER-PARLIAMENTARY UNION AND RELATED MEETINGS
Geneva, 16 – 20.3.2014

Assembly A/130/2-P.1
Item 2 10 December 2013

CONSIDERATION OF REQUESTS FOR THE INCLUSION OF AN EMERGENCY ITEM IN THE ASSEMBLY AGENDA

Request for the inclusion of an emergency item in the agenda of the 130th Assembly of the Inter-Parliamentary Union submitted by the delegation of Uruguay

On 9 December 2013, the President of the IPU received from the President of the General Assembly and of the Senate and President of the IPU Group of Uruguay a request for the inclusion in the agenda of the 130th Assembly of an emergency item entitled:

"Cyber warfare – A serious threat to peace and global security".

Delegates to the 130th Assembly will find attached the text of the communication submitting the request (Annex I), as well as an explanatory memorandum (Annex II) and a draft resolution (Annex III) in support thereof.

The 130th Assembly will be required to take a decision on the request of the delegation of Uruguay on Monday, 17 March 2014.

Under the terms of Assembly Rule 11.1, any Member of the IPU may request the inclusion of an emergency item in the Assembly agenda. Such a request must be accompanied by a brief explanatory memorandum and a draft resolution which clearly define the scope of the subject covered by the request. The Secretariat shall communicate the request and any such documents immediately to all Members.

Furthermore, Assembly Rule 11.2 stipulates that:

(a) A request for the inclusion of an emergency item must relate to a major event of international concern on which it appears necessary for the IPU to express its opinion. Such a request must receive a two-thirds majority of the votes cast in order to be accepted;
(b) The Assembly may place only one emergency item on its agenda. Should several requests obtain the requisite majority, the one having received the largest number of positive votes shall be accepted;
(c) The authors of two or more requests for the inclusion of an emergency item may combine their proposals to present a joint one, provided that each of the original proposals relates to the same subject;
(d) The subject of a proposal that has been withdrawn by its authors or rejected by the Assembly cannot be included in the draft resolution submitted on the emergency item, unless it is clearly referred to in the request and title of the subject adopted by the Assembly.

COMMUNICATION ADDRESSED TO THE PRESIDENT OF THE IPU BY THE PRESIDENT OF THE GENERAL ASSEMBLY AND OF THE SENATE, AND PRESIDENT OF THE IPU GROUP OF URUGUAY

Montevideo, 6 December 2013

Dear Mr. President,

In accordance with the relevant provisions of the Inter-Parliamentary Union, in particular Assembly Rule 11.1, the IPU Group of Uruguay would like to request the inclusion of an emergency item in the agenda of the 130th IPU Assembly, to be held in Geneva, Switzerland, from 16 to 20 March 2014, entitled:

"Cyber warfare – A serious threat to peace and global security".

Please find attached an explanatory memorandum as well as a draft resolution in support of this request.

I would kindly ask you to circulate this request to the Members of our Organization.

Please accept, Mr. President, the assurance of my highest consideration.

(Signed) Danilo ASTORI
President of the General Assembly
and of the Senate and
President of the IPU Group of Uruguay

A/130/2-P.1
ANNEX II
Original: Spanish

CYBER WARFARE – A SERIOUS THREAT TO PEACE AND GLOBAL SECURITY

Explanatory memorandum submitted by the Inter-Parliamentary Group of Uruguay

The Inter-Parliamentary Group of Uruguay wishes to propose the inclusion of an emergency item in the agenda of the 130th IPU Assembly, entitled "Cyber warfare – A serious threat to peace and global security" for the reasons provided below.

At the IPU Assembly held in Quito, Ecuador, the Uruguayan delegation had proposed this topic to the Committee on United Nations Affairs, considering it sufficiently important to be addressed. We had already stated then that "in recent times we have been witnessing a dramatic increase in information on what can be called cyber warfare".

Government after government has been denouncing cyber attacks on their corporate or military facilities, sometimes even vaguely pointing the finger at certain States. It is clear that public condemnation of such acts are part of the consequences of these acts, but are not reprimands per se of this type of practice. In general, these condemnations are not based on ethics or principles but rather, as we said, are indictments on their effects, their ramifications.

A large share of these practices is not revealed to the public because what we are dealing with here are secret activities.

The actual dimensions of the issue we are proposing today are but the tip of a gigantic iceberg.

Moreover, we should reflect on one fact: many international media reports assume that these activities are a "natural" continuation of military activities, which brings us to the crux of the matter: we should not assume that these are natural or even legitimate activities.

We believe that given the magnitude of the problem, the Inter-Parliamentary Union should take a proactive approach, debate cyber warfare and issue a statement on behalf of the world's parliamentarians against this activity, which affects not only peace and global security and their implications for States, but also civil society in its entirety, the economy, science and culture globally. After all, very soon, the world's critical infrastructure will be based on information platforms, with everything that implies.

Given this situation, the international community should have sufficient legal guarantees to criminalize and punish such activities that often attack installations in any part of the world.

Now would be a good time to ask ourselves these questions: Who can guarantee that the "weapons" that governments and private technology firms are developing today will not fall into the hands of criminal organizations as is currently the case with conventional weapons? How can the problems associated with this new "invisible" and "intangible" war that deviates from traditional forms of expression and eludes detection be managed in terms of global policy?

Information-related crime is clearly not new. In fact, this is a growing problem that requires urgent and rigorous action by multilateral institutions.

The sheer magnitude of events such as those that have occurred over the past months leave us vulnerable. The blow was so heavy that even the Head of the International Telecommunications Union (ITU), Mr. Hamadoun Touré, declared "There is a cyberwar going on" in reference to the inter-State espionage denounced by Edward Snowden. He went even further, proposing a cyber peace treaty.

In much the same way as there are conventions prohibiting and punishing the use of chemical or nuclear weapons, for example, or others protecting human rights or the environment, it seems that the time has come to work towards what we are proposing.

History shows that 200 years ago slavery was not considered morally reprehensible, neither was homophobia until very recently. What must not be allowed to happen is a situation where espionage, in this case cyber espionage, which involves invading and altering the lives of nations and persons, is not condemned. Worse still, a situation where it is not seen as the serious problem it really is.

The Inter-Parliamentary Group of Uruguay proposes that the IPU include this item in the agenda of its 130th Assembly and that it invest all its technical and political resources into addressing cyber warfare, which is so crucial to peace and global security. It should be stressed that maintaining world peace has been one of the central objectives of the Inter-Parliamentary Union since its inception in 1889.

A/130/2-P.1
ANNEX III
Original: Spanish

CYBER WARFARE – A SERIOUS THREAT TO PEACE AND GLOBAL SECURITY

Draft resolution submitted by the Inter-Parliamentary Group of URUGUAY

The 130th Assembly of the Inter-Parliamentary Union,

(1) Deeply concerned by the recent occurrences involving acts of cyber espionage, including accusations of cyber attacks among States, on civil society and on the information platform that supports industrial and commercial production, tourism, science and culture at the global level,

(2) Alarmed at the global consequences generated by this escalation of acts denounced on a daily basis at the international level, especially the ramifications these may have for peace and security in the world,

(3) Considering that the onus is on us, parliamentarians – as representatives of the people – to work for the protection of privacy and security of persons, not only of States,

(4) Bearing in mind the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, in which the protection of individuals in the enjoyment of the rights to freedom and privacy are enshrined, and which prohibit any arbitrary interference with their privacy,

(5) Reaffirming the need to address the problem of cyber warfare from a global perspective, and supporting the call made by the International Telecommunications Union (ITU) to negotiate a cyber peace treaty in order to avert criminal activities that jeopardize the physical integrity of individuals, cause material damage and gravely interfere with States' cyber infrastructure,

(6) Reiterating the need to take urgent action in order to curb this problem of growing magnitude,

1. Expresses its deep concern over publicly known acts related to cyber espionage that reportedly involve nations which, to defend their own interests, are resorting to methods that defy the most elementary standards of civilized relations among States, and which may jeopardize the civil rights of citizens across the world;

2. Is very worried by recent events of cyber espionage, including accusations of cyber attacks not only on civil society but also on the information platform supporting industrial and commercial production, tourism, science and culture at the global level;

3. Welcomes the initiative proposed at the United Nations to promote a convention on the protection of the rights of nations to security and sovereignty and the rights of persons to privacy and liberty through new legal instruments;

4. Invites all parliaments and the IPU to participate in efforts spearheaded by the United Nations and its specialized agencies, in particular ITU, aimed at galvanizing political will to develop instruments aimed at inculcating a culture of peace and condemning cyber warfare and its effects, it being understood that the development of international law instruments resulting in an institutional framework to combat cyber warfare is an approach that must go hand in hand with other actions to change cultural perceptions and values about the rights of persons and nations.