Inter-Parliamentary Union
For democracy. For everyone.

132nd IPU Assembly

Hanoi (Viet Nam), 28 March - 1 April 2015

Standing Committee on
Peace and International Security

C-I/132/DR
15 January 2015

Cyber warfare: A serious threat to peace and global security

***Draft resolution* submitted by the co-Rapporteurs**
Mr. N. Lazrek (Morocco) and Mr. J.C. Mahía (Uruguay)

The 132nd Assembly of the Inter-Parliamentary Union,

(1) *Convinced* that, given the immense socio-economic benefits that cyberspace brings to all citizens around the world, predictability and stability in the cyber domain are essential,

(2) *Fully aware* that many concepts, definitions and standards of cyber policy, especially as they relate to international peace and security, are not commonly understood and are still being clarified at the national, regional and multilateral levels, and that international consensus still does not exist in some areas,

(3) *Acknowledging* that public international law as well as specific bodies of law and legal instruments, in particular the United Nations Charter, the Geneva Conventions and their Additional Protocols, the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, are relevant and applicable to the use of information and communication technologies (ICTs) by States and are essential to reducing risks, maintaining peace and international stability and promoting an open, secure, peaceful and accessible ICT environment,

(4) *Considering* that cyberspace is more than the Internet, and includes not only hardware, software, data and information systems, but also people and social interaction within these networks and the entire infrastructure/architecture;

(5) *Cognisant* of that the fact that different areas of cyber policy, while distinct, are inextricably linked and that decisions made in areas such as, but not limited to, Internet governance, impact international peace and security aspects of cyberspace,

(6) *Considering* that cyberspace can be understood to mean a new dimension of conflict as well as a new operating environment where many, if not most, cyber assets have both civilian and military applications,

(7) *Aware* that cyberspace is not an isolated domain and that destabilizing activities within it may trigger other forms of traditional insecurity or conflict,

(8) *Convinced* that, because of the interconnectivity of military and civilian computer networks, States should encourage the private sector and civil society to play an appropriate role to improve the security and use of ICTs, including supply chain security for ICT products and services; *also convinced* that that there is a need for regional and international cooperation/concerted action against threats resulting from the malicious use of ICTs,

(9) *Noting* that the use of ICTs has reshaped the international security environment and that while such technologies bring immense economic and social benefits they can also be used for purposes that are inconsistent with international peace and security; *also noting* that in recent years, the risk of ICTs being used to commit crimes and conduct disruptive activities by both State and non-State actors has significantly risen,

(10) *Considering* that cyber warfare may encompass, but is not necessarily limited to, operations against a computer or a computer system through a data stream as a means and method of warfare intended to cause death, injury, destruction or damage during armed conflicts,

(11) *Noting* that, even though cyber warfare has fortunately not led to dramatic humanitarian consequences thus far, the military realities of cyberspace and the impacts of specific activities are not yet fully understood, *also noting* that many cyber activities may destabilize the security situation in the cyber domain, even though these may not amount to “use of force”,

(12) *Acknowledging* that a lack of strategic State-to-State communications, prompt attribution of responsibility and a limited understanding of allies’ and adversaries’ priorities may lead to miscalculation, misconception and misunderstanding in the cyber domain,

(13) *Considering* that the absence of a common understanding on what is “acceptable” State conduct with regard to the use of ICTs increases the risk to international peace and security and that the development and spread of sophisticated malicious tools and techniques, by States or non-State actors, may further heighten the risk of mistaken attribution of responsibility and unintended escalation,

(14) *Condemning* the use by terrorist groups of ICTs to communicate, collect information, recruit, organize, plan and coordinate attacks, promote their ideas and actions and solicit funding,

(15) *Considering* that there is a need to strike a balance between security control of computers and communication systems and respect for individual privacy and State secret,

At the national level

1. *Recommends* that parliaments build their capacities to better understand the complex nature of international security in the cyber domain and to take into account the interlinkages between different areas of cyber policy development;

2. *Encourages* parliaments to work with other branches of government to develop a holistic understanding of cyber dependence, risks and challenges at the overarching national level;

3. *Calls upon* all parliaments to review their countries' legal framework to examine how best to adapt it to potential threats which might arise from the evolving nature of cyberspace;

4. *Encourages* parliaments to scrutinize public finances to ensure that adequate resources are allocated to cyber security and cyber defence, and that these funds are spent efficiently and effectively to meet intended targets;

5. *Also encourages* parliaments to make use of all the oversight tools at their disposal to ensure that cyber-related activities are rigorously monitored;

6. *Recommends* that parliaments from States which have not yet done so request that their respective governments expressly state that international law, including the law of armed conflict, must apply to cyber warfare in order to ensure that limits are placed on the use of cyber operations as a means and method of warfare while noting that the exact manner of application is still a matter under international discussion;

7. *Calls upon* all parliaments to ensure meaningful participation by the private sector and civil society in efforts aimed at addressing these challenges;

8. *Recommends* that parliaments ensure that appropriate distinctions are made in legislation between civilian and military cyber levels in order to reasonably restrict citizens' ability to make use of ICT tools;

At the international level

9. *Recommends* that at the legislative and executive levels, consideration be given to cooperative measures likely to enhance peace and international stability and security and lead to a common understanding of the application of relevant international law and derived standards, rules and principles underpinning the responsible conduct of States;

10. *Further recommends* that parliaments press for the formulation and adoption at the regional and international levels of practical confidence-building measures to help increase transparency, predictability and cooperation and reduce misconceptions, thus diminishing the risk of conflict;

11. *Urges* the IPU, together with relevant international organizations, to lend support to inter-parliamentary cooperation with a view to sharing of good practices on confidence-building measures that are conducive to peace and international stability and security;

12. *Encourages* parliaments to play a positive role in creating a secure environment in support of the peaceful use of cyberspace and ensure that the right balance is struck between freedom of speech and information exchange and the means required to guarantee security.