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/M
22 January 2015

Cyber warfare – a serious threat to peace and global security

***Explanatory memorandum* submitted by the co-Rapporteurs, Mr. N. Lazrek (Morocco) and Mr. J.C. Mahía (Uruguay)**

1. Over the past years, the increasing use of the Internet and interconnected computer systems has resulted in a sharp rise in the number of cyber attacks. Today, almost every political, economic or military conflict entails a cybernetic component. The term "cyber warfare" is regularly used by the media to describe various situations with multiple consequences that are not always encompassed by cyber warfare per se.

2. To draft the resolution, the co-Rapporteurs of the Standing Committee on Peace and International Security undertook first and foremost to make the distinction between cyber warfare and other elements of cyber security such as cyber crime, cyber terrorism and cyber espionage.

3. The latter are mainly caused by private actors (individuals, groups or companies), although States also can place companies and citizens under heavy surveillance. In all cases, these cyber threats target both national economies and individual privacy and have a direct impact on the public interest and the interest of nations. In the face of rapidly evolving technology, the legal approach to safeguarding privacy often falls behind, thus clearly illustrating the dilemma between the need to guarantee security on the one hand and to respect individuals' privacy and basic human rights on the other. The Standing Committee on Peace and International Security debated this topic in October 2014 within and the subject item chosen by the Standing Committee on Democracy and Human Rights for its next resolution, *Democracy in the digital era and the threat to privacy and individual freedoms* is also linked to this problem.

4. In their draft resolution, the co-Rapporteurs adhered to the initial subject item adopted by the Standing Committee, namely: *Cyber warfare: A serious threat to peace and global security*. To this end, they defined cyber warfare as war waged in cyberspace and consisting of mainly military activities using computer systems and networks to attack an adversary. They drew inspiration from the presentations made by experts and MPs at the panel discussion organized at the 131st IPU Assembly (Geneva, October 2014) and written input from IPU Member Parliaments received in the weeks that followed. The co-Rapporteurs would like to thank all those who made an input.

5. The draft resolution underscores the fact that, for the time being, the body of international law governing cyber space is still extremely opaque and there still is no commonly accepted definition by the entire spectrum of international stakeholders of what constitutes an "act of cyber warfare". This is despite the fact that several regional and multilateral organizations have started reflecting on the matter and various initiatives have been implemented at the national and multilateral levels, particularly at the United Nations.

6. The draft resolution is thus based on several assumptions. The first is the need to make the link between cyber warfare and the law of war in order to fill any legal loopholes, to categorize cyber attacks and better identify which of these can be considered acts of cyber warfare. Cyber attacks conducted during peace time without unleashing a war cannot in fact be described as cyber warfare. They can neither justify application of the law of war nor a military response. They can, however, lead to the implementation of non-military coercive measures in cyber space or in the real world, such as economic or commercial measures or boycotts. Cyber warfare can thus only be invoked when a cyber attack results in changing the situation from one of peace to one of war.

7. The co-Rapporteurs are nevertheless aware that the application of prevailing international law is by no means a perfect solution and, in many cases, this new stake for international security requires the amendment and different interpretation of existing rules if not the adoption of new rules entirely.

8. The second assumption is taking a step-by-step approach to the issue. As is the case for other topics of international scope such as nuclear disarmament, the involvement of parliaments in activities dealing with cyber warfare can hardly be limited to a single resolution. The draft resolution should be understood as a first step on a relatively new topic of which the international parliamentary community is taking note. As the topic is developed, subsequent resolutions will allow parliaments to update their knowledge and devise new strategies.

9. The third assumption is parliamentary action. It is quite clear that the majority of action on cyber warfare is the purview of governments. Nevertheless, members of parliament, as representatives of the people, can also play a pivotal role, in particular in striking a balance between national security, human security and individual freedoms. The co-Rapporteurs accordingly wanted this draft resolution to focus mainly on the roles parliaments could and should play, notably by using their law-making and oversight powers to ensure that governments honour their existing commitments and obligations or bring pressure to bear on them so as to encourage them to contribute to other concrete actions.

10. The draft resolution reflects the agreement reached by the co-Rapporteurs on a number of important questions and provides a solid basis for the debate that will take place at the 132nd IPU Assembly. The document that will be adopted at that Assembly will offer the possibility of making a vigorous parliamentary contribution to the definition and framing of cyber warfare, in particular through concrete measures that can be taken in the near future.