EU Statement – United Nations 1st Committee: Thematic Discussion on Other Disarmament Measures and International Security

New York, 26/10/2018 - 20:26, UNIQUE ID: 181026_26

Statements on behalf of the EU

26 October 2018, New York – European Union Statement by Ms. Narcisa Vladulescu, Counsellor, European Union Delegation to the UN, at the 73rd Session of the United Nations General Assembly First Committee Thematic Discussion on Other Disarmament Measures and International Security
Mr. Chairman,

I have the honour to speak on behalf of the European Union. The Candidate Countries the former Yugoslav Republic of Macedonia*, Montenegro*, and Albania*, as well as the Republic of Moldova and Georgia, align themselves with this statement.

The EU reiterates its concerns raised by the increased ability and willingness of some States and non-State actors to pursue their objectives by undertaking malicious cyber activities that threaten international peace and security.

In that light, the EU is gravely concerned with the attempt by the Russian military intelligence service (GRU) to undermine the integrity of the Organization for the Prohibition of Chemical Weapons (OPCW), as reported by the Netherlands, which hosts the organisation. This aggressive cyber operation demonstrates grave contempt for the solemn purpose of the OPCW, which works...
to eradicate chemical weapons worldwide, notably under a UN mandate. The EU and its Member States deplore such hostile
cyber operations which undermine international law and international institutions. We reaffirm our commitment to uphold the
rules-based international system, and defend international institutions from those that seek to do them harm, by improving and
strengthening stability in cyber space, including through the UN.

Recognising the challenges posed by cyber threats, EU Member States have adopted a “Framework for a Joint EU Diplomatic
Response to Malicious Cyber Activities”. This Framework contributes to conflict prevention, cooperation and stability in
cyberspace by detailing how measures within the EU’s Common Foreign and Security Policy, including restrictive measures, can
be used to prevent and respond to malicious cyber activities. The measures within the Framework aim to protect the integrity
and security of the EU, its Member States and their citizens, encourage cooperation, facilitate mitigation of threats and influence
the behaviour of potential aggressors, both State and non-State actors, in the long term. By providing clarity on EU response to
malicious cyber activities, the Framework contributes to international peace and security.

On 18 October 2018, the European Council called for measures to build strong cyber security in the European Union. EU
leaders referred in particular to restrictive measures able to respond to and deter cyber-attacks.

Mr. Chairman,

The EU and its Members States promote the establishment of a strategic framework for conflict prevention, cooperation and
stability in cyberspace that is based on the application of existing international law, and in particular of the UN Charter in its
entirety, the development and implementation of universal norms of responsible state behaviour, and regional confidence
building measures between States.
The EU recognises the role of the United Nations in further developing norms for responsible state behaviour in cyberspace. The EU emphasises that the consecutive UN Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, over the years, have reached consensus on a number of measures contributing to greater cyber stability, including on norms, rules and principles of responsible behaviour of States, the promotion of confidence building measures, capacity building and the application of international law in cyberspace. We should continue to build on this work.

Regarding the application of international law, the EU recalls that "International law and in particular the UN Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."

The EU recalls that the 2013 and 2015 reports of the Group of Governmental Experts, which the General Assembly has repeatedly endorsed, contain important recommendations that States should fully implement and in particular 11 voluntary, non-binding norms, rules and principles of responsible behaviour of States that are listed in paragraph 13 of the 2015 GGE report, which include, among others, the following: "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs", "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty", and "States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions". The GGE also stressed that States should guarantee full respect of human rights, including the right to privacy and freedom of expression.

The EU also emphasises the following international principles deriving from the UN Charter which, inter alia, apply to State use of ICTs: sovereign equality; non-intervention in the internal affairs of other States; the settlement of international disputes by peaceful means by such a manner that international peace, security, and justice are not endangered; the right to respond,
including by non-forcible countermeasures, to internationally wrongful acts committed through the use of ICTs; refraining in international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; the inherent right to self-defense against an armed attack; respect for human rights and fundamental freedoms. We also believe that international humanitarian law applies to cyber operations in war time, including the principles of precaution, humanity, military necessity, proportionality and distinction.

The EU supports and encourages the development of regional confidence building measures, which are an essential element to increase cooperation and transparency and reduce the risk of conflict. Implementing cyber security confidence building measures in the OSCE, ARF, OAS and other regional settings will increase predictability of State behaviour and further contribute to stabilising cyberspace.

In order to build trust and strengthen cooperation among States, as well as to implement the cyber norms, the EU acknowledges the role of capacity building, and stands ready to continue assistance to third countries in responding to cyber threats and increasing law enforcement capabilities to investigate and prosecute cybercrime. The EU considers it essential to advance cybersecurity capacity building through the development of appropriate domestic policies and legislation, protection of infrastructure, provision of training as well as upholding the rule of law in cyberspace.

Furthermore, the EU recognises that the interconnected and complex nature of cyberspace requires joint efforts by governments, private sector, civil society, technical community, users and academia to address the challenges faced, and calls on these stakeholders to recognise and take their specific responsibilities to maintain an open, free, secure, stable, accessible and peaceful cyberspace.

Mr. Chairman,
The EU and its Member States reaffirm their commitment to improving and strengthening stability in cyberspace. We should all recognise the achievements of the previous UN GGEs which provide the basis to continue work. We call on the UN Secretary General to continue to study and implement the measures to promote stability and security in cyberspace, and convene a new Group of Governmental Experts in 2019 with a view to providing a consensus report to the General Assembly.

To be successful, the GGE should remain effective and dynamic, and be able to deliver detailed results. Its mandate should be focused and guided by cumulative conclusions agreed in previous GGE reports, including the applicability of existing international law in cyberspace and the 11 norms of responsible State behaviour listed in paragraph 13(a)-(k) of the 2015 GGE report.

The EU believes that UN Member States, and in particular future GGE members, should submit national contributions on the subject of how international law applies to the use of ICTs by States as it builds on the consensus view that international law applies to cyberspace and advances the global understanding on national approaches which is fundamental to maintaining long-term peace and security and reducing the risk of conflict in cyberspace. Such contributions could be annexed to the GGE’s report.

Furthermore, the EU considers the aspect of consulting the UN membership as well as other stakeholders an important element of the mandate. The GGE shall hold regular, open-ended, inter-sessional consultations with the wider UN membership and interested stakeholders.

In conclusion, the EU will prioritise a resolution that reaffirms the consensus views articulated in previous Groups of Governmental Experts reports, including norms, rules and principles of responsible behaviour of states, confidence building measures, international law and capacity building and the importance of respect for human rights and fundamental freedoms in cyberspace. We note that draft Resolution L.37, co-sponsored by all EU Member States, is based on the previous First Committee resolutions that usually enjoy consensus. We note with regret that the traditional sponsor of the ICT Resolution, the Russian
Federation, has chosen to pursue a different course of action this year. In particular, we would like to point to operational paragraph 1 of its current draft, which offers a selective list of recommendations of the previous UN GGE reports and norms established by a regional organization. Imposing this on UN Member States through a UN General Assembly Resolution would set an unwelcome precedent for cyber security and all other areas of future work. It would undermine the consensual recommendations of the previous UN GGEs and prejudge the outcome of any consultative process which is neither inclusive nor open-ended.

Thank you, Mr. Chairman.

* The former Yugoslav Republic of Macedonia, Montenegro and Albania continue to be part of the Stabilisation and Association Process.

Tags:

UNGA73
FIRST COMMITTEE – DISARMAMENT AND INTERNATIONAL SECURITY

Author

Press and information team of the Delegation to the UN in New York