STATEMENT BY THE REPRESENTATIVE OF AUSTRALIA TO THE FIRST SUBSTANTIVE SESSION OF THE OPEN ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF ICTS (December 2021)

International law

Existing international law provides a comprehensive and robust framework to address the threats posed by State-generated or State-sponsored malicious cyber activity.

> It provides victim States with a "tool kit" to identify breaches of international legal obligations, attribute those acts to the responsible State, seek peaceful resolution of disputes and, where the victim State deems appropriate and it is permissible under international law, take measures in response.

When we refer to 'existing obligations under international law', we are referring to the treaties, customary international law and general principles of international law that States are already a Party to and have already consented to be bound by.

The application of existing international law to cyberspace can enhance international peace and security by increasing predictability of State behaviour, reducing the possibility of conflict, minimising escalation and preventing misattribution.

Australia has published its views on international law and cyber on several occasions, most recently as an annex to the 2021 GGE report.

> In 2020, as a means of practically demonstrating international law's value in the cyber context, Australia submitted a non-paper to the OEWG with a series of case studies on hypothetical unlawful cyber operations against victim States.
>
> These looked at different examples of cyber operations, including a case of misattribution, and demonstrated how international law provides victim governments with protections, options and solutions.

Australia aligns with the many delegations that have emphasised the importance of sharing our positions on the application of international law in an effort to deepen understandings, as set out in the 2021 OEWG report.

The advantage of States publicly articulating their views on how international law applies in cyberspace is that it may actually provide us with the opportunity to identify areas of convergence between State positions on this issue – something which we cannot do unless States share their positions.

This process could quickly deliver clarity and deepen common understandings on key questions of how international law applies to State conduct in cyberspace as well as contributing to the development of applicable customary international law.

OEWG sessions provide a great opportunity for States to share with other States their views on how international law applies in cyberspace, and we have valued hearing other States' views in these processes, which is often the first time they have expressed a position publicly.

Australia also aligns with those who have emphasised the importance of increased capacity building for countries to better understand and develop their positions.

Chair
The International Commission of the Red Cross has confirmed that the use of cyber during armed conflict is a contemporary reality, and that an increasing number of States are relying on cyber, in an ever-growing number of applications, to achieve military objectives.

It is a reality that this group – with our mandate to concentrate on the peace and security dimensions of cyber – cannot ignore and should confront.

Along with the rules in the UN Charter prohibiting the use of force, IHL is the key body of law to address this area of cyber activity.

Australia welcomed States' affirmation in the 2021 GGE report that IHL applies to cyber activities in situations of armed conflict.

Australia has consistently recognised that international humanitarian law is applicable to cyber activities in armed conflict, and that IHL's applicability does not encourage or legitimise warfare by cyber means.

As the word ‘humanitarian’ in the name of this body of law suggests, IHL’s core purpose is to limit the effects of hostilities and protect civilians.

Chair
Australia strongly supports this OEWG deepening our understanding of the application, to State activities in cyberspace, of the customary international law on State responsibility.

The customary international law on State responsibility – much of which is reflected in the ILC Articles on the Responsibility of States for Internationally Wrongful Acts – provides the mechanics for the application of most international law, including the UN Charter.

It details strict rules on attribution, provides what measures a State may take in response to unlawful acts, and determines the consequences of internationally wrongful acts, including reparations.

The international community would greatly benefit from clarity on how this body of law applies in cyberspace.

Chair
I would also like to take the opportunity to respond to several points raised by other delegations:

Regarding terminology, the creation of any kind of glossary of common definitions goes beyond a plain text meaning of ‘discussions on terminology’.

We understand that many countries do not have agreed national definitions of key terms in the sphere of the concepts we are discussing at the OEWG.

This will make it very difficult to gain consensus on basic definitions.

Consequently, Australia does not support the creation of any glossary of common definitions.

Australia prefers we instead focus any discussions around terminology on encouraging voluntary sharing national definitions in the interest of providing greater transparency and understandings between us.

Discussions aimed at harmonising or agreeing terminology could be potentially harmful because, by necessity, harmonisation disregards the particulars of cultural context and diversity.

The OEWG itself is a confidence building measure. Our aim should be to increase transparency and understanding of each others' systems, policies frameworks, and interpretations.

Chair
We note the concerns raised by the Russian delegation regarding the application of the inherent right to self-defence, as articulated in article 51 of the UN Charter, in cyberspace.

Noting that there is consensus that the UN Charter - in its entirety - applies in cyberspace, it follows that article 51 also applies to cyber activities that constitute an armed attack and in respect of acts of self-defence that are carried out by cyber means.

On the issue of whether there has been an armed attack, I would like to share Australia's position on this matter, to assist other member states in coming to their own position.

In Australia's view, if a cyber activity – alone or in combination with a physical operation – results in, or presents an imminent threat of, damage equivalent to a traditional armed attack, then the inherent right to self-defence is engaged.

Australia also notes that any use of force in self-defence must be necessary for the State to defend itself against the actual or imminent armed attack, and be a proportionate response in scope, scale and duration.

Any reliance on Article 51 must be reported directly to the UN Security Council.

These additional requirements of article 51, in Australia's view, help safeguard against the risk of armed escalation, which was also an issue raised by the Russian delegation.

As to the issue of imminence, an issue raised by the delegation of the Philippines, Australia notes that the rapidity of cyber activities, as well as their

potentially concealed or indiscriminate character, does indeed raise new challenges for the application of established principles.
However, existing international law does assist in this regard.

As explained by Australia's then Attorney-General, a State may act in anticipatory self-defence against an armed attack when the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts.

This standard reflects the nature of contemporary threats, as well as the means of attack that hostile parties might deploy.