Good Evening, Ladies and Gentleman

At the outset, I would like to thank ORF for inviting me to speak, and kick off the proceedings for this year's CYFY conference on Cyber Security and Internet Governance. As you all know, the theme for the session this evening is Cyber Arms Control.

Let me first attempt putting the subject in **CONTEXT**

The connotation and application of Cyber space has expanded exponentially in the recent years, and this trend is likely to continue. While there are numerous all-round benefits of this growth, a number of challenges have also come to the fore.

Incidents of commercial espionage, IPR theft, Technology and Military Intelligence, Surveillance, Denial of Service, and other attacks in this domain have shown an increasing trend.

Given the fact that many entities and individuals are working on developing Cyber tools, or Cyber weapons as some prefer to call it, there is also an emerging view, that some form of Cyber competition or race, is probably, already underway.

Consequently, there have been calls for some treaty, or convention, or code of conduct, for regulating Cyber space and Cyber weapons. This is linked to a broader quest to strengthen strategic stability, in a digitised global environment.

Inherently, there are ideological, political and legal aspects intertwined in this whole debate. While some countries are more focused on criminal threats, others have greater concern regarding political and social threats from Cyber space. As may be expected, there are distinct and opposing approaches, based on interests and priorities.

A few issues that are being grappled with include:

- Is Treaty Based approach the solution, given the experiences of earlier treaties in Nuclear, Chemical, Biological, Outer Space, and other domains.

- What is the applicability of International Laws in their present form?

- How do we look at issues related to scope and jurisdiction from national security, socio - cultural, and law enforcement points of view, concurrently?

With this backdrop, let me move on to giving an **overview of the progress made** in this direction thus far.

Exploratory efforts have been on since around late nineties.

Council of Europe Convention on Cyber crime or Budapest convention of 2004, Cooperation in the field of Information Security by the Shanghai Cooperation Organisation in 2008, and adoption of African Union Convention on Cyber Security in 2014, are the only multi-lateral agreements in the cyber domain till now.

Various UN General Assembly resolutions have been adopted, highlighting concerns on Cyber Security. A report was submitted by a Group of Government Experts in Jul 2010.

More iterations have followed since then, and in 2013, the report explicitly mentioned applicability of international laws, particularly the UN Charter, to state or state-sponsored, activities in cyber space. The fourth UNGGE report was submitted in July this year. The report recommends norms for responsible state behaviour in cyber sphere and has identified a few CBMs as well as steps for capacity building.

NATO had earlier commissioned a study on the Applicability of International Law to Cyber Warfare, and the report titled Talinn Manual covered a large ground, but is not a legally binding document.

In 2011, Russia submitted a draft international code of conduct to the UN, supported by China, Tajikistan and Uzbekistan. The draft was updated in 2014. ARF, OSCE, OAS and other forums are also working on achieving international cooperation in cyber space.

As can be seen, a beginning has been made, but there is considerable ground yet to be covered.

I will now briefly touch upon <u>some of the Challenges of the Cyber Space Domain</u>.

- There are no geographical boundaries, and tools can be routed through servers or VPNs in widely separated locations.

- There is a thin line between malicious and non-malicious software.

- Millions of viruses get introduced every year, with rapid multiplication.

- Listing or classification of Cyber tools or Cyber weapons is impractical, even with exclusion clauses, as was the case in the CWC.

- Dual use software is very different from dual use chemical, nuclear or space technologies. Hardware, software, networks, domains, SCADA systems, protocol layers, analytics etc. bring in different dimensions.

- Identity of originator of a Cyber incident can be easily concealed.

and

- Degree of difficulty towards compliance and verification, for any treaty, far exceeds our earlier experiences.

We can see that, while the earlier and existing arms control mechanisms focused on prohibition or limitations on development and testing, physical deployment, build-up of arsenal, or actual usage – most of these models do not apply to the Cyber domain. Export control mechanisms, particularly for limiting cyber offensive capabilities, bring in a different set of challenges.

Further, issues related to growth and development, increasing access and affordability, and privacy concerns need to be duly factored.

There are also different positions on the applicability of laws of armed conflict - specifically with regard to the principles of necessity, proportionality, and discrimination between military and civilian infrastructure and personnel.

Let me now briefly talk about National Security Perspectives and Challenges.

Cyberspace applications today include surveillance, intelligence, and actual conduct of military operations – both defensive and offensive. Some countries have outlined Cyber doctrines and strategies, with national and military security as the backdrop. There are also moves to shift from reactive to pro-active strategies. Further, terms like deterrence, escalation, pre-emption and retaliation have been included in some doctrines and strategies.

Militaries today are increasingly dependent on ICT networks for conduct of operations. Requirements of situational awareness, Network Centric Warfare, and Information Dominance have led to focus on ICT capabilities. Consequently, these have also led to anxieties. Cyber structures are being created in defence forces around the world, to factor in these dimensions of warfare.

Militaries also recognise that vulnerabilities in Cyber space come from technology itself, as has been highlighted by the Zero-Day exploitation concept.

It is pertinent to mention that Cyber domain also offers an attractive option for asymmetric warfare, in terms of offsetting conventional superiority. Further, attacks on critical ICT networks can provide significantly higher military advantages, than physical attacks on some targets. Such Cyber attacks also provide surprise, and desired effect, with the added advantage of deniability.

There have also been reports, since around 2008, of Cyber operations having preceded, or run in parallel, with conventional military operations.

It is hardly surprising therefore that some countries now consider Cyber to be the biggest National security threat.

Under these circumstances, we need to see if any treaty or agreement can reduce the risks of an armed conflict or its escalation. I will now highlight a few bullet points – **on some key take-aways**, **and put forward some thoughts as a way forward**, to this informed gathering:

- Mental maps that we form, whenever we talk about Cyber arms control based on existing templates, need to be discarded.

- The challenges of Cyber domain are unique, requiring innovative responses. New approaches of open and democratic internet governance will also bring new challenges. There is a need to take into account the reality that Cyber Space has substantially increased ownership with the private sector, and the society at large.

- While interface, overlap and continuum in malicious cyber activities is recognised, there is a need for cyber offences and crimes to be examined somewhat differently, from considerations of sovereignty and National security. The debate has so far tended to put all cyber attacks in one basket, but as we all know issues related to cyber theft or cyber crime are very different from issues related to Cyber Attacks from security or military point of view.

- As cyber gets more integrated with security strategies, new concepts of paradoxes, thresholds and counter-measures, to Cyber provocations, are likely to surface in the near future.

and

- While seeking international consensus on any norms of behaviour in the Cyber domain would be difficult, and feasibility of implementation even more challenging, efforts in this direction are necessary to strengthen peace, stability and development.

- There is a need to segregate the debate into two parts – Law Enforcement Objectives, and Sovereignty cum National Security Objectives. Cyber thefts, cyber crime and cyber intrusions for nuisance need to be distinguished from cyber attacks from security and military point of view.

- To expand cooperation mechanism towards Law Enforcement Objectives, there is a need to evolve a multi-lateral framework.

- In parallel, we should continue efforts to develop a broad based code of conduct, instead of a treaty or convention, for strengthening International security. This is however, likely to be limited in scope and implementation.

- Both approaches should have participation from the private sector, as well as the civil society, to strengthen cyber security.

- And finally, there is a need to outline suitable clarification with regard to the Laws of Armed Conflict, to achieve alignment with the planned code of conduct. This will bring the ongoing debate on Applicability of these Laws, to a logical conclusion.

Thank You.