



**United Nations Office
for Disarmament Affairs**

**2026 Singapore International Cyber Week - “Cyber at a Crossroads:
Shaping the New Cyber Order”**

**Izumi Nakamitsu
High Representative for Disarmament Affairs**

As delivered keynote address



15 October 2026
Singapore

Your Excellency, Foreign Minister Dr. Vivian Balakrishnan,

Excellencies,

Distinguished participants (and especially Ms. Gwenda Fong, CEO of CSA),

Dear colleagues,

It is always a pleasure to be in Singapore—especially for this Singapore International Cyber Week.

I am really grateful to the Cybersecurity Agency of Singapore for the kind invitation to reflect on this year's theme "Cyber at a Crossroads: Shaping the New Cyber Order".

To reflect on the "*Cyber Order*" it is perhaps necessary to zoom out and reflect on the broader *world order*.

The world of today is not the one of 10 years ago.

In the last decade, we have seen a significant rise in strategic competition, including over the deployment, control and use of advanced technologies.

Competition in connection with frontier AI models, semiconductors, space capabilities and digital infrastructure has become a defining feature – if you will - of our times.

And this competition is no longer confined to two poles of power reminiscent of the Cold War era.

An increasing number of countries are becoming important drivers of global

economic growth and technological investment, contributing to a more multipolar global economy.

This diffusion has brought great benefit but also revealed vulnerabilities, including dependencies on concentrated supply chains.

At the same time, the international security landscape has seriously suffered.

Trust levels have plummeted.

New wars and the intensification of decades-old or even centuries – old conflicts have seriously strained our multilateral institutions, including the United Nations.

Countless civilians are paying the price.

The very nature of those conflicts has transformed through advances and diffusion of technologies that were, until recently, the domain of only the most advanced militaries.

This trend is particularly clear in relation to uncrewed aerial vehicles and missiles, which have greatly proliferated.

Today, information and communications technologies are routinely used to support hostilities through disruption, intelligence gathering, and strategic signaling.

And current battlefields are becoming testing grounds for AI and autonomy, which are increasingly integrated across military functions.

All in all, the world has moved increasingly towards insecurity, fragmentation and competition.

But I would not like to only focus on the negatives.

While the challenges before us are considerable, the international community has the ability and responsibility to reverse course.

And this brings me back to the matter of “*shaping the new cyber order*”.

Implicit in the question of how we shape this “new order” is the idea of *agency*.

We—as individuals, as governments, as a global community—maintain the agency to make choices about how digital technologies like ICTs are addressed so that risks are mitigated.

But these choices are not easy.

A growing number of threat actors are employing a range of techniques in cyberspace—ransomware, distributed denial-of-service attacks, supply chain compromises, and vulnerability exploitation.

And advances in AI have increased the scale, speed, and complexity of these threats. AI has been a vicious enabler of cyber attacks for some time, but the frontier models of agentic AI are also becoming orchestrators of such attacks. So we are clearly entering a new phase of the cyber reality.

The result is an increasingly complex threat landscape that is ultimately

redefining the “*cyber order*” at regular intervals.

The challenge is *shaping* outcomes in response to these threats rather than *accepting* them as inevitable.

I believe the United Nations remains the essential forum for achieving just that.

When it comes to international peace and security, ICT security has stood out as one area where States have regularly sought and found consensus solutions—even as the international security landscape has sharply deteriorated. And Singapore has played a leadership role in those efforts.

UN discussions on ICT security have steadily evolved over more than two decades—from expert-level, exploratory discussions to an inclusive process addressing threats evolving before us.

Successive open-ended working groups have solidified the framework of responsible State behaviour in the use of ICTs, which serves as the backbone of our multilateral work in this area.

The norms of responsible State behaviour in the use of ICTs—from commitments to inter-State cooperation to the protection of critical infrastructure—remain our guidepost.

But States have achieved other highly practical outcomes, from a Global Intergovernmental Points of Contact Directory to concrete confidence-building measures.

The UN processes have been a platform belonging to all States, where inclusive

conversation generated confidence and also flexibility.

It is this atmosphere of constructive engagement that must be maintained in the new permanent mechanism that has launched this year—the Global Mechanism.

This process is building on a considerable body of work, but we should be clear in our intentions to move decisively forward, including, and especially, on the thorniest issues.

These include:

- Continuing to assess the evolving ICT threat landscape, including pressing challenges related to critical infrastructure and the impact of emerging technologies such as AI;
- Considering implementation and potential further development of the normative framework for responsible State behaviour in the use of ICTs;
- And unpacking the applicability of international law to the ICT domain, including key principles derived from the UN Charter

As the Global Mechanism prepares for the first meetings of the Dedicated Thematic Groups in December this year, I am hopeful that progress will be made.

These groups represent the real innovation of the Mechanism providing a space for *shaping* action-oriented, concrete outcomes.

But success at the United Nations, while critical, benefits from efforts at the regional level.

No better example of this is the work undertaken here in Southeast Asia where sustained commitment to confidence-building and practical cooperation has made the region a leading example of how cybersecurity can be advanced collectively.

Key milestones include the establishment of the ASEAN Regional CERT facility in Singapore, the development of the ASEAN Regional Action Plan, and the ASEAN Norms Implementation Checklist.

The strong regional example of ASEAN, and the energetic engagement and leadership of Singapore, has been a driving force behind the collaborative efforts between my Office and the Cyber Security Agency of Singapore.

I warmly welcome the extension our joint activities, under the umbrella of the UN-Singapore Cyber Programme, for the next three years.

From the highly popular UN-Singapore Cyber Fellowship to the development of new courses on emerging technologies and cybersecurity, to training workshops on emerging cyber threats for ASEAN Member States, our agenda is quite full.

But we are pleased to be busy in this way and to contribute to capacity-building.

Without robust capacity-building, meaningful and inclusive cooperation cannot be fully realized.

Your Excellency, Mr. Foreign Minister,

Excellencies,

Distinguished participants,

Dear colleagues, (and “comrades” in a common purpose)

The task of shaping the “cyber order” remains in our hands.

The United Nations stands ready to support those efforts, and I look forward to working with all of you in the years ahead – and indeed more urgently, in the days and months ahead.

I thank you very much for your attention.