Organization for Security and Co-operation in Europe

VIENNA CYBER SECURITY WEEK 2019

- Protecting Critical Infrastructure -

Opening remarks by
Secretary General Thomas Greminger
Vienna, 11 March 2019

Excellencies,
Colleagues,
Ladies and gentlemen,

I would like to congratulate **Energy Pact Foundation** and its co-organizers for the impressive agenda for Vienna Cyber Week. In particular, I applaud them for having a dedicated panel and a parallel session on **women and cyber security,** as well as panels on **Artificial Intelligence** and how cyber security challenges relate to **youth issues**. Also, I am very pleased that Slovakia, which holds the OSCE Chairmanship this year, is collaborating with this conference, organizing two high-level panels later today.

Before addressing the matter at hand, I would like to mention that as part of my International Gender Champion commitments, I have pledged to promote gender parity in panels and not to sit in all-male panels, so called "manels". Well, I make an exception today.
I firmly believe we need to increase the participation and influence of women (or men on women's issues) to achieve inclusive perspectives, insights and innovation. There are many brilliant women, and I find it hard to believe that one could not be found to join us on this panel.

Ladies and gentlemen,

I will focus my remarks on **critical infrastructure protection** and the role of the OSCE. First allow me to say a few words as background about the Organization.

The OSCE is the world's largest regional security organization, with 57 participating States in Europe, Asia and North America. We work to **enhance stability and security** for more than a billion people **through political dialogue and co-operation.**

The OSCE originated from an important multilateral forum for dialogue and negotiation between East and West in the early 1970s. One of our key objectives is to increase trust and foster greater co-operation between States. We also take a **comprehensive approach to security**, taking into account its politico-military, economic and environmental, and human rights aspects. Our approach is particularly relevant and beneficial to enhancing **cyber/ICT security since it is cutting across all dimensions of security.**

Despite the current tense and polarized political climate and the increasing frequency of cyber incidents being attributed to States, **cyber security remains what we like to call an 'Island for Co-operation' within the OSCE.** In other words, it is **a shared concern going beyond the East-West divide, which builds basic consensus and allows for joint efforts.**
So we believe **there is merit in looking at how well-established methods of multilateral diplomacy can help to build confidence and enhance transparency** to reduce risks of conflict stemming from the use of Information and Communication Technologies.

Now, you're probably wondering **how** the OSCE contributes to the solution of cyber security challenges. The OSCE participating States **adopted 16 practical cyber/ICT confidence-building measures (CBMs)**.

I believe that these ground-breaking "cyber CBMs" are a core pillar of international cyber diplomacy, especially when we look at the value of preventive diplomacy.

These political commitments are aimed at building trust among States. They **enhance interstate transparency and predictability** by reducing the risk of misperception and miscalculation associated with the use of information and communication technologies by States. So they can stop unintended conflicts by slowing down or putting an end to potential escalatory behaviours.
The 16 CBMs can be broadly categorised in **three clusters**:

Posturing CBMs allow States to "read" another State's posture. This is achieved through information exchange on national organizations, strategies, policies and programmes. The OSCE provides participating States an online platform to exchange these documents.

Communication CBMs offer opportunities for timely communication and co-operation, including to defuse potential tensions. This is supported by the nomination of national focal points. The OSCE curates this list and fosters its practice through regular Communication Checks.

Preparedness CBMs promote the further development of national capacities. These include activities to enhance protection of ICT-enabled critical infrastructure.

Ladies and gentlemen,

Currently, we are focussing on operationalizing these CBMs through practical means. This includes a series of **capacity-building workshops, table-top exercises, facilitating deeper co-operation, and establishing a crisis communication network** among participating States.
For example, a few weeks ago senior government officials from the OSCE region met in Athens with diplomats, policy-makers and private sector representatives for a workshop about the latest cyber/ICT security policy developments on the international level.

They also took part in a **scenario-based discussion** highlighting how CBMs and other means can be used to reduce the risks of conflict following high-threshold cyber-attacks, for instance against critical infrastructure. Such exercises enable participants to **better understand each other's concerns, share perceptions, and discuss possible measures to prevent conflict.**

A good starting point for outcome-oriented co-operation is to focus on issues that are of shared interest to all. **Protecting critical infrastructure from cyber-attacks benefits citizens across the entire OSCE region**. So I will discuss **CBM 15,** which focuses on critical infrastructure protection, in more detail.

CBM 15 includes a commitment to develop shared responses, including crisis management procedures among States. It encourages States to adopt voluntary national arrangements to classify ICT incidents by their scale and seriousness. And it calls for enhancing the security and integrity of national and transnational ICT-enabled critical infrastructure.

Ladies and gentlemen,

Of course, the **UN plays a central role** in exploring how greater cyber stability can be achieved internationally. No other platform can produce overarching recommendations on matters of international law, norms, confidence- and capacity-building.

But current international cyber negotiations are blocked by the lack of confidence in a constructive solution to this global policy challenge. This needs to change and everyone has to do their part, including regional organizations.

The **OSCE is not the only regional organization working with cyber CBMs.** The **Organization of American States (OAS)** and the **Association of Southeast Asian Nations (ASEAN)** also deserve recognition for their work.

All three regional organizations are **developing practical measures** to turn the UN's recommendations into reality. In a sense, regional organizations are **incubators for national implementation of the UN Governmental Group of Experts reports**. They have also developed their own innovative ideas on how to address some of the most pertinent international cyber security policy challenges.

Regional organizations also tend to **have closer relations with national authorities, so they can better understand their views and concerns.** In the OSCE, we established a Network of **Cyber Focal Points** in our Missions and Offices **to ensure that we are well informed about national and regional developments.** This feeds into our deliberations and negotiations in Vienna, and helps in preparation of our conference and capacity-building efforts.

Ladies and gentlemen,

Implementing the OSCE's 16 cyber CBMs remains crucial, particularly in the current political environment. They provide States with **means to address non-political and practical issues.** They also offer **mechanisms that can create and foster routine interactions between States, which in turn can lead to more ambitious goals.** Ultimately, they **enhance and institutionalize international co-operation** on cyber security.

This has a broader implication: OSCE cyber CBMs can help rebuild trust, which is the prerequisite for reducing tensions and preventing conflict.

The best way to resolve cyber security challenges is through **continued and extensive engagement with a wide range of stakeholders**. So this conference on critical infrastructure protection is an ideal platform. I wish you exciting and stimulating discussions today, and throughout Vienna Cyber Week.

Thank you.