16 October 2024
GS messages @ IVEY event
"What are Some Takeaways for Canada?"

Thank you for having me! It is again a great pleasure and honor for me to be here!

My short input to this workshop is structured in the following way:

- The geopolitical background and the need to develop and apply a strategic-analytical skillset
- Reflections on the today's workshop and the threat landscape
- Finally, I will conclude with concrete recommendations.

The geopolitical background

Western countries are **confronted with an unprecedented complex threat landscape**. Disruptions to digital systems caused by natural phenomena (storms, floodings, landslides, etc.) and man-made activities, such as cyber-and cyber-physical attacks, sabotage, etc. In addition, a growing new phenomenon is the gray area between natural and man-made causes, triggered by climate change.

Telecom regulators can and should play a crucial role in this context and their importance is sometimes underestimated. However, regulatory authorities in most cases do not have a mandate to develop or apply a holistic view and break out of their vertical silos. This is a wakeup call for policy makers to give regulators a new mandate which would enable them taking up a crucial role in telecoms and the broader digital landscape.

For decision-makers in politics, public administration and industry, it is essential to develop two crucial analytical and strategic skills: Firstly, **develop and apply a geopolitical view** of the threat landscape and secondly, **understand the effect of hybridization**.

So, **what is hybridization?** Behind acts of sabotage seemingly carried out by criminal actors, there is often a connection that is not immediately visible. Hostile state and state-backed actors are increasingly using criminal groups as proxies.

This phenomenon has been intensified by the growing number of cases of specific embassy staff from hostile countries being expelled because their actual activities are not in line with the provisions of the Vienna Diplomatic Convention. This means, that such a country doesn't have sufficient own operational forces on the ground and therefore using proxies. There is still a lot of awareness-raising work to be done here.

Looking at the geo-political situation globally, resilience and security of digital systems is an urgent issue and should be high up on the agenda of policy makers, regulators and industry. The event today was a very useful opportunity for awareness raising and advocating for a Public-Private-Partnership to successfully tackle these challenges.

But the elephant in the room are the very high cost of resilience and the need to revisit regulatory paradigms (for example all kinds of infrastructure sharing) which are decreasing

redundancy and subsequently resilience and at the same time increasing single-point-of-failures.

Reflections on the today's workshop and the threat landscape

"Satellite" is the magic word of our today's event. I do not want to spoil the party, but as Andre Arbour rightly alluded to, satellite is not the silver bullet for all resilience concerns. Such a belief (I would rather say a misbelief) would be a mistake on many levels and can become, itself, a form of resilience risk. To put it in perspective, as we have heard today, satellite is a powerful and valuable means for emergency applications when terrestrial infrastructure fails, but not a magic cure against all resilience issues.

Let me also add the **aspect of trust**: What we are currently seeing in the market for LEO constellations is a quasi-monopoly of Starlink, which belongs to a man who repeatedly attracts attention with bizarre comments and is able to exert economic power that is more powerful than that of some nation states. This does not exactly build trust when it comes to operating critical infrastructure.

Digital infrastructures, in particular those labelled as "critical infrastructures" represent the backbone of our society. It is very costly to improve the resilience and security of digital systems, and this requires a new form of public-private partnership between governments and the private sector. Governments cannot tackle these challenges alone, nor can industry.

The security and resilience of digital systems are under pressure from

1. climate change induced natural disasters,
2. cyber- and cyber-physical attacks and sabotage from criminal actors and state (backed) actors. Cable (copper) theft falls in the same category. We need to assess the complex threat landscape through the lens of geopolitics,
3. human error (most prominent example is the CloudStrike outage, which affected millions of Windows systems globally and Phil Moore alluded to this incident just before).

Talking about implications, we should look at the Islandic model and experience which seems relevant (also Ukraine in some way). The Icelandic regulator considers a lack of redundancy and resilience to be a market failure that allows the regulator to intervene and to impose measures to increase redundancy and resilience.

We have seen from international comparison, that a **combination of incentives and regulations** seems to be most effective to raise the resilience level:

- **On the incentive side,** a new, more collaborative approach is needed: dedicated funding and public-private partnerships will be key to building resilient networks, particularly in high-risk and underserved areas.
- **On the regulatory and legislative side**, it is important to adopt a system that supports operator investment and consumer compensation mechanisms. It is highly recommended that stricter rules and enforcement be put in place to address cable theft and other forms of infrastructure sabotage.

Let me conclude with three policy takeaways:

1. **Adopt a Collaborative model for resilience** in particular for areas most at risk from climate events, rural and remote areas, often served by single, older, terrestrial networks.
2. **Create a Supportive Policy Environment**: Regulatory policies need to support the rollout and operation of multiple networks/platforms and to provide funding to address the cost of resilience upgrades.
3. **Integrate Emergency Management (EM) into Telecom Regulation**: Integrating emergency management frameworks into telecom regulation is crucial to ensuring operators can prevent, prepare, respond, and recover from disasters, strengthening infrastructure and minimizing service disruptions during crises.

Thank you!