Question 1/ Role of Diplomats in the Cyber Landscape

Noor's Remarks:
Thank you
Practically speaking, to effectively adapt to the evolving cyber landscape, diplomats must enhance their cyber literacy, leverage secure tools, Call for international collaboration with their counterparts, academia, and the private sector and should promote ethical cyber conduct. while that in a nutshell covers the "how", it is often faced by the realities on the ground and so focusing on two layers of responsibility when shaping this conversation is also important layer 1, at the institutional level -MFAs and beyond, where we set protective policies, standards, and frameworks; and Layer 2, at the individual level- the diplomat's own initiative and awareness.

Depending on the Nation, the balance between these layers will vary—while some Nations have robust institutional support, many don't- meaning unwittingly the greater responsibility ends up falling on the individual diplomat.

This is why I urge that we approach this topic with an understanding that true strength lies not in competing against each other but in developing institutions and fostering collaboration.

This is also true of the Hashemite value that guides Jordan's approach and shapes my own perspective on cyber diplomacy and its impact on diplomats.

With this guiding perspective, I view the topic while baring in mind that the digital transformation of diplomacy has unfolded in three main dimensions as many of you are aware;
The Environment in which diplomacy is conducted.
The Policy Topics covering over 50 areas,
and thirdly By Tools used such as social media, big data, and AI.
Each dimension positions diplomats at the centre. However, we lack frameworks focused on equipping diplomats to navigate this new terrain.

Perhaps this is because diplomacy is often seen as a uniquely national endeavour rather than as a collaborative field, which limits our perspective on the need and the potential for collective, cross-border solutions that has a trickle-down effect on individual foreign ministries.

While addressing this gap at an institutional level by preparing diplomats individually is doable— doing it at a collective scale is what really bears fruits, and in terms of my research this is what gave birth to the idea of my framework, and why I am happy that this topic is gaining more attention.

Identifying this need to empower individual diplomats is a crucial first step, the second emphasises the unique vulnerability of diplomats.

Given that they operate on the front lines of a digital battlefield whether they are aware of it or not, making them targets. They face personal risks to their devices, communications, and the integrity of their ministries, the impact of which is hard to measure in real-time but given past cases we know is great and this is why we need more conversations on the regional level in a similar model to what took place in the first Arab Foreign Ministries' Cyber Diplomacy Dialogue held at the Dead Sea in Jordan. While promising and had some positive spillover effects, this dialogue needs to translate into actionable outcomes for cyber diplomacy and regional collaboration. Perhaps a second dialogue here in Muscat, inshAllah—to continue where we left off at the Dead Sea

Lastly, we need to advocate for digital sovereignty— independent of influence whether stemming from another nation or big tech. In much of the Global South, there is a sense that exposing their nations to heightened cyber risks and compelling them to rely on external support- is the target whether that is the case or not, the reality is that their institutional resilience is undermined, directly impacting diplomats' ability to conduct secure diplomatic work and impedes them from utilising emerging tech at the same level as their counterparts.

Furthermore, the misaligned global priorities exacerbate these challenges especially since the digital infrastructure of most nations is developed and delivered by a handful of nations, and so it's important to call for a shift that prioritises collaboration and mutual benefit rather than only self-serving interests and that starts regionally for sure, and ironically I find that diplomats are best suited to build that trust.

Question 2/ Challenges of Applying International Law & Regional Cooperation in Cyberspace

Noor's Remarks:
International law is the compass for cyber diplomacy, but the challenge is that a compass alone - doesn't build the road. And we have seen that in action this past year in our region as it relates to the lack of enforcement of international law.
With today's political reality both young and old in the Arab world have felt the double standards at a shocking level, and it was a clear demonstration that they are not seen as equals by their counterparts from the global north so the current impact and future role of international law in cyberspace, and in general, is a crucial area of concern and alarm to many of us, who believe that without strong institutions & respect for the law we risk undermining our collective stability & security-which, we have already begun to see.

This fundamental problem— translates as well to cyberspace given that while we have frameworks, like the UN's work on developing norms of state behaviour in cyberspace, enforcement and practical application lag behind.

Meaning this is not just a regional issue; globally, we see gaps between what is agreed upon diplomatically and how it's applied in the real world. In the Arab region, the regional institutions like the Arab League, the GCC, and the ARCC have taken steps to discuss cyber security frameworks,
but without a cohesive regional mechanism to enforce these, we are left reacting to incidents individually rather than collectively shaping our defences proactively and fostering innovation.

we do have the seeds of hope, such as Muscat's ARCC, as well as the agreement this year to establish the Arab League's Council of Arab Cybersecurity Ministers in Riyadh, and the spillover from the Dead Sea's first Arab Foreign Ministries' cyber diplomacy dialogue. The real opportunity lies in building on these steps with a sense of urgency, focusing on practical and coordinated implementation.

-END-