Forum of Strategic Dialogue

Cyber – an Israeli Response

Israel views cyber space first and foremost from the perspective of national security given Israel's unique security situation and threats to its security. In this context, one should consider that Iran is a strong actor in cyber space and that not only state actors, but also non-state actors, can threaten vital national security assets. In Israeli eyes, cyber warfare is a new and upcoming dimension of warfare as a whole.

One of the side effects of Israel heavily investing in military cyber security is that it also became a commercial engine. Though Israel is a very small country, its cyber industry is second only to that of the U.S., taking 20 percent of the overall venture-backed cyber investments worldwide, according to an analysis of PitchBook and Start-Up Nation Central databases.

Aside from cooperation on national security issues including in the fields of weapons of mass destruction, terrorism, and protection of critical infrastructure, we should focus our attention and cooperation – beyond cyber infrastructure, resilience, AI, cloud storage, and quantum computing – also in the fields of immigration and organized crime (with an emphasis on drugs), which are both connected to cyber space. We would also suggest thinking about joint working groups analyzing AI in terms of threats, challenges and opportunities.

While the heavy focus on privacy is understandable, special attention should be given to drawing the exact balance between protecting privacy and human rights and providing effective solutions in the cyber world. Over-regulation and too many barriers could sometimes hamper effectiveness. Finally, we need to develop an internationally accepted legal codex and code of conduct in cyber space, including an update in international law.