Opening remarks CSD 30.1.2025

- Dear Mr. Stefanov, friends of CSD, colleagues, guests … thanks for providing me the opportunity to make some opening remarks.

- In the first 9 months of 2024, 110 Russian vessels were spotted in the North Sea off the BE coast (more than in the previous 12month period in 2023). These included military vessels, research vessels and fishing vessels. *Preventing espionage and sabotage of critical infrastructure in the North Sea, such as submarine cables, has become a constant focus of the Belgian intelligence and security services.*

- Submarine cables greatly matter. The **cloud** for one, is not something high up in the sky. Clouddata - data stored on someone elses computer - is very often transferring through submarine cables.

- We now live in an environment that is **VUCA**: *Volatile, Uncertain, Complex and Ambiguous*. Let me give you some examples how Belgium deals with this on a bilateral level, on a regional leve, on the European level and beyond.

1. On a bilateral level

Example 1: cybersecurity & attribution

- Prior to coming to Bulgaria, I was heading the cybersecurity department at the Belgian MFA.

- When asked: ***what´keeps you up at night,*** the honest answer is **USERS = all of us here** (*the human factor as weakest link*). At the MFA, we´ve been working hard to turn users into human firewalls through an engaging & MFA tailored cybersecurity education platform. *For training purposes, we created an elaborated phishingcampaign targeting EU Presidencies at large*.

- However, apart from ´´users´´, **APT** or **advanced persisent threats** coming from nation-state backed actors – are a reality for every MFA nowadays. For the techies in the room: we got up close with APT27, APT28 and APT29, also known as **Goblin Panda** – China based ; **Fancy Bear** and **Cozy Bear**– Russia based. So what do we do? Well, we speak out – we **attribute**. In summer 2022, Belgium exposed malicious cyber activities targeting the Ministry of the Interior and the Belgian Defence. For the first time, we very publicly attributed those activities to Chinese Advanced Persistent Threats. We denounced those activities and urged the Chinese authorities not to allow its territory to be used for malicious cyber activities

Example 2: cracking the code

- To tackle high-risk criminal networks, we have a highly successfull Police and judicial cooperation with Albania. We provide SKY ECC data - decrypted data from the previously encrypted and now defunct SKY ECC chatservice - to the Albanian counterparts. This intel proves critical in multiple police raids as well as in court *(the Albanian Supreme court upheld the legitimacy of such data end of december last year)*. This is a little known successstory.

2. On a regional level

- Despite a modest coastline of 67 kilometres, Belgium is the **fifth-largest producer of offshore wind power** in the world. The Princess Elisabeth Island (under construction) is the world's first energy island, that will serve as a hub for offshore wind power. To assist others and promote the green energy transition, we will host – in early March - the Belgian Offshore days in Ostend, a seatown in Belgium.

- We believe **offshore windpower** might very well be worth considering in the Black Sea Region. That´s why we invited the Ministers of energy of Bulgaria and Romania to these Belgian Off Shore days for a round table on the offshore potential in the Black Sea Region.

- It should be noted that one of the tasks of Marta Kos, the new EU Commissioner for Enlargement, is to come up with a **Black Sea Strategy**. Cooperation by EU partners on offshore wind energy should be part of this strategy, as it would result in less reliance on authoritarian states fueling intolerance and undermining democracy.

3. On a European level & beyond

European level

- Belgium is fully inbedded in the EU sanctions regime : the EU has over 45 sanctions regimes, both geographical and thematic. The number lists is increasing and will most likely continue to do so. Belgium gives particular attention to the effectiveness and impact of sanctions, the implementation of sectoral measures, coordination with like-minded partners, as well as outreach and advocacy of EU measures towards the Global South.

- To keep track of EU sanctions, simply visit the sanctionsmap.eu website (that´s : sanctionsmap.eu).

Beyond

- **Disclaimer**: what follows is **not** an official Belgian position but my personal opinion.

- The forensic analyses of various cyberincidents by our CSOC (*our own, inhouse Cyber Security Operations Center*) spotted striking similarities in various attack vectors, one of which was the use of the infamous **beacon** payload from Cobalstrike (that´s *an ´´offensive-defence´´ commercially avalailble tool, meant for pentesting or mimicking red team tactics)*. There´s plenty of other, highly effective attack tools available out there *(kali, parrot, backbox… just to name a few).*

- Really worrying I believe, are digital marketplaces for **zero day exploits** (exploits for yet publicly unknown vulnerabilities/security flaws). Such digital weapons are available for those with deep pockets (private and state actors alike). Well known is ZERODIUM, branding itself as the leading exploit acquisition platform for premium zero-days : a proven to work iOS exploit used to sell for over 2 million US; an android one for 2,5 million US, *far more than what an ethical hacker might receive from the affected company or from a bug bounty program.* Nowadays, the site does not publish its bounties anymore, just an e-mail adress + Public PGP key for encrypted communication. Apparently, they feel the heat. And they should: this sector should undergo greater scrutiny.

Thank you