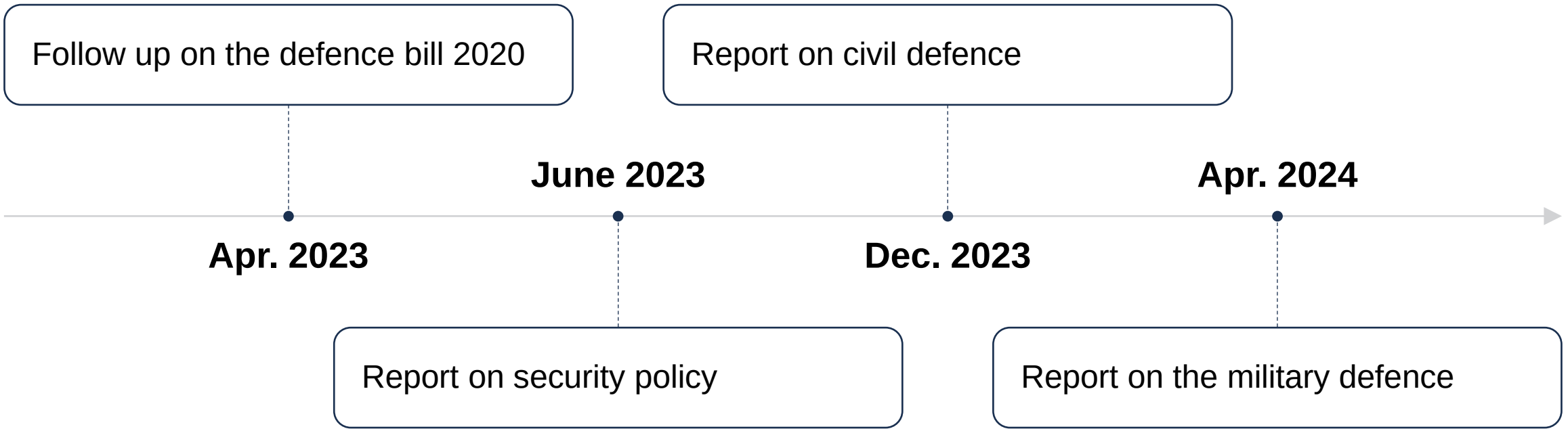
The Swedish Defence Commission's view on Cyber Security and Cyber Defence

Mårten Levin, Deputy Director
MoD/Secretariat to the Defence Commission

22 May 2024

The Defence Commission’s reports



Key messeges

- We have a historic defence bill ahead of us
- War in Europe, Russia is the long term threat.
- Real risk of an escalating war
- Sweden as a Nato ally
- Sense of urgency
- Continued and long-term support to Ukraine

The development of military capability must be accelerated and adapted to the requirements that follow as a NATO ally.

Time must be a decisive factor in the political and military decision-making regarding issues such as personnel structure, acquisition of defence materiel and infrastructure development in the coming years.

Security situation analysis

The conclusions made in the Commission's previous report on the security situation remain.

Sweden must shape its security and defence policy to deal with the long-term threat that Russia poses to European and global security.

There is a risk that the war in Ukraine will be prolonged and may escalate. An escalation could include attacks on other states.

Lessons learned from Russia's (cyber) war in Ukraine

The Russian large-scale and brutal warfare costs enormous resources, especially in the land domain. Personell, ammunition and defence materiel are expended and depleted in a way that has not been seen in decades.

At the same time, the war in Ukraine demonstrates Russian cyber warfare capacity that uses sophisticated attacks combined with more commonplace methods (denial-of-service, phishing) and integration of cyber with other domains.

Ukraine's cyber defence showcases the importance of political leadership and prioritization, preparedness, rapid adaptation, public-private cooperation and international support structures.

An armed attack cannot be ruled out

The Defence Commission concludes that an armed attack against Sweden or our Allies cannot be ruled out. Nor can it be ruled out that military means, or threats of such military means, can be directed against Sweden or our Allies.

The Defence Commission underlines that there is a tangible risk that the security policy situation will continue to deteriorate

Cyber attacks are an ongoing threat to the Swedish society

Cyber defence

Cyber defence is an integral part of military defence and is an essential part of modern warfare. Cyber security is a broad concept that includes everything from the individual's responsibility to society's digital systems.

The ability to carry out defensive and offensive cyber operations as well as the ability to detect, identify and ward off cyber threats against Swedish interests is of central importance for the entire total defence, also as a deterrent.

Continuous research and development is necessary for the maintenance and development of cyber defence capabilities. The Defence Commission also emphasizes the need to develop competence in cyber defence, bilaterally and multilaterally with Allies in NATO and member states of the EU.

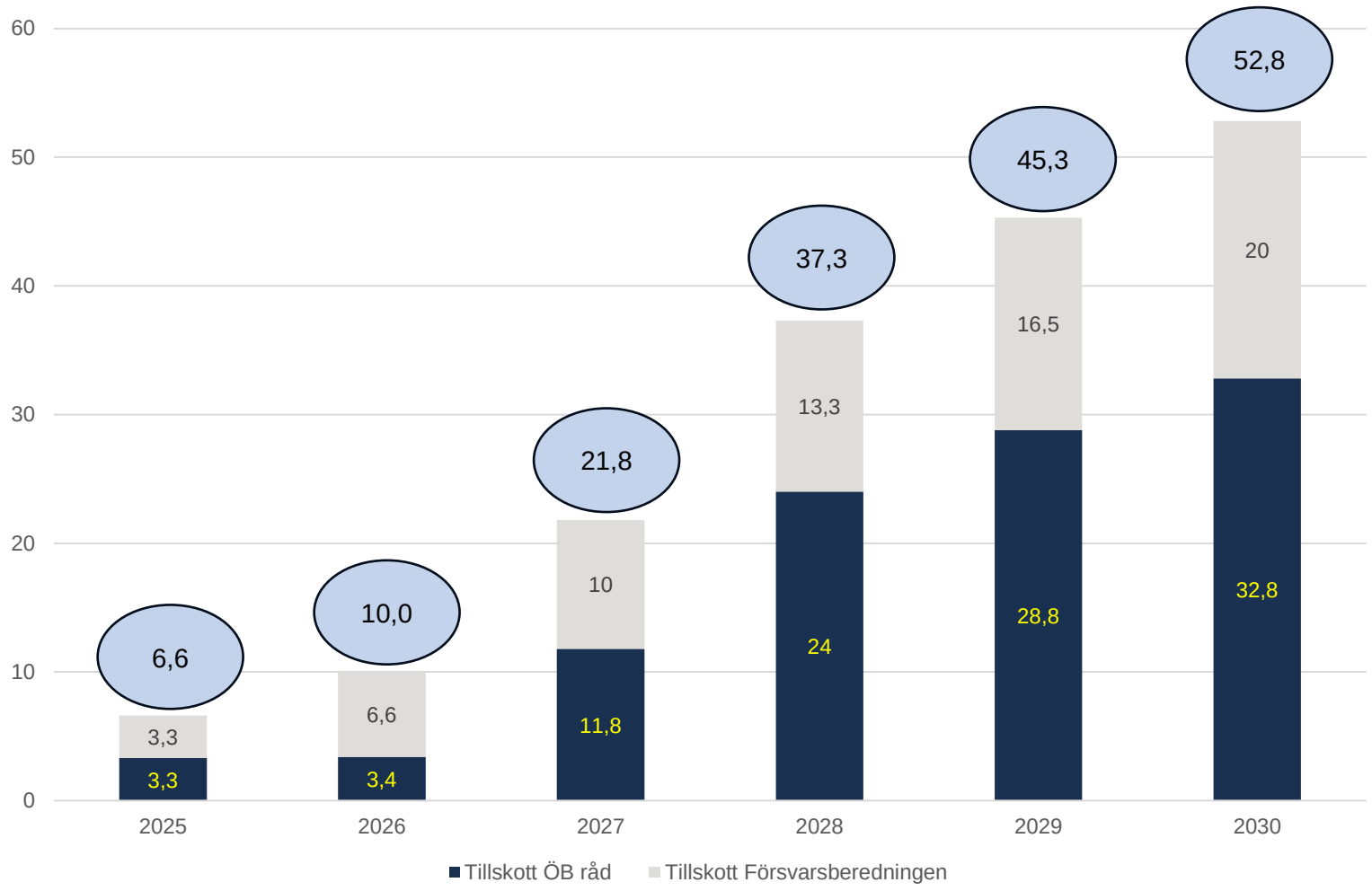
Cyber security and digitalization

Sweden's digital infrastructure for critical functions in society must be so robust that it can function across the entire scale of conflict – peace, crises and war.

In war, the society must be able to withstand cyber attacks, especially regarding attacks on information systems that are important for Swedish total defence capability. Systematic and preventive preparations of cyber security in peacetime are essential.

The Defence Committee believes that further measures are required to secure competence and human resources for Sweden's cyber security in war. Sweden has a large IT sector and a lot of expertise in this area. The Defence Committee emphasizes the importance of involving this capacity in the total defence. This should be a priority for concerned agencies and other stakeholders.

Funding military defence



Funding civil defence