Cybersecurity for increased competitiveness

Royal Swedish Academy of
Engineering Sciences

Foreword

»The Cybersecurity for Competitiveness project aims to contribute to a broad and nuanced discussion on the importance of a solid and coordinated effort to strengthen Sweden's cyber security.«

Digitization has become necessary for businesses in all areas of society, so cybersecurity is becoming increasingly important. Sweden is far ahead in international comparison when it comes to digitalisation. But there is a gap between this leading position and the fact that we lag behind other countries regarding our ability to protect ourselves against cyber threats.

This gap must be closed if Sweden is to benefit from the full benefits of digitalisation. Different actors are attacking our society daily. To counter them requires both cutting-edge technology and organisational efficiency. It also requires a broad knowledge among decision-makers in business and the public sector about cyber threats and the means to deal with them.

The Cybersecurity for Competitiveness project aims to contribute to a broad and nuanced discussion on the importance of a solid and coordinated effort to strengthen Sweden's cyber security. The project started in 2021 and runs until June 2023. This report is part of this work.

Our focus is on how the level of Sweden's cybersecurity affects the competitiveness of Swedish businesses and society at large. We also put forward proposals whose common denominator is that they will contribute to more effective cybersecurity in business and government.

IVA's strength as an independent actor is to engage individuals' expertise and experience in the areas the Academy works. Around fifty people have participated in the workshops and seminars conducted by the project as well as in the three working groups working on cybersecurity from different perspectives

The report's analysis and proposals are primarily based on the documents of the working groups. However, the Steering Group alone is responsible for the report's content.

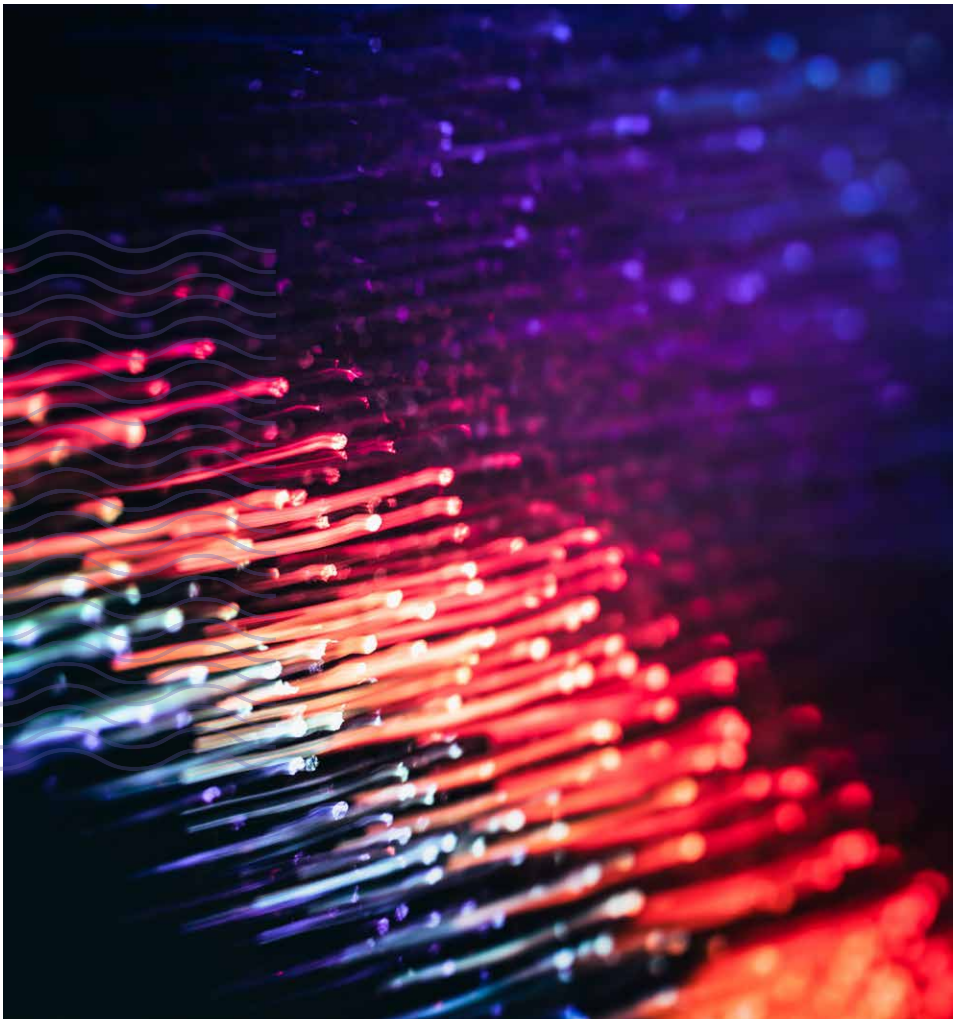
Stockholm in October 2022

Håkan Buskhe, Steering Group Chairman, CEO FAM and member of IVA's Department of Mechanical Engineering

Per Hjertén, Project leader IVA

Funders
Vinnova (Swedish Innovation Agency)
FRA (The National Defence Radio Establishment)
FMV (The Swedish Defence Materiel Administration)
Swedish Transport Administration
Swedish Bankers Association
Ericsson
Saab
The Swedish Internet Foundation
The Association of Swedish Engineering Industries
SNUS (Swedish Network Users' Society)

Download the full report at:
https://www.iva.se/globalassets/bilder/projekt/cybersakerhet/202210-iva-cybersakerhet-rapport-rev2.pdf



Summary

»Since June 2021, IVA has been running the project Cybersecurity for increased competitiveness. This report summarises the work and the project's proposals.«

Since June 2021, IVA has been running the project Cybersecurity for increased competitiveness. This report summarises the work and the project's proposals. Our focus is on cyber threats and the cybersecurity required to address them. The aim is to put forward proposals that can increase Sweden's cybersecurity and thus our competitiveness.

With digitalisation comes new vulnerabilities, with the effects of cyber-attacks being among the greatest threats. The ability to deal with cybersecurity issues is central to Sweden's competitiveness for business and society. Swedish companies are developing world-leading, high-tech products for the global market in several areas. Security by design, i.e. the ability to build in security throughout the lifecycle, is fundamental to the competitiveness of these products.

The interaction between politics and industry provides necessary conditions for business. Therefore, competitiveness from a societal perspective is important for business. Examples of areas where policy decisions and initiatives at societal level affect cybersecurity efforts and hence the competitiveness of enterprises are the provision of skills, legislation, the deployment of critical and secure infrastructure, and the ability to adapt and reassess regulatory frameworks in line with technological developments.

Effectively addressing cybersecurity issues within a nation requires coordinated actions and initiatives from policy, government, industry, and other parts of society. International regulation and legislation at the EU level significantly impact this work.

In Sweden, cybersecurity efforts are ambitious and often effective in different parts of the cyber ecosystem. But our conclusion is that there is much to learn from other countries that have worked longer and more focused on implementing cybersecurity strategies. This applies to areas such as political governance, the division of responsibilities and collaboration between public authorities and industry, and more significant national investment in research and skills provision.

Our conclusion is that Sweden is not adequately equipped to meet cyber threats:

- We do not take cyber threats seriously enough.
- There is a lack of understanding of the link between cybersecurity and competitiveness;
- There is insufficient cooperation between private companies and government actors on cybersecurity.
- Our decision-making power at central policy level is not sufficient to face cyber threats that are increasing and changing at a rapid pace.
- We are failing to provide the necessary cyber security skills.
- We are not preparing and mobilising enough.

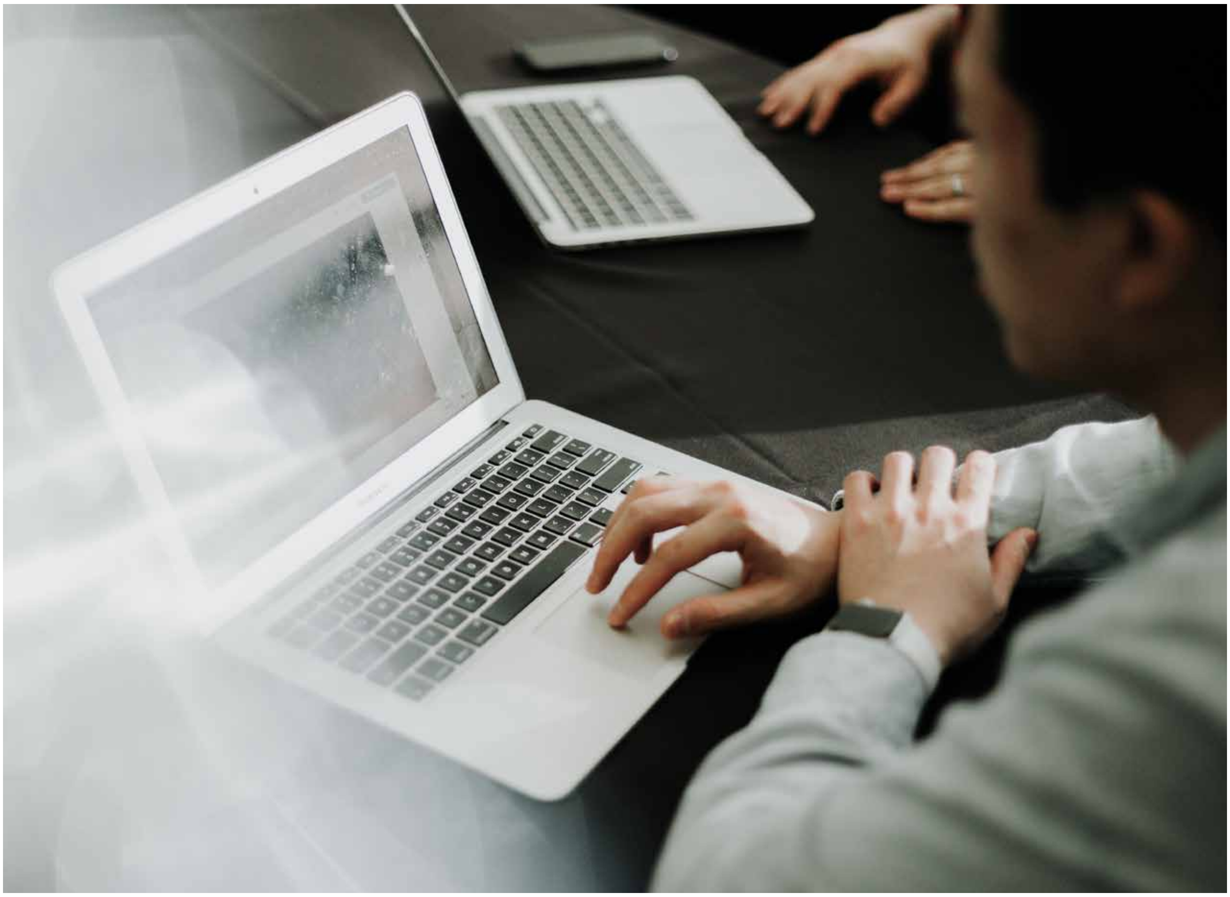
In the project's three working groups and steering group, we have identified five key areas, within which we propose

measures to strengthen Sweden's cybersecurity and competitiveness:

- **Political governance at national level needs to be improved.** We therefore propose that a Cyber Security Council be established within the Cabinet Office. The task will be to follow up and develop the national cyber security strategy and ensure that the agencies within the National Cyber Security Centre's activities are designed appropriately.

- **The exchange and use of information need to be improved.** We propose four measures to do this: a common platform for information sharing in the cyber domain; stimulating industry associations to initiate and ensure the continuity of various ISACs (Information Sharing and Analysis Centers); and mandating the MSB unit CERT-SE to provide clear advice based on the incident reports received. We also propose the establishment of a cyber incident commission.

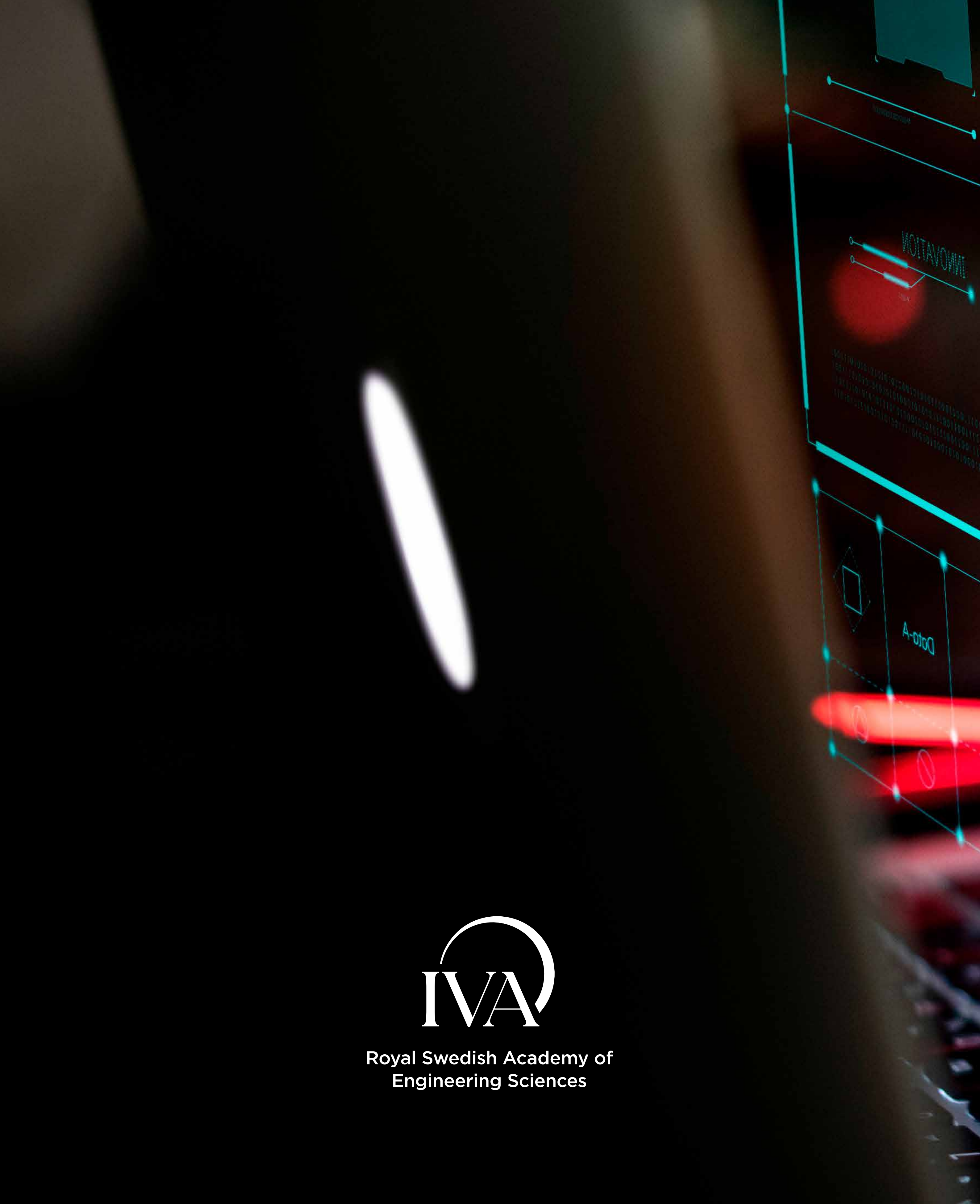
- **Operational capacity within organisations needs to be strengthened.** We therefore propose that the National Cyber Security Centre be tasked with coordinating the development of a national cyber security standard with the aim of becoming a national model for managing cyber security. The



standard aims to provide support, not least for boards and management, through concrete tools and principles so that it is "easy to do the right thing".

- **Research, innovation, and skills provision.** Sweden needs to make a concerted effort to ensure the supply of skills, not least top-level skills, in the field of cyber security. There is also a need for broad education and training efforts. As part of meeting some of these needs, we propose that a national cyber campus be set up. Its mission will be to conduct research, education and stimulate innovation on different aspects of how to protect the digital infrastructure. The centre will also help to ensure that expertise in "security by design" is available in Sweden so that industry can develop products that are competitive in a global market.

- **Mobilising resources.** More actors need to mobilise their resources to manage and prevent incidents. We propose to establish a national exercise and testing strategy with an associated framework for the cyber domain, to create a competence pool of volunteers to assist in extraordinary situations resulting from cyber attacks, and to initiate a national incentive-driven Bug Bounty programme for socially critical activities



IVA

Royal Swedish Academy of
Engineering Sciences