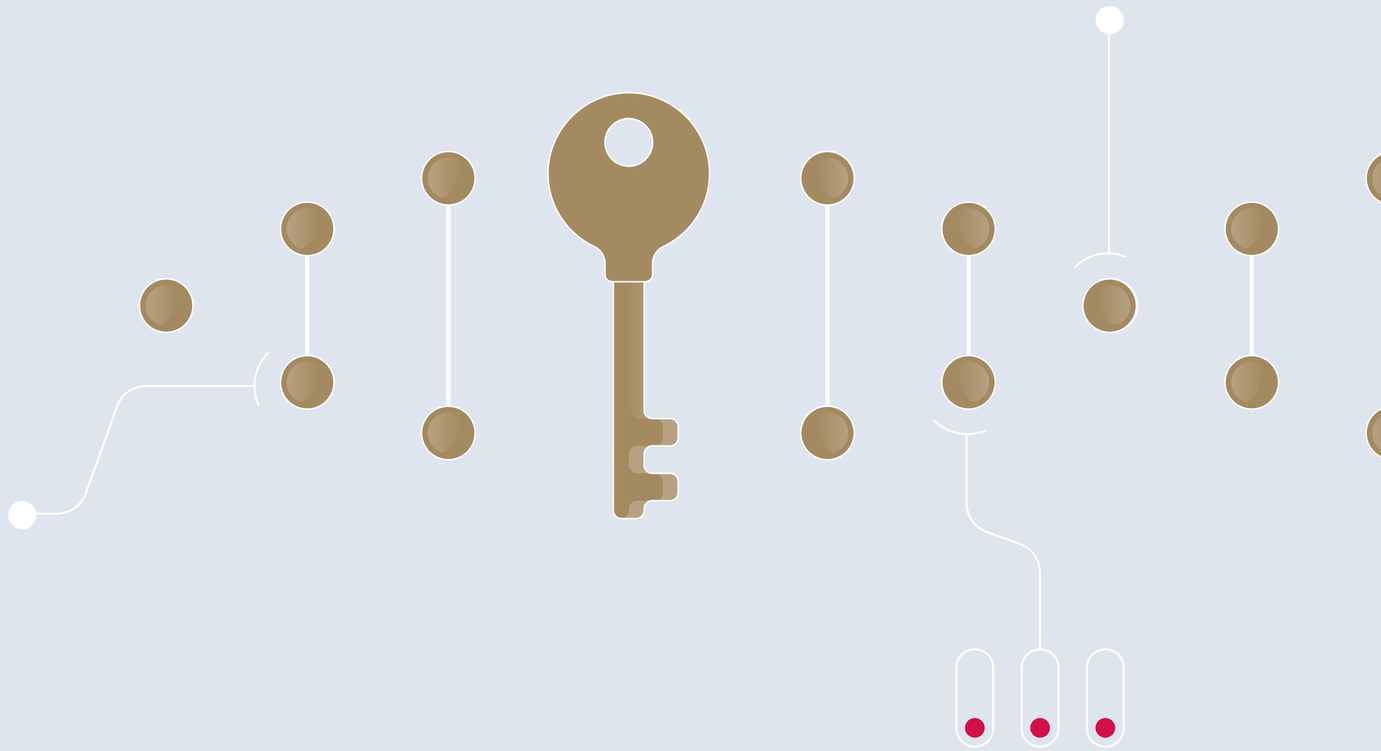
Protect Danish biotechnology and innovation



– and develops prototype for a biological weapon

When working with biotechnology at a university or in industry, you are responsible not only for your own professional integrity, but also for ensuring that knowledge and insight from your work are not exploited in ways that compromise Denmark's security interests.

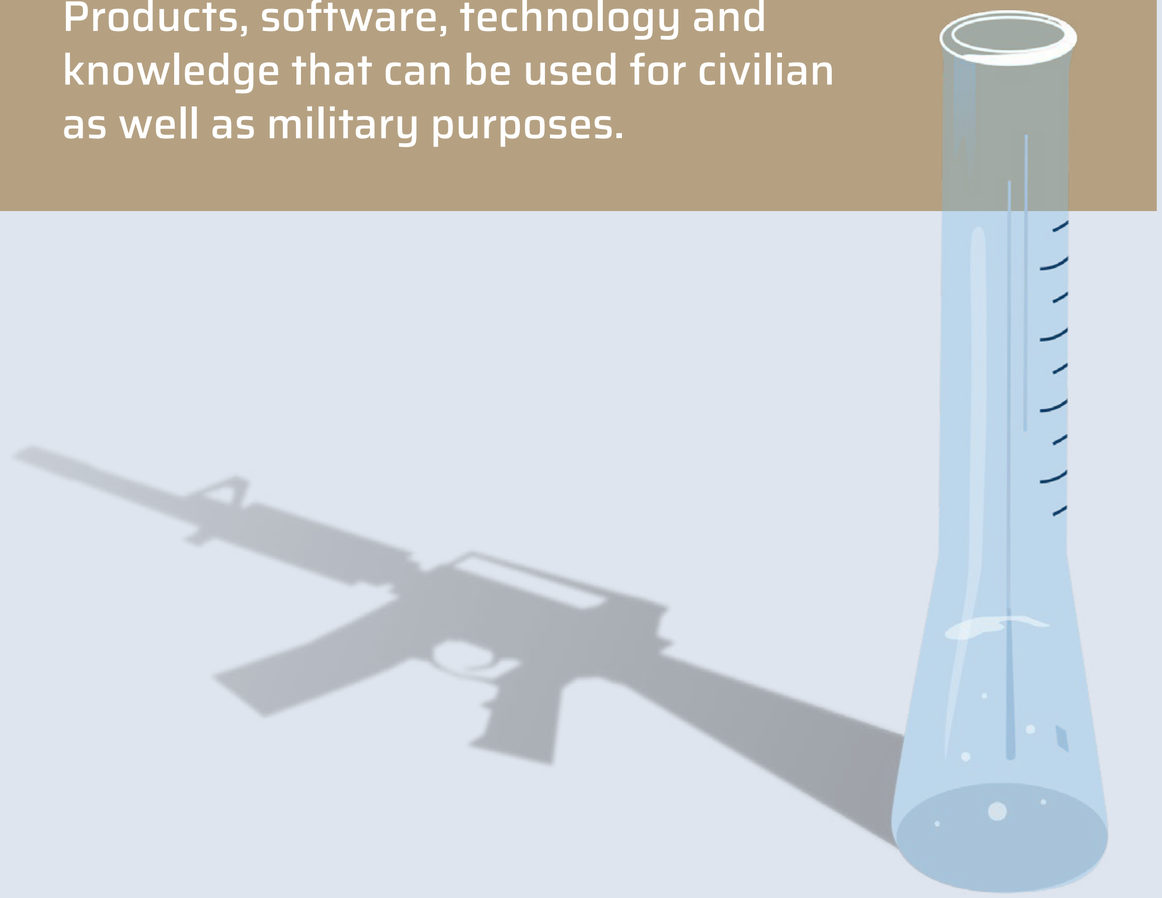
PET recommends that you actively address and consider potential risks associated with your collaboration agreements, appointments and projects – whether national or international. You should be aware of who you are collaborating with, which data and information you share, and who is funding your projects or your company. This is particularly relevant if your work involves biotechnology with dual-use potential. Consequently, you should consider whether the specific knowledge or technology you are working with has a potential for dual use.

The threat to biotechnology in Denmark

Denmark is at the forefront of biotechnology development in several areas, and biotechnology represents a field with significant economic potential, but also with a potential for dual use, since much of the technology can be used for military purposes. Therefore, your work contributes to one of Denmark's most important, but at the same time most vulnerable, research and development fields.

Your research and development may be a possible target of espionage and unwanted knowledge transfer by non-like-minded states seeking to acquire the most recent biotechnological knowledge. If your work falls into the wrong hands, there is a risk that you inadvertently help non-like-minded states strengthen their military capabilities or surveillance efforts.

Dual use:
Products, software, technology and knowledge that can be used for civilian as well as military purposes.



Civilian and military potential

PET assesses that biotechnologies such as synthetic biology and genetic engineering have a great potential in both civilian and military fields. The threat to biotechnology is not limited to the specific development of biotechnology, but also extends to related technological fields affecting this development, for example artificial intelligence, automation, robotics and cloud technology.

Interest from foreign states

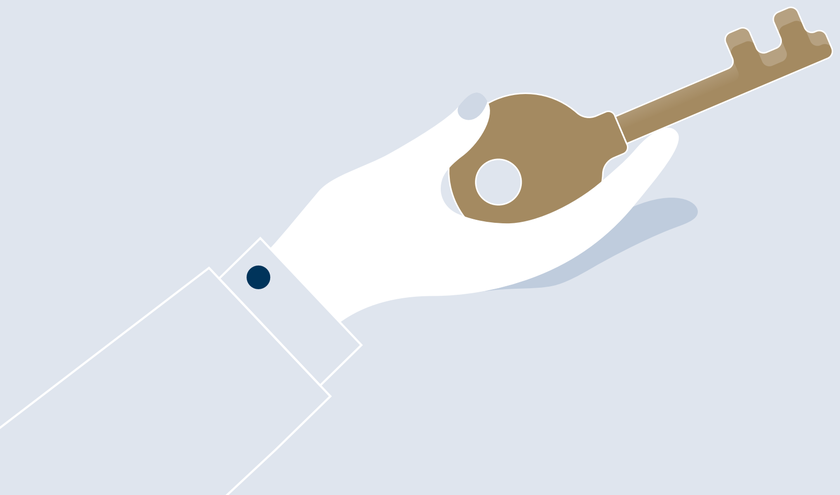
China is particularly focused on biotechnology that can be used for military purposes, and PET assesses that China is prepared to go to great lengths to acquire knowledge in strategically prioritized areas, such as biotechnology. Russia and Iran have also shown an interest in biotechnology with dual-use potential.

Contact and resources:
www.pet.dk/secureinnovation

Illegal technology transfer constitutes a direct violation of the rules of espionage and export control, while unwanted technology transfer involves cases where the technology is not subject to regulation, but the transfer is nonetheless contrary to Denmark' s strategic interests. Unwanted technology transfer takes place for example in connection with research or business cooperation in the field of biotechnology.

What can you do?

When assessing whether granting access to your biotechnology community is worth the risk, PET recommends that you consider various factors before choosing a new supplier, accepting a new investment or forming a new partnership.



Consider the following before allowing anyone into your biotechnology research community

01 **What you excel at could be what others want**

Consider why your research or your company is particularly interesting to others. Be sure to protect the areas where you excel.

- Is it clear who is behind the interest in your work?
- Would a potential partnership offer unique benefits to you?

02 **Your work may have strategic, military or political value**

Consider the risk of your work being exploited for unintended purposes. Even if your work is aimed at civilian use, it could have potential for military application, especially for non-like-minded states such as China and Russia, which also strive for a world-leading position in the biotechnology field.

- Could the technology also be used for military or surveillance purposes?
- As part of your work, are you processing sensitive data, e.g. relating to health, the population or infrastructure?

03 Know who you are actually collaborating with

Consider how much you know about a potential collaboration partner. It is essential that you know about their background – including any aspects that they have not told you about. In-depth knowledge about the background of a potential collaboration partner puts you in a better position to assess, for example, whether they have ties to the military of non-like-minded states or to unwanted civilian actors.

- Do the publications and collaborations listed by the partner align with the information you can find online?
- Does the person or organization have any current or previous affiliation with military institutions?
- Does the partner have ties to actors in high-risk countries or on sanctions lists?

04 Collaboration can offer digital, academic and physical gateways to your work

Consider the access granted to others through the collaboration. Think about the potential exposure of your work – not just physically, but also through digital access and access to specialized knowledge, and make sure that your partner does not gain insight into strategies, plans or ideas that you do not want to share with them.

- Will your partner be allowed entry to physical facilities that can reveal important details about your research or production?
- Will you have to give others insight into your most important data, products or new ideas?
- Will the collaboration allow the partner access to critical infrastructure or large data sets containing sensitive information?

Contact and resources:

www.pet.dk/secureinnovation