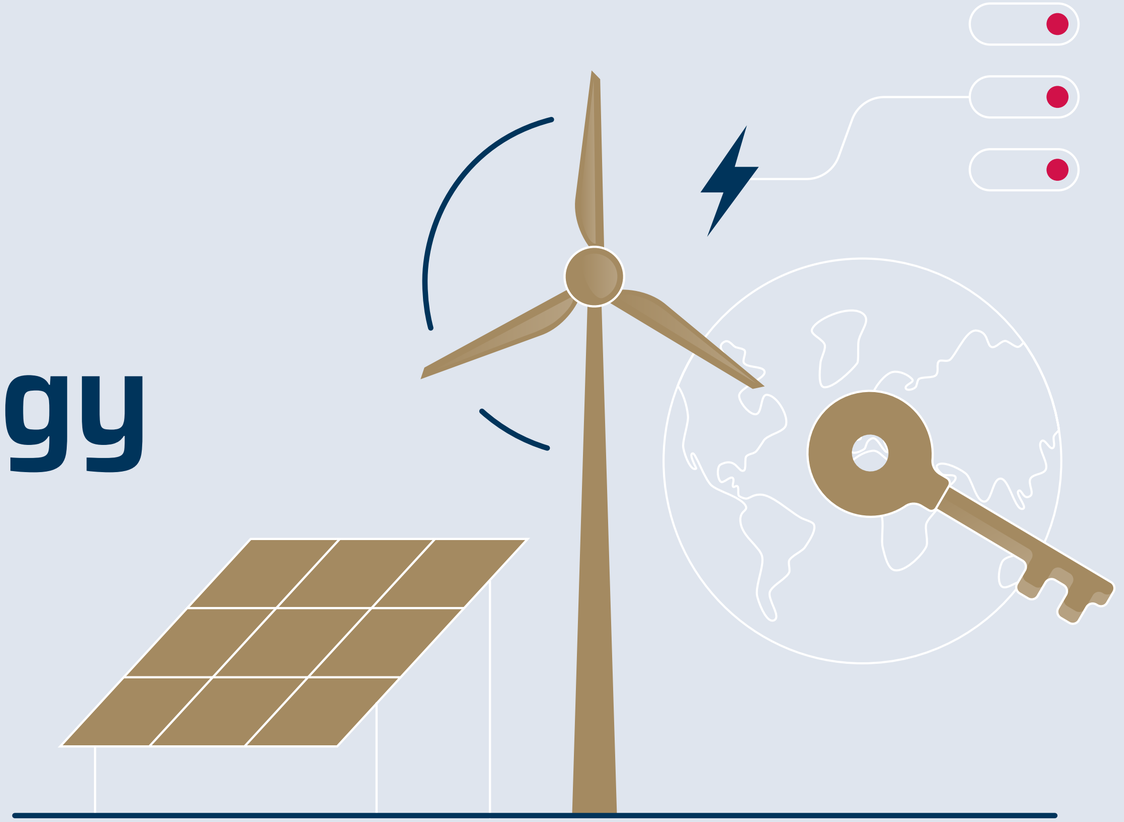
Protect Danish energy technology and innovation



– and maps every cable in the Baltic Sea

As part of the energy technology research community 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 the energy technology community are not exploited in ways that compromise Denmark's security interests.

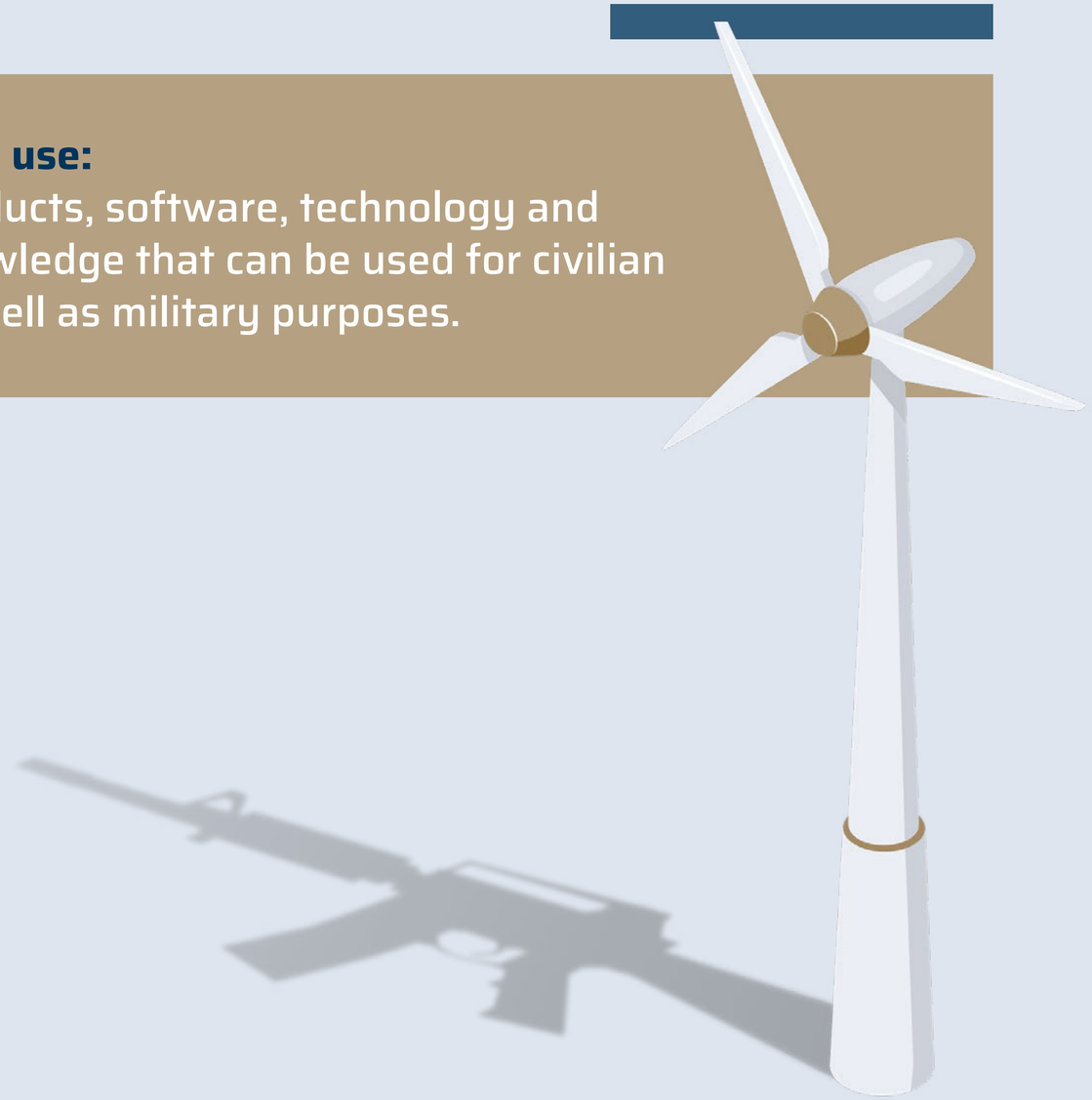
PET recommends that you actively address and consider potential risks associated with your collaboration agreements, appointments and projects – whether national or international. You should therefore be aware of who you are collaborating with, which data and information you share, and who is funding your projects or investing in your company.

The threat to energy technology in Denmark

Danish research and development in energy technologies is internationally recognized, and energy technology will be crucial for Denmark's future economy and security of supply. Therefore, your work contributes to one of Denmark's most important, but also most vulnerable, research and development fields.

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

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

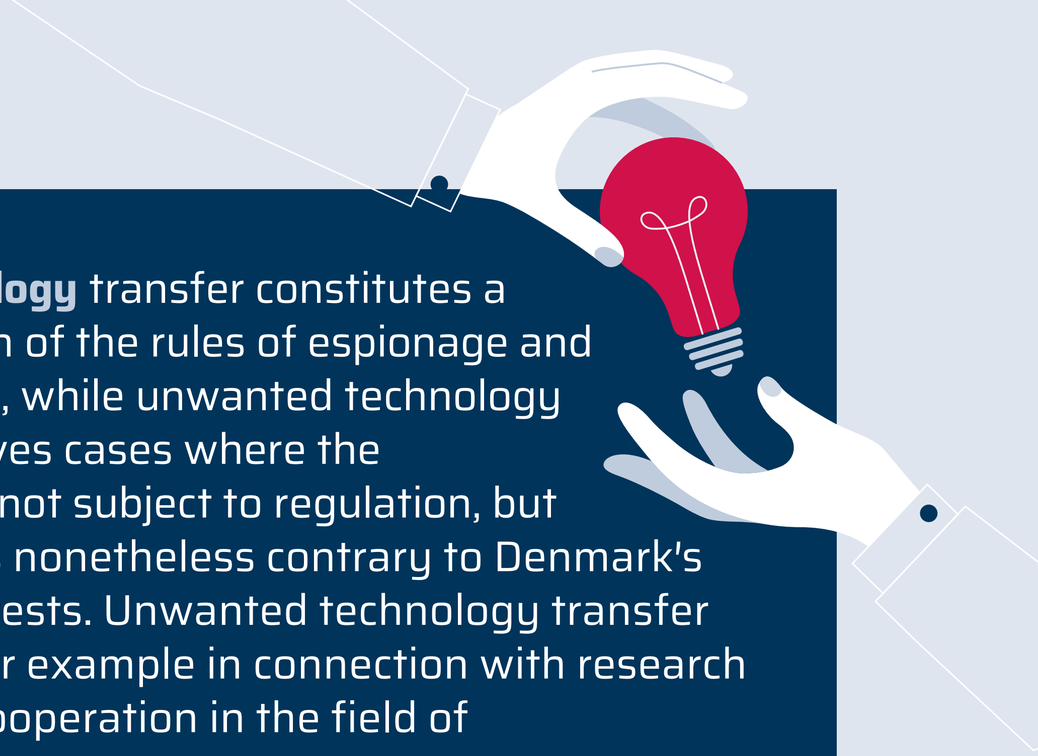


Interest from foreign states

Both China and Russia are prepared to use their dominant positions in the raw materials and critical minerals sector as a means of exerting political pressure. But both countries are also acting more offensively in Denmark. For example, the Chinese intelligence services continuously attempt to collect information on Danish technology and research in the energy technology field.

Furthermore, PET assesses that a sabotage threat emanates from the Russian state, targeting particularly the energy and transport sectors and facilitated by previous espionage activities. The espionage focuses on obtaining important information, for example about IT systems, technical equipment, collaboration partners and employees connected to critical infrastructure in Denmark. This also poses a significant risk of unwanted knowledge transfer.

Contact and resources:
www.pet.dk/secureinnovation



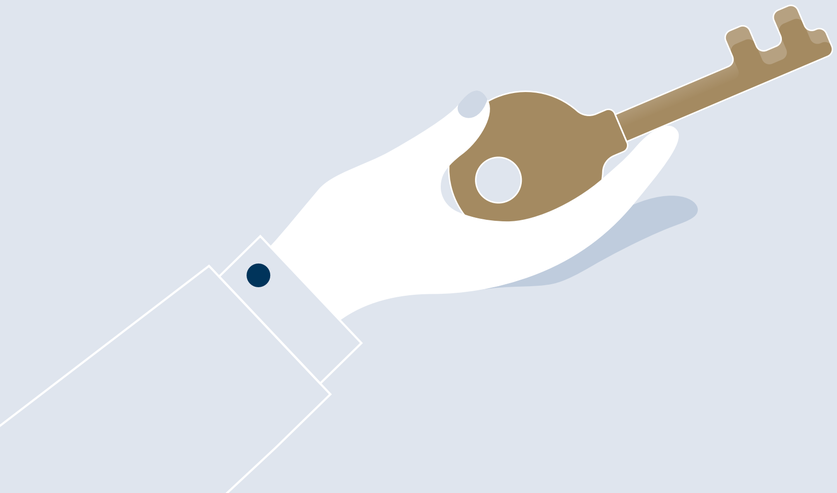
Illegal technology transfer constitutes a direct violation of the rules of espionage and export control, while unwanted technology transfer involves cases where the technology is not subject to regulation, but the transfer is nonetheless contrary to Denmark's strategic interests. Unwanted technology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

Civilian and military potential

PET assesses that energy technologies such as storage and conversion technologies and modular nuclear technologies have a great potential in both civilian and military fields. The threat to energy technology not only relates to the specific development of energy technology, but also to technologies that are foundational for Denmark's energy supply and critical infrastructure, for example semiconductors, cables and battery storage systems.

What can you do?

When assessing whether granting access to your research 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 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 energy technology 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