# Protect Danish quantum technology and innovation

– within the Russian military

As part of the quantum 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 your quantum 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 be aware of who you are collaborating with, which data and information you share, and who is funding your projects or your company.

# The threat to quantum technology in Denmark

Danish research into quantum technology is internationally recognized, and quantum technology will have a major impact on the future economic and military landscape. Therefore, your work contributes to one of Denmark's most important research and development fields.

Due to Denmark's strong position within this research area, your work 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 quantum 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 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 quantum technologies such as quantum computers, quantum sensors, quantum communication and quantum cryptography have a great potential in both civilian and military fields. The threat to quantum technology not only relates to the specific development of quantum technology, but also to technologies that are foundational within the different research areas, for example refrigeration technology, laser technology and other photonics-based technologies.

## Interest from foreign states

Both China and Russia are investing in quantum technology with military applications in mind. PET assesses that the Chinese state is prepared to go to great lengths to acquire knowledge in strategically prioritized areas, such as quantum research. The Russian intelligence services continuously attempt to collect information on Danish technology and research in the quantum field, which 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.

# What can you do?

When assessing whether it is worth the risk to form a partnership that will give others access to your research community, PET recommends that you consider various factors before choosing a new supplier or accepting a new investment.

## Consider the following before you enter into a collaboration

### 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 quantum 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 infrastructur?

## 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.

- 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 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**