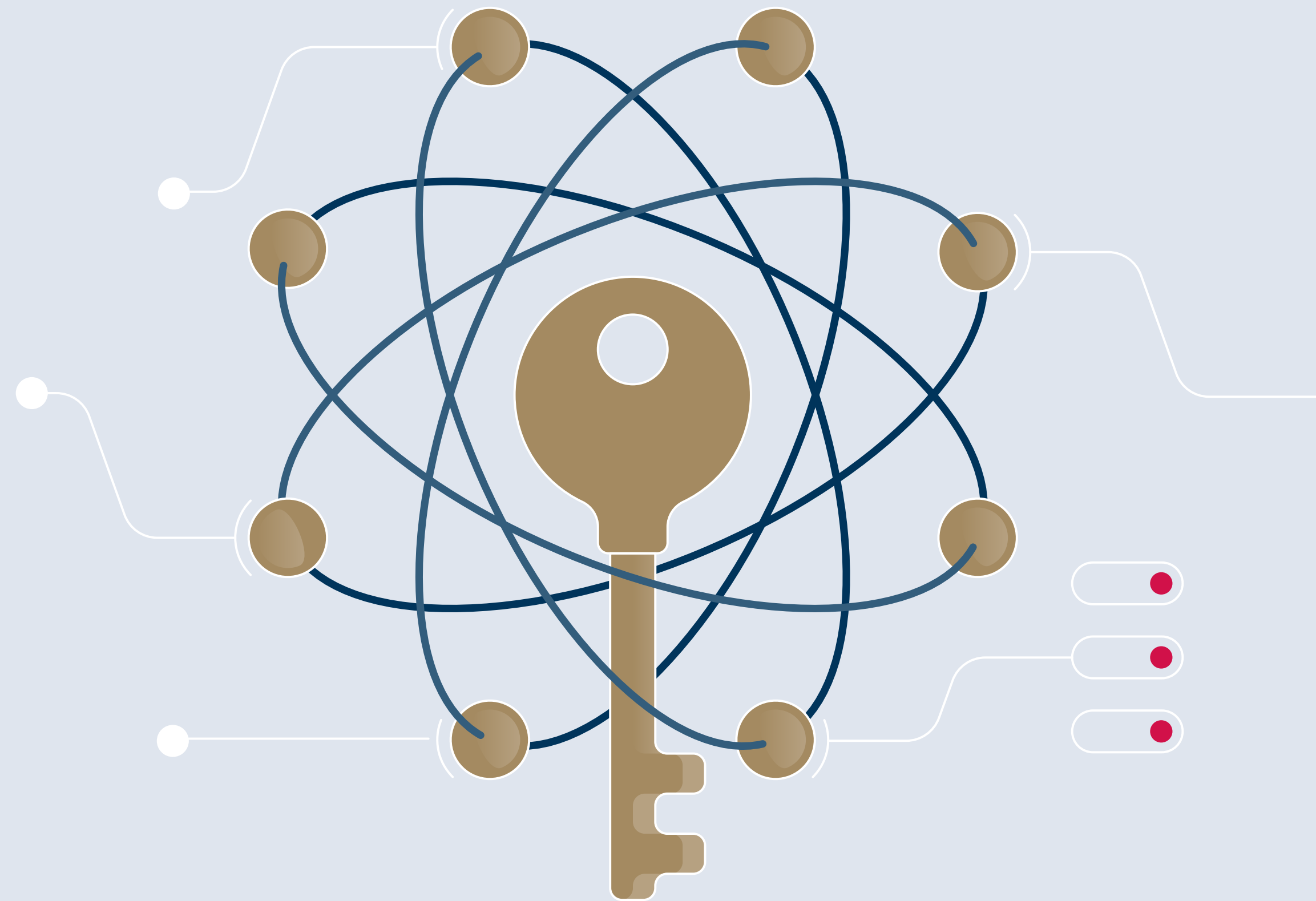
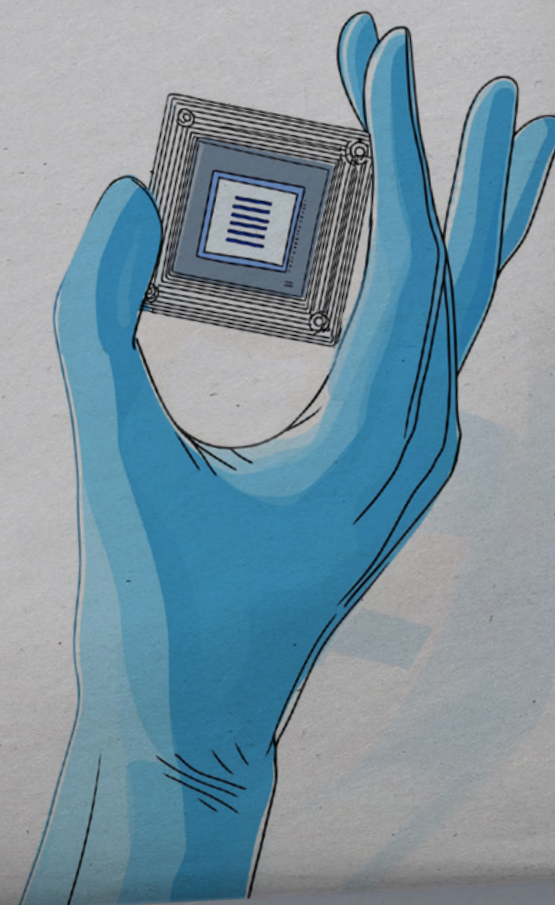


Beskyt dansk kvanteteknologi og innovation



SEKTION 1 – INDLAND

Kvantesensor fra dansk universitet opnår stor anerkendelse



– i det russiske militær

Som en del af kvantemiljøet på universiteterne eller i industrien har du ikke kun ansvaret for din faglige integritet, men også for at sikre, at viden og indsigt fra dit kvantemiljø ikke bliver udnyttet i sammenhænge, der strider mod Danmarks sikkerhedsinteresser.

PET anbefaler, at du aktivt forholder dig til og overvejer mulige risici i dine samarbejdsaftaler, ansættelser og projekter – både nationale og internationale. Du bør derfor være opmærksom på, bl.a. hvem du samarbejder med, hvilke data og informationer du deler, og hvem der finansierer dine projekter eller din virksomhed.

Truslen mod kvanteteknologi i Danmark

Dansk forskning i kvanteteknologi er internationalt anerkendt, og kvanteteknologien vil få meget stor økonomisk og militær betydning fremover. Derfor er du med dit arbejde en del af et af Danmarks vigtigste forsknings- og udviklingsområder.

Som følge af Danmarks styrkeposition inden for forskningsområdet kan din forskning være et muligt mål for både spionage og uønsket vidensoverførsel fra ikke-ligesindede stater, der ønsker at erhverve sig den nyeste viden inden for kvanteområdet. Hvis dit arbejde ender i de forkerte hænder, risikerer du uforvarende at bidrage til at styrke ikke-ligesindede staters militære kapaciteter.

Dual-use/dobbelt anvendelse:

Produkter, software, teknologi og viden, der kan anvendes til både civile og militære formål.



Civilt og militært potentiale

PET vurderer, at kvanteteknologi som eksempelvis kvantecomputere, -sensorer, -kommunikation og -kryptografi har et stort potentiale både civilt og militært. Truslen mod kvanteteknologi retter sig ikke kun mod den specifikke udvikling af kvanteteknologi, men også mod teknologier, der er forudsætningsskabende inden for de forskellige forskningsområder. Det gælder fx køleteknik, laserteknologi og anden fotonik.

Fremmede staters interesse

Både Kina og Rusland satser på kvanteteknologi med militære formål for øje. Det er PET's vurdering, at den kinesiske stat er villig til at gå meget langt for at erhverve viden på de områder, som Kina prioriterer strategisk, hvilket bl.a. gælder kvanteforskning. De russiske efterretningstjenester forsøger til stadighed at indhente oplysninger om dansk teknologi og forskning på kvanteområdet. Også her er der en betydelig trussel for uønsket vidensoverførsel.

Kontakt og ressourcer:

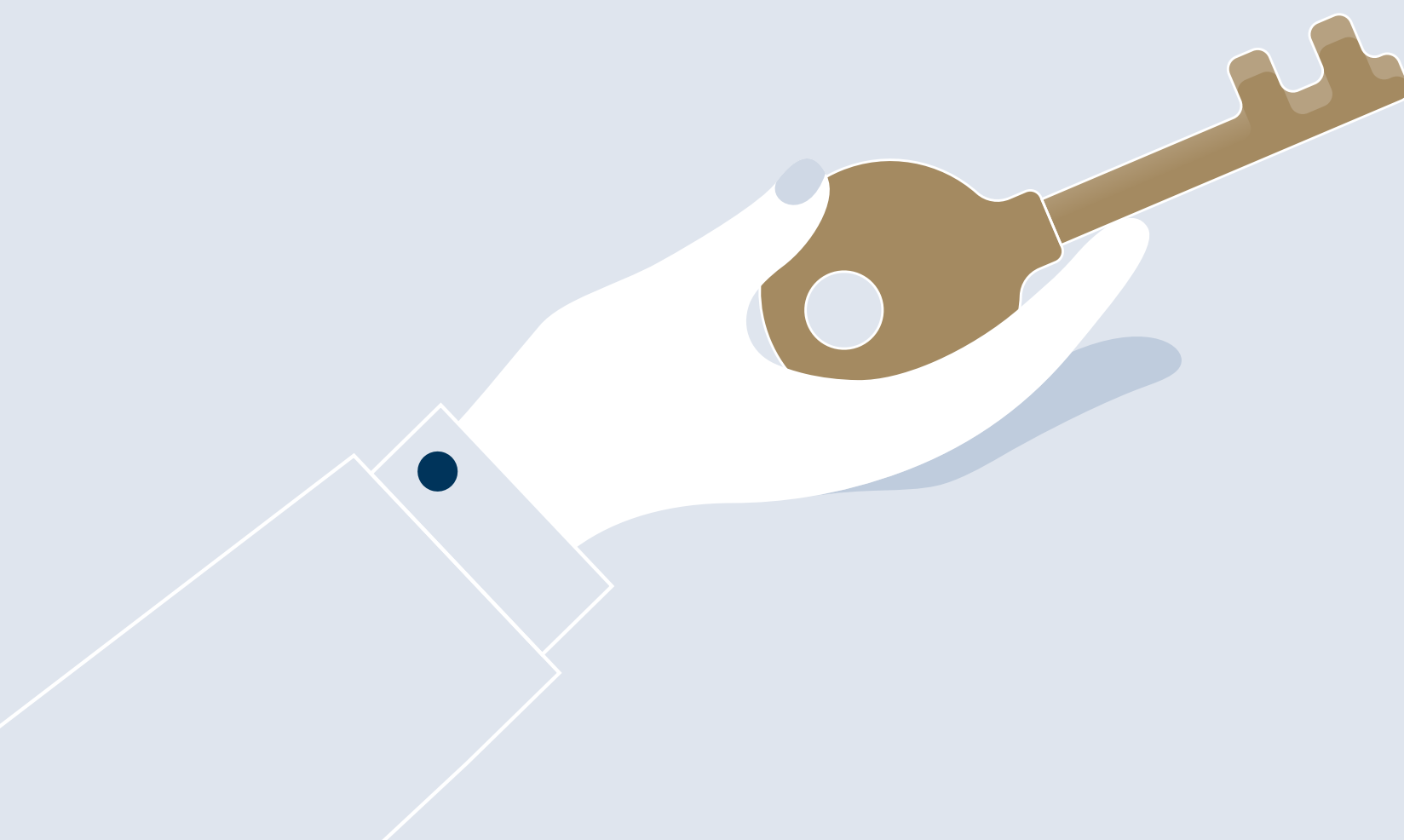
www.pet.dk/sikkerinnovation



Ulovlig vidensoverførsel er i strid med fx spionage- eller eksportregler, mens **uønsket vidensoverførsel** finder sted, når teknologien ikke er reguleret, men kan stride mod Danmarks strategiske interesser. Uønsket vidensoverførsel sker bl.a. i forbindelse med grundforskning på kvanteområdet.

Hvad kan du gøre?

For at vurdere, om det er risikoen værd at lukke andre ind i dit forskningsmiljø, anbefaler PET, at du gør dig en række overvejelser, inden du fx vælger en ny leverandør, takker ja til en ny investering eller påbegynder et nyt samarbejde.



Overvej følgende, før du indgår et samarbejde

- 01 Det, du er god til, kan være det, andre gerne vil have fat i**

Overvej, hvorfor din forskning eller din virksomhed er særlig interessant i andres øjne. Du skal passe godt på det, du er særligt god til.

 - Står det helt klart for dig, hvem der står bag interessen for dit arbejde?
 - Er der noget helt særligt at vinde for dig ved et eventuelt samarbejde?
- 02 Dit arbejde kan have strategisk, militær eller politisk værdi**

Overvej mulighederne for misbrug af dit arbejde. Selvom dit arbejde retter sig mod civil brug, kan det have potentiale for militær anvendelse særligt for ikke-ligesindede stater som Kina og Rusland, der også gerne vil være førende på kvanteområdet globalt.

 - Kan teknologien også anvendes i militær sammenhæng eller til fx overvågning?
 - Behandler du i dit arbejde følsomme data, fx om sundhed, befolkning eller infrastruktur?

03 Forstå, hvem du reelt samarbejder med

Overvej, hvor meget du ved om nye samarbejdspartnere. Det er vigtigt, at du kender deres baggrund – også de dele, de ikke selv fortæller dig om. Dybere viden om dine eventuelle samarbejdspartneres baggrund ruster dig til bedre at kunne vurdere, om de fx har forbindelse til ikke-ligesindede staters militær.

- Stemmer de opgivne publikationer eller samarbejder overens med, hvad du kan finde online?
- Har samarbejdspartneren tilknytning til militære institutioner, eller har denne haft det på et tidligere tidspunkt?
- Har samarbejdspartneren forbindelser til aktører i ikke-ligesindede stater eller på sanktionslister?

04 Digitale, faglige og fysiske adgangsveje til dit arbejde

Overvej, hvad et samarbejde giver andre adgang til hos jer. Tænk over, hvad du potentielt giver andre adgang til – ikke kun fysisk, men også digitalt og fagligt, så en samarbejdspartner ikke får indsigt i strategier, planer eller idéer, som du ikke ønsker at dele.

- Vil din samarbejdspartner få adgang til fysiske faciliteter, som afslører vigtige detaljer om jeres forskning eller produktion?
- Vil du skulle give andre adgang til jeres vigtigste data, produkter eller nye idéer?
- Vil du i samarbejdet give adgang til kritisk infrastruktur eller store datasæt med følsomme oplysninger?



Kontakt og ressourcer:
www.pet.dk/sikkerinnovation

