HÅVARD RUSTAD MARKUSSEN

How Dual Use Puts Research Under the Microscope

A recent case in Norway demonstrates how dual-use controls can constrict international scientific collaboration without offering commensurate protections.

In December 2019, a professor at the Norwegian University of Science and Technology (NTNU) found himself unexpectedly in the crosshairs of the law. The professor, who has never been named publicly, was arrested on suspicion of breaking Norwegian export control rules. After a lengthy legal process, he was charged, convicted, and sentenced by a district court to eight months in prison. His crime? Welcoming four Iranian civilian PhD candidates as guest researchers to his lab, where they had access to a scanning electron microscope (SEM).

SEMs have been commercially available since the 1960s and are ubiquitous in scientific settings all over the world. The technology is essential in many areas of research. Commenting on the professor's case, the rector at the University of Oslo, Svein Stølen, described SEMs as "knife and fork in a lab that treats materials." That said, Norwegian law also classifies SEMs as *dual use*—a technology with both civilian and military applications. SEMs can be used to study aluminum alloys deployed in centrifuges that enrich fissile materials for nuclear weapons. For this reason, in Norway—and many other nations—the export of knowledge about SEMs may require a license, which the professor did not obtain.

On appeal, the decision was overturned and the professor acquitted. The higher court noted that use of an SEM is exempt from licensing where such use constitutes basic research and where knowledge of such use already exists in the public domain—conditions that applied in the case of the professor and his guests. Still, the legal ordeal, which lasted four years, ended the man's academic career. The case also led to constrictions on Norwegian higher education and laboratory work: Research institutions have established increasingly firm controls on international collaboration and are now considering outright bans on collaboration with researchers from "red-listed" countries, most prominently China. The successful appeal has made no difference to administrators, who have made clear that universities will engage in hyper-enforcement to ensure that the authorities stay away from their doorstep.

Despite the acquittal, Norway's regulatory framework for classifying and controlling dual-use technology puts international research cooperation—and accordingly, scientific progress—under political pressure. To what end?

The purpose, in theory, of labeling and then regulating technologies as dual use is to prevent potentially destructive tools from falling into the wrong hands. But the label is increasingly arbitrary; by some arguments, all research and all technology are dual use. Under such a framework, any and all research can be presumed potentially dangerous, enabling the imposition of security protocols on any research collaboration and knowledge-sharing that "crosses the line," regardless of how indistinct that line may be to researchers. Unsurprisingly, security

concerns are then used as a cudgel against politically disfavored researchers, such as the Iranian guests and the NTNU professor, himself partly of Iranian descent.

Dual use export control is common the world over. In the United States, as in Norway, the dual use regime fosters suspicion surrounding research, leading to *prior restraint*, or censorship before the expression—in this case, publication of research—occurs. For example, US research on artificial intelligence is subject to special scrutiny and limits on knowledge-sharing, which incentivizes secrecy, discourages university-based researchers (many of whom are foreign born) from involvement in the field, and potentially limits innovation. These obstacles to academic collaboration contribute to AI research moving out of universities and into the private sector, which will determine how the technology is developed in the future.

Protecting fundamental research requires export control systems that are designed to be sensitive to the need for scientific collaboration and research openness before they are enforced. It's notable that even though the verdict of the NTNU case was overturned, it did lasting damage to the professor's career and to Norway's culture of research collaboration. Rather than continuing down this path, the research enterprise should consider alternatives to the dual use framework that better support nonproliferation and other security concerns without sacrificing scientific development.

A brief history of dual use policy

With some stretch of the imagination, all tools, no matter how benign, can be used for military as well as civilian purposes. Of course, some technologies have greater potential for harmful use than others. During the twentieth century, this reality became too urgent to ignore, particularly as mustard gas and chlorine were appropriated for chemical weapons and conceptual research on atoms led to the development of nuclear bombs. After World War II, the notion of dual use entered national and international legal frameworks, becoming an important concept in the regulation of research.

The first major international accord on dual use was established in 1949, with the Coordinating Committee on Multilateral Export Controls, or COCOM. Joined by NATO allies—principally the United States—plus Japan and Australia, COCOM was designed to control export of dual-use technologies, goods, and research to the Warsaw Pact countries, as well as to China and later North Korea and Vietnam. COCOM expired shortly after the end of the Cold War. The existing framework was dissolved in favor of an alternative export control regime that would include Russia and newly independent former Soviet states as members, in hopes of involving them more fully in diplomacy and international trade.

The post–Cold War export control regime, launched in 1996, is known as the Wassenaar Arrangement. Its 42 member states are obligated to enforce controls of dual-use items as specified in the agreement's authoritative, 250-page manual. In addition, Wassenaar limits "intangible transfer of technology"—that is, communication of knowledge about use of the listed items. In this way, the system controls not only the distribution of physical goods but also other activities like international research collaboration. Unlike COCOM, Wassenaar is not directed toward specific countries; it does not target particular states, like the former Soviet Union, for technology export bans. Rather, Wassenaar signatories are expected to report on the control of exports of specified technologies and research to any country, including those not party to the arrangement, and especially to countries of concern to the members.

On paper, at least, the Wassenaar Arrangement is still operative today. But it is quickly losing force, as Russia often blocks attempts to build consensus among signatories—a problem that has worsened since its full-scale invasion of Ukraine in 2022. Furthermore, China is a notable nonmember. Given concern about China's pursuit to integrate its civilian and military technology development capabilities, its absence from Wassenaar significantly limits the arrangement's effectiveness.

As Wassenaar's legitimacy and usefulness wane in concert with a general decline of multilateralism, states and international bodies are increasingly turning to sanctions against specific countries and individual technologies to curb the export of dual-use goods. For instance, the European Union's sanctions on Russia in response to the invasion of Ukraine include strict controls on dual-use exports. US policy restricting the export of semiconductors to China offers another example. Any given state may have a distinctive national export control strategy, involving a potpourri of limits on dual-use technology and research.

The regulation of dual-use goods and research is supposed to support national security. Today, however, the dual use concept has turned scientific laboratories into arenas where scientists must navigate the complexities of geopolitical competition, while the greatest risks occur elsewhere. This misplaced scrutiny is curtailing scientific trust and collaboration without considering how such scrutiny itself may harm national interests.

How the dual use idea stymies research

When the NTNU materials science professor was arrested for exporting knowledge about SEM without a license, the very activity of international collaboration in scientific research, and more concretely the practice of inviting guest researchers into the lab, became suspect. Testimony during the appeal proceedings confirms as much.

In court, one of the professor's former colleagues explained that NTNU had dramatically altered its approach to research security in the wake of the professor's arrest and conviction. In the past, the colleague said, he had never applied for an export license when providing Iranian and Chinese PhD students and

postdocs access to SEM equipment and training. No one at the university raised security concerns. But in the wake of the conviction, the university instituted strict requirements for export license applications and began performing thorough background checks on potential new hires and even guest researchers. "Everything goes through the head of security at the university," the witness testified.

In a security-first environment, where bureaucrats decide whether scientific collaboration and hiring is permitted, researchers give up on collaboration and forego hiring. Nils Halberg, a professor of biomedicine at the University of Bergen, described applying for an export license to hire a Chinese researcher, only to find the paperwork held up interminably, threatening Halberg's funding. Speaking to a reporter, Halberg noted that a colleague had been awaiting a license to hire a different Chinese researcher for nearly a year. "I am concerned that good researchers will get tired of waiting and find another job when it takes so long to get an answer," Halberg explained. "Then Norway will lose good researchers." The bureaucratic process ultimately discourages attempts to hire researchers from red-listed countries in the first place. "One quickly thinks in the direction of, 'OK, I have a very good candidate from China. But I also have a candidate who is not quite as skilled, but who can start within a couple of months,'" Halberg said.

Such concerns may become moot as higher education and research institutions pull back on international collaboration. Leaders of NORCE, the Norwegian Research Centre, have ceased all hiring from Iran, China, Russia, and other red-listed countries, citing "risk and security assessments." Meanwhile, a number of Danish universities have cut ties with universities in China and Iran. The deputy rector of the Technical University of Denmark explained that collaboration had been canceled due to the "risk of espionage" and because there "may be a risk that we break export control regulations." The university referenced no specific evidence of espionage, but given the situation in nearby Norway, the risk of running afoul of prosecutors could hardly be more evident. Denmark, then, need not ban collaborations with China and Iran: Its universities will do so on their own for fear that any such collaboration may trigger further restrictions on research.

An alternative to dual use

There are certainly cases in which research and technology ought to be subject to export control, such as those involving nuclear, chemical, and biological weapons. Still, the debate around the efficacy of export controls is ongoing. For example, in the current geopolitical environment, one could argue that US controls on the export of advanced computer chips and semiconductor manufacturing equipment to China were warranted to slow down Chinese innovation. However, as demonstrated by the recent launch of the Chinese AI model DeepSeek, such controls may result in the United States missing out on technological progress developed elsewhere.

In any case, export control policy can and should be guided by a more nuanced and careful risk assessment framework than the dual use classification currently affords. To prevent harm and fairly adjudicate difficult questions without casting all research as suspect, risk should be assessed as it arises in individual cases.

The exceptions afforded by the current law provide a starting point for imagining a new approach. One of these exceptions is awareness: If research processes and findings are easy to find in publicly available resources, then exporting these processes and findings—through collaboration or publication—poses no risk beyond that which already exists. A second condition for exception is the extent to which research is *basic* as opposed to *applied*. Much scientific research is carried out with no specific use case in mind; its purpose is to increase knowledge, not to further the development or optimization of a technology. The NASA-developed technology readiness levels, or TRLs, a widely used scale for evaluating the development stages of technologies, can be employed to demonstrate the basic or fundamental nature of research in specific cases.

An export control regime sensitive to the need for openness and collaboration could, as a threshold matter, rely on common knowledge and basicness to assess the riskiness of knowledge transfer. In other words, these would be the first factors considered in deciding whether technologies and research are controllable. Under the current system, these are exception criteria—applied after the fact—in legal defenses.

In the case of the NTNU professor, a security-first paradigm enabled the presumption that research and research collaboration are risky. Had Norwegian authorities been tasked with assessing the potential damage associated with the unauthorized proliferation of knowledge acquired by the use of an SEM, rather than looking up a specific technology in a list of what is considered dual use, they would have likely moved on from the professor's case, and NTNU would not have become a high-security environment where collaboration is discouraged. Instead, today institutions and researchers inside and outside the country have started digging moats and erecting high walls around domestic research.

Policymakers should consider retiring the dual use concept and establishing in its place a more detailed taxonomy of risk for scientific research. Such an effort would be a complex undertaking involving a great deal of study and care, but a course correction of the climate surrounding international research collaboration requires a paradigm shift. By moving beyond dual use, we can set aside the presumption that science itself is a security issue and focus instead on genuine risks, all the while developing and sharing knowledge safely.

Håvard Rustad Markussen *is a senior researcher at the Nordic Institute for Studies of Innovation, Research, and Education.*