Knowledge Security at Stake

A free, open, and international research and education environment is essential to scientific progress. At the same time, geopolitical tensions pose new challenges to the science, technology, and innovation sector. In many Western countries, approaches to knowledge security are being developed to protect core scientific values and preserve national interests.

By Leo Eigner

Students protesting against threats to academic freedom in Budapest, Hungary, 21 June 2020.
Bernadett Szabo / Reuters

Research-performing organizations, such as universities and private companies, are at the forefront of scientific and technological breakthroughs and are therefore the fulcrum of geopolitical competition. The global science, technology, and innovation (STI) sector relies on international mobility and cooperation, which has benefited scientific and economic actors around the world. In the last decade, however, evidence has come to light that authoritarian governments, in China, Russia, Iran, and elsewhere, are exploiting the openness of the STI sector to modernize their militaries, strengthen their governance and surveillance systems, and spread propaganda abroad. As it is scientifically, economically, and politically desirable to continue cooperation with these countries, stakeholders in the US, the UK, the EU, Japan, Australia, and other Western countries are trying to balance openness with security. These wide-ranging policies are generally referred to as "knowledge security."

Knowledge security is a broad, ill-defined concept. Certain stakeholders, particularly scientists, dispute whether knowledge can or even should be "secured." Generally speaking, knowledge security refers to the prevention of the unwanted transfer of sensitive information, know-how, and technology, the mitigation of foreign interference in higher education and research, and the reduction of dependencies that could endanger national security and competitiveness. Ethical concerns are also important aspects. The aim of knowledge security is to protect core scientific values, ensure that international cooperation remains ethical and safe, and safeguard national interests and values. Although the concept of knowledge security is new, the practice is not. Export control of dual-use goods that seek to prevent the research and development of nuclear, biological, and chemical weapons can be traced back to the Second World War. Knowledge security – also sometimes referred to as research security – is a broader concept that addresses a wider palette of risks.

Knowledge security risks arise from the highly internationalized STI sector and occur along the entire value chain – from basic research to the manufacture of commercial goods. Economic security and

knowledge security are thus closely interrelated. Responsibility for knowledge security is spread across multiple actors and affects many policy areas, such as education, civil security, intelligence, immigration, foreign investment, and privacy. Knowledge security is, therefore, a joint challenge. Universities and companies are responsible for protecting core scientific values, enforcing export control compliance, and implementing knowledge security measures. Meanwhile, protecting national security and competitiveness is a core duty of the state. Governments play a key role in mitigating risks by sharing information, providing resources, coordinating policies, and supporting research-performing organizations. A piecemeal or incomplete response poses severe risks. Over time, it could erode scientific and economic competitiveness, increase security threats, and weaken core scientific and democratic values. A well-coordinated, strategic response at the intra- and international level is thus needed to address these challenges.

Paradigm Lost

Science is considered a universal language and flourishes in free environments. Academic mobility, international cooperation, and open access to research publications, methodologies, and data are essential to scientific discovery. Following the end of the Cold War, Western governments, companies, and universities rushed to internationalize their STI sectors. Governments in particular promoted the idea that "change through exchange" would lead developing countries to adopt the "Western model" of liberal democracy, a free market economy, and a permissive society. Scientific actors were thus encouraged but also self-motivated to forge institutional links with foreign partners, launch mobility schemes, and grant open access to research material. These policies have become so deeply embedded in the STI sector that they are held as core values by many scientific actors.

The old paradigm of unlimited internationality and openness in the STI sector is increasingly called into question.

Over the years, this internationality and openness exposed the Western STI sector to numerous risks. Knowledge transfer in sensitive areas, like aerospace or artificial intelligence, occurs routinely when foreign students return to their home country. It is also a common challenge for universities or companies collaborating with a foreign partner or client whose independence is not guaranteed or who willingly cooperates with their country's government. This becomes critical when the knowledge or technology in question is used to advance military or surveillance technologies. Where sensitive information is better protected, state or state-affiliated actors have engaged in academic and industrial espionage, cyberattacks, and intellectual property theft. The openness of the Western STI sector has increased the risks of foreign interference, such as the surveillance of researchers and students on foreign soil or the leveraging of dependencies to shape perceptions by suppressing certain topics and spreading propaganda. Researchers also face risks to their own privacy, reputation, and research when collaborating with foreign partners or conducting research abroad.

These infringements are not incidental but part of larger, long-term strategies. The Chinese government, for example, views science as serving the aim of "national rejuvenation" and has made STI a top political priority. China's strategy follows the principle of *ganchao*, meaning to "catch up and surpass" rivals, and aims to indigenize innovation, reduce dependencies, and become the preeminent scientific, technological, and military power by 2049. To achieve this, the government seeks to: acquire foreign knowledge, technology, talent, and capital; promote and protect Chinese assets; and influence global norms for emerging technologies, scientific practices, and governance structures. It accomplishes this through a variety of legal, paralegal, and illegal tactics that inhabit a gray zone that is difficult for Western actors to challenge without appearing paranoid or xenophobic. In addition, new laws, like the Data Security Law, enable the Chinese government to use and modify data gathered or owned by international researchers without their consent, which makes it harder for researchers to work there.

Geopolitical events have sharpened the attention on knowledge security and the challenges faced by the STI sector. Russia's invasion of Ukraine, China's human rights abuses and ambitions in the Pacific, and the increased belligerence between world powers has brought about a shift in policy towards "derisking" and "deglobalization." In addition, the rise of illiberal democracies and so-called swing states, like Turkey, Hungary, or Saudi Arabia, have alerted Western scientific, political, and economic actors to the scale and severity of the risks faced by the Western STI sector. In 2015, the EU adopted a policy of "open innovation, open science, and open to the world." By 2020, this was revised to be "as open as

Knowledge Security Risks

Dependencies are widespread in the STI sector. Due to a lack of public funding, universities in the UK, Canada, and Australia rely heavily on foreign funds and tuition fees. Australian universities depend on Chinese students – the largest contingent of foreign students – for up to 23 per cent of their revenue. This dependency has also spread the culture of social control and censorship to Australian universities. In 2019, evidence that Chinese students were denouncing other Chinese students to their government was a major factor in knowledge security receiving greater attention in Australia.

The **repression and persecution of researchers** is a routine risk. In Turkey, international and local researchers working on sensitive topics have experienced political harassment, delays to visa applications, and arrests. In 2007, Taner Akçam, a leading historian of the Armenian Genocide, was prosecuted under Article 301 of the Turkish penal code for "insulting Turkishness." In China, repression of taboo topics, like Taiwan, Tibet, and the Tiananmen Massacre, have successfully spread self-censorship among researchers at home and abroad.

The **misuse of research** in human rights abuses is common. Since 2016, researchers have collaborated with Chinese law enforcement agencies to collect biometric data, like DNA or facial scans, from ethnic minorities, often without their consent. The Chinese security apparatus collected biometric data from nearly 19 million people in Xinjiang in 2017 alone. It has since deployed genetic-profiling infrastructure for the purposes of surveillance and social control. In Kuwait and Kenya, governments have tried to pass laws requiring citizens (and sometimes foreigners) to submit biometric data but have faced legal setbacks.

Academic hostage-taking is a rare though increasingly common tactic. In 2016, Xiyue Wang, a Princeton PhD student and US citizen born in Beijing, was conducting archival research on the history of the Qajar dynasty when he was accused of espionage by an Iranian court and sentenced to 10 years in prison. Since then, Iran has arrested dozens of scientists, often with dual-Iranian citizen, to pressure Western governments and stoke self-censorship abroad. China also engages in academic arrests to intimidate researchers.

possible and as closed as necessary." In short, the old paradigm of unlimited internationality and openness in the STI sector is increasingly called into question. Scientific, political, and economic actors now regard knowledge security as having an important role to play in national security and competitiveness, in international relations, and for liberal democracy.

The Dilemma

Awareness of knowledge security risks have increased steadily over the past decade. Since the late 2010s, scientific, political, and economic stakeholders have debated these issues and the possible responses. Cutting ties with foreign partners would be bad for international relations and for science, as it would be difficult to disentangle the global STI network and may deprive Western actors from access to important scientific and technological developments abroad. China, for instance, has managed to transform itself into an indispensable partner and become a leader in areas like artificial intelligence, biotech, and space (see CSS Analysis no. 323). The country's capital, talent, research infrastructure, and natural resources, like rare earths used in emerging technologies, make it highly attractive. Decoupling would be disruptive and curb scientific and technological progress.

The other extreme of doing nothing is also a bad option. A business-as-usual response would irresponsibly expose the STI sector to further exploitation, infringe upon core scientific and democratic values, risk the manipulation of dependencies, and weaken the ability of Western countries to shape ethical standards and the governance of emerging technologies. Doing nothing or too little would aggravate national security risks, such as unwanted knowledge transfer to China's military universities, as well as erode national competitiveness.

The third option is to reassess and recalibrate scientific cooperation and economic ties with difficult foreign partners. This is the most sensible but also the most difficult option. It requires a finely tuned balancing act between keeping science open and mitigating risks. These risks are very granular, multifaceted, and constantly evolve, requiring a sustained monitoring and mitigation network among multiple scientific, political, and economic actors. To achieve this, stakeholders must come together and agree on how best to respond to these challenges. Unfortunately, stakeholder groups have very different perspectives on knowledge security.

Stakeholder Perspectives

Political actors, like government agencies or parliamentarians, tend to treat knowledge as power. To them, basic research and commercial products are the source of national prosperity, competitiveness, and security. It is the basis of innovation, a guarantor of sovereignty, and a bargaining chip in international relations. As states see themselves as being in competition with one another and understand collaboration as being part of that competition, political actors are sensitive to knowledge and technologies falling into the wrong hands. When laws, values, or institutions are being undermined, political actors are quick to perceive and fear that this will lead to social and political instability in the long term.

In recent years, Western political actors have become increasingly concerned by the range and scale of knowledge security incidents as well as frustrated by the STI sector's lack of response. This has occasionally led to bad policies. A case in point is the China Initiative launched by the Trump Administration in 2018. It aimed at tackling Chinese academic and industrial espionage but was widely criticized for indiscriminately targeting Chinese and Chinese Americans, often on poor evidence, and stoking xenophobia. In general, political actors perceive STI as a form of statecraft, view knowledge security through a security lens, and, if left to their own devices, tend to opt for top-down approaches.

Scientific actors, like universities, funding agencies, or individual scientists, generally believe that knowledge is – or should be – free. This is a matter of principle but also of practice. As science flourishes in free environments, scientific actors generally oppose measures that restrict open science, international cooperation, and academic mobility. They are wary of knowledge security for the same reasons, but also because they fear the potential infringement of core scientific values and liberties, particularly academic freedom and institutional autonomy. Academic freedom refers to the rights of scientists and students to research, teach, learn, and share their knowledge in and with society without interference or fear of reprisal. In most liberal democracies, academic freedom is a legal, sometimes even a constitutional right, and protects scientific actors from foreign and domestic interference. Institutional autonomy ensures that scientists govern themselves without political meddling and enact policies that are good for science.

Further Reading

Asena Baykal / Thorsten Benner, **"Risky Business: Rethinking Research Cooperation and Exchange with Non-Democracies,"** *Global Public Policy Institute* (October 2020).

OECD, **"Integrity and security in the global research ecosystem,"** *OECD Science, Technology and Industry Policy Papers,* No. 130 (June 2022).

Irna van der Mohen et al, **"Keeping science open? Current challenges in the day-to-day reality of universities,"** *CESAER* (October 2023).

Scientific actors have good reason to believe that knowledge security could lead to political overreach. In the US and Turkey, political actors have harassed and replaced key figures within the STI sector. In 2021, the Hungarian government transformed 34 public universities and institutions into public trust foundations, thereby forcing them to cede all rights to a governing body consisting of members loyal to the government. Despite legitimate misgivings, most scientific actors recognize the need for regulation, which often stems from ethical concerns. In the Netherlands, for example, a research collaboration between Dutch universities and Huawei was criticized by political and scientific actors alike, but for different reasons. While politicians were critical for economic security reasons and because they feared unwanted knowledge transfer, scientists objected to the collaboration because Huawei was implicated in human rights abuses against Uyghurs in China. The threat representation of the collaboration as both a security and human rights risk helped to align stakeholder interests and made the threat actionable.

Economic actors generally treat knowledge as capital. To them, protecting trade secrets, intellectual property rights, and access to production sites is a matter of profit and commercial competitiveness. This is especially true for research-intensive companies, and even more so for those who work in sensitive industries, like robotics or semiconductors. When the knowledge, good, or service produced is of strategic value, then the risks faced by economic actors becomes a matter of economic or even national security. Risks include supply chain dependencies, digital and physical protection of critical infrastructure, and unwanted knowledge and technology transfer. In recent years, industrial espionage has become a serious threat. Between

2018 and 2022, the British domestic intelligence agency, MI5, registered a sevenfold rise in its China-related investigations, most of which were espionage cases targeting research-performing organizations. Another concern is that companies are offshoring innovation. For instance, Microsoft is currently debating whether to relocate a research lab specializing in artificial intelligence away from Beijing following scrutiny from US officials.

A Uniting Front

Despite these different perspectives, most scientific, political, and economic actors agree that the geopolitical context has made knowledge security a necessity – although they still disagree on its urgency. They also agree that protecting core scientific values and preserving national interests is a matter of proportionality. Science cannot be cut off from the world, nor can it be completely open. Instead, a good balance between mitigating risks and promoting international exchange must be found. The main challenge is in finding this balance given the number of individual and institutional actors from different stakeholder groups across multiple countries.

Since the late 2010s, stakeholders have taken various measures to tackle knowledge security risks. A number of universities and academic associations have published guidelines, checklists, and codes of conduct to provide scientific institutions and individual scientists with information and advice. In coordination with government agencies, national advice centers, working groups, and taskforces have been established to provide cross-institutional support, define best practices, and coordinate efforts. Meanwhile, governments, including the US and EU states, plan to revamp existing export controls and screen foreign investments in sensitive areas. In Canada, security agencies have become integrated in the vetting of research funding applications with mixed results. National approaches to knowledge security vary according to the structure and culture of a country's STI sector. Some countries, like France or Canada, are more top-down. Others, like Germany, are bottom-up. The Netherlands has combined both approaches with good results. While certain countries target specific countries, others remain country-agnostic. Coordination has also been established at the international level. In 2023, a G7 working group published a report on knowledge security, and the EU launched the European Economic Security Strategy.

Overall, this variety has led to a patchy, uncoordinated response, but consensus is beginning to emerge. Stakeholders agree that a proportionate approach to knowledge security is best achieved if it is based on the established principles of academic freedom, institutional autonomy, and open science. This entails certain rights and liberties, but also responsibilities. Most actors agree that the responsibility to prevent unwanted knowledge transfer, foreign interference, dependencies, and human rights abuses lies with scientific and economic actors. They are responsible for in-house risk assessment and management, screening foreign investments, and the due diligence of foreign partners and projects. As knowledge security is ultimately a political problem, scientific and economic actors require support from political actors. This support largely consists of empowering stakeholders to act through the provision of information, resources, policy guidance, and relevant legal frameworks. Finally, all actors agree that the complexity of the challenge entails shared responsibilities for awareness-raising, standardizing best practices, and coordinating efforts both intra- and internationally to close loopholes and common vulnerabilities.

The challenge for all stakeholders concerned is to find a way of engaging in strategic competition in an interconnected world.

Taking the Long View

Although knowledge security has received increased attention in the last few years, many challenges remain. Generally speaking, the Western response remains badly coordinated and fragmented. Indeed, fragmentation is a core structural weakness. The bottom-up culture of the STI sector makes decision-making painfully slow. When guidelines and recommendations are coordinated at a national level, institutional autonomy allows each scientific actor to interpret or adopt these differently and creates loopholes. A general lack of awareness and understanding of knowledge security risks among scientists exacerbates risks and protracts the response. Furthermore, the focus on risk assessment and management entails a reactive rather than a proactive response. Though intra- and international working groups exist, Western stakeholders have so far failed to set common priorities, define strategies, and confront the challenges together. Overall, scientific, political, and economic actors prioritize short-term gains (funding, sales, re-election) over long-term interests (national competitiveness, security, and sovereignty), which is a major weakness common to all Western, democratic countries.

In this new era of strategic competition, science and technology lie at the heart of what is likely to be a long, complicated, and uncertain contest, encompassing everything from the mundane to the ideological. The risks that come with globalization and an open STI sector will not go away any time soon. Knowledge security is therefore a long-term policy issue. The challenge for all stakeholders concerned is to find a way of engaging in strategic competition in an interconnected world. There are many possible responses, but whichever is chosen, the new paradigm must be sustainable, adaptive, and calculated to strengthen core scientific values, technological assets and capabilities, and national interests.

For more on perspectives on Euro-Atlantic Security, see CSS core theme page.

Leo Eigner is Senior Researcher in the Swiss and Euro-Atlantic Security Team at the Center for Security Studies (CSS) at ETH Zürich.

CSS Analyses in Security Policy is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editors: Fabien Merz
Language editing: Allyson Chandler
Layout and graphics: Miriam Dahinden-Ganzoni

Feedback and comments: analysen@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses

Most recent editions:

Watching Armed Conflicts from Space No. 336
The Challenges of Wartime Polling in Ukraine No. 335
Geopolitical Echoes of the Karabakh Conflict No. 334
The New Frontier of Space Militarization No. 333
Assessing Hybrid War: Separating Fact from Fiction No. 332
The Role of Mediation Support Structures No. 331

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000663049