January 15, 2026

EXPERTS TAKE

Resilient Science: Transatlantic Challenges and Opportunities

An Interview with Alicia Hennig and David Biggs

In this Experts' Take, conducted by Melita Phachulia from ISDP's Stockholm Center for Research and Innovation Security (SCRIS), David Biggs, a Senior Fellow, and Alicia Hennig, Associated Senior Research Fellow at the Institute for Security and Development Policy (ISDP), discuss how Europe and the United States can build resilience in science and research amid growing hybrid threats, disinformation, and intensifying global competition in technology and innovation."

Dr. Hennig, who spent several years working in Chinese academia, offers insights into China's academic environment, institutional structure, and the ethical challenges of international collaboration. Her work bridges business ethics and political science, with a particular focus on responsibility in non-democratic contexts.

Mr. Biggs, a former U.S. diplomat and Senior Policy Advisor at the U.S. State Department, contributes expertise in international science and technology (S&T) diplomacy, with a focus on research security and global collaboration.

The term cybersecurity can carry different meanings—for some, it evokes digital warfare and cyberattacks; for others, it represents tools and systems for protection, resilience, and trust. How do you define cybersecurity in the context of science, technology, and research?

Alicia Hennig: Cybersecurity is both an understanding of strengths and a practical approach to risks. It means identifying the threats you face, managing those risks, and building systems that defend the organization. In practice, cybersecurity is about risk awareness, risk management, and active defense—all aimed at ensuring that an organization can continue its work safely.

David Biggs: I don't see these two as separate definitions - digital warfare and cyberattacks versus tools and systems for protection, resilience, and trust. To me, they are part of the same concept. You use the tools and systems to counter cyber-attacks and digital warfare.

As a former systems administrator, cybersecurity is about being able to control the information and data you have on your digital systems and ensuring it doesn't leak or get accessed when it shouldn't. So, cybersecurity involves tools, resilience, systems, and trust to counter both attacks and leaks. It's about protecting and controlling your digital environment: your information, files, and data, and maintaining access on your own terms: allowing those you trust in, keeping others out.

What can be learned from European and U.S. societies that have successfully responded to hybrid threats targeting critical infrastructure, data, or research institutions? Are there specific models or practices that stand out?

Alicia Hennig: I'm not aware of a single, well-established set of models for responding to hybrid threats, and this looks like an important research gap. What we first need is systematic research to identify promising practices and then assess which elements can be effectively transferred across different social, cultural, and political contexts. A key prerequisite for any such model is that researchers and staff possess a high degree of risk awareness. If researchers have never encountered or considered risks, that lack of awareness will influence their work and reduce the model's overall effectiveness.

David Biggs: One key lesson is that not all infrastructure needs to be accessible. Some systems should be completely isolated, air-gapped from the internet. For instance, some networks running nuclear power plants are air-gapped.

TAKEAWAY

The most important thing to note is that resilient science starts with people and trust. Technology can keep data safe, but integrity and accountability can safeguard the credibility of knowledge. When there is a lack of trust, misbeliefs spread easily and target minds for manipulation. That's when science loses credibility.

So, one takeaway is that physical security is as important as digital security. When I was an assistant sysadmin, my boss once demonstrated this by walking into a trusted client company's building wearing coveralls, unplugging their server, and walking out. They were digitally secure but physically vulnerable. (The company's CIO had challenged him to find a weakness in their systems).

Another lesson is finance: many institutions don't invest in cybersecurity until it's too late. Companies often hesitate to increase their IT security budgets until a breach has already cost them millions. The reluctance to invest in prevention remains a major issue, even though once you lose your data, it's gone.

How does public trust in universities, government, and media affect societal resilience in the face of technological or hybrid threats? What strategies help maintain that trust amid disinformation and information warfare?

Alicia Hennig: Trust is essential, but universities, governments, and media act in different ways, and play different roles in society. Governments should communicate clearly about threats without causing panic so that citizens understand the environment and the state's response. Too often, incidents are not clearly classified or communicated as hybrid threats. Better classification and transparent communication would improve public preparedness. Universities are a particular concern. I see little urgency in research institutions' preparedness or research security, which undermines confidence that they can protect sensitive work. The media generally reports these threats, but accurate, and responsible coverage remains crucial for maintaining public trust.

David Biggs: Public trust is vital. Right now, in the U.S., trust in universities, government, and media is at a low point, and it's causing chaos. When people lose trust in these institutions, they start trusting unreliable actors and conspiracy theories instead.

For example, there are people who don't believe humans affect the climate but do believe the government can control the weather. That's the kind of cognitive dissonance that disinformation exploits.

Education is essential. I recently downloaded a Latvian *"Handbook Against Disinformation: Recognize and Oppose."* I've also seen others. If I remember correctly, Sweden includes disinformation lessons in its curriculum. Every country under hybrid threat, especially from Russia, should have similar programs.

Unfortunately, the U.S. shut down one of its best tools for countering disinformation. When trust in government, academia, and official data collapses, society starts getting into chaos—exactly what we are witnessing in America.

Which cybersecurity strategies best safeguard research networks and sensitive data without unduly hampering international collaboration or innovation?

Alicia Hennig: Protecting research goes beyond cybersecurity. While cyber measures are necessary to protect data and networks, research security is a broader concept. It includes inspecting partners, assessing whether collaborators have ties to security services or hostile actors, and managing physical and organizational access. Cybersecurity always needs to be part of research security, but research security is broader than just cybersecurity and includes additional tools.

David Biggs: That question is probably for the cybersecurity expert, which I am not.

For example, a friend once created a system for a national lab that tracked researchers' physical movement via their badges, raising alerts if someone from one lab spent a lot of time in another. Some might see this as invasive, but in high-security research environments, it's necessary.

Beyond that, my knowledge of modern cybersecurity strategies is about 20 years old.

Should Europe pursue greater strategic autonomy in science and tech, or deepen ties with the U.S.? Where are the strongest opportunities for cooperation and where are realistic areas of divergence?

Alicia Hennig: Maintaining ties with the U.S. remains important because of the depth of talent and research capacity there. However, our cooperation is likely to differ across disciplines. In some fields, such as climate change or social discrimination, research has become more restricted in the U.S., which changes the scope of collaboration. So, I guess, Europe may face new areas of cooperation compared to previous years.

David Biggs: Europe should do both. It should not rely entirely on other countries like the U.S. for vital data and infrastructure, such as satellites or pandemic-tracking databases. Europe should have its own versions or at least maintain partial control, so if another country cuts access or manipulates the data, Europe isn't left vulnerable.

As for cooperation, I see the strongest opportunities at the subnational level between the U.S. and European institutions. For example, state-level partnerships or memorandums of understanding with Maryland, Washington, or university systems like the University of California or Harvard could be more sustainable than relying solely on federal agreements. That's already happening: Maryland alone reportedly has dozens of international agreements.

How can laws and regulatory frameworks protect ecosystems for innovation and research while preserving openness and academic collaboration?

Alicia Hennig: Legal and regulatory frameworks should avoid unnecessarily constraining academic freedom while clearly defining shared responsibilities. These responsibilities must be distributed across levels: organizational measures at the university level, clear institutional policies, and individual accountability among researchers and research groups. When it comes to the openness of the system, ideally, we should maintain it, but we also need to be very clear that certain actors in the world, particularly, China, have been exploiting the open science system. A parallel can be seen in the economic sphere, where liberal and open markets are similarly targeted by state actors. Therefore, developing a strong degree of risk awareness is crucial to understanding where and how openness can be maintained – to whom, for what purposes, and under what conditions.

The concept of openness has changed, and we need to adapt our approach accordingly. In some cases, it will be necessary to establish specific red lines for state actors, rather than applying country-agnostic measures. I am not a supporter of a one-size-fits-all approach. Instead, we should pursue a more targeted approach that address the behavior of

TAKEAWAY

Institutional structures and personal responsibility are both needed for resilience. This tells researchers, policymakers, and communicators to be willing to work together but also to be aware of the risks.

specific countries while still allowing for meaningful and secure international cooperation.

David Biggs: Before drafting new laws, countries should first define their vision – what does effective research security look like in 2035, or 2045? Once that vision is established, they can assess whether their current legal and regulatory systems can achieve it, identify gaps, and adjust accordingly.

Every country will differ. Some may need stronger laws, while others may need to relax overly restrictive ones. For instance, aspects of GDPR could be refined to improve data sharing that's essential for EU and transatlantic security collaboration. So, it's not just about creating new regulations, but about ensuring the existing frameworks support the desired future state. When a country starts off by coming up with new laws or regulations before they fully visualize the solution, though, it usually leads to questionable results.

Looking ahead, what joint initiatives, platforms, or mechanisms could Europe establish to strengthen resilience against disinformation and other hybrid threats targeting the scientific community?

Alicia Hennig: There's always the question of whether we need to expand EU bureaucracy or not. Initially, I thought about having a working group at some level, but that might only add more bureaucracy. It's probably wiser to work with people who are already in place and identify the right balance—those who understand risk in research security and research cooperation. Eventually, we need to develop concrete measures.

If we don't establish measures at the European Union level that allow for a certain degree of harmonization across all European countries, we will continue facing loopholes that state actors can exploit to infiltrate our systems. Harmonization is essential, but it's also the most difficult part, as member states perceive risk differently.

Any initiative should therefore focus on practical, risk-based measures and a clear allocation of responsibilities across organizational and national levels. Without clearly defining who is responsible for what—whether at the individual, institutional, or intermediate level, implementation becomes inconsistent and weak.

I believe developing such measures will be important, but I don't think it will happen very soon, to be honest. If not, we will likely remain in a situation where individual countries deal with these issues at the national level, depending on their own perception of the urgency of the matter.

David Biggs: One of my dreams is to have a shared international database for research security. If one country flags questionable activity, that information would automatically appear for all participating countries.

Of course, this would require navigating legal barriers like GDPR and establishing robust checks and balances to prevent misuse. But such cross-border coordination could help safeguard science against hybrid threats.

In a time of disinformation, how can researchers, institutions, and journalists collaborate to protect the credibility of science and public understanding?

Alicia Hennig: Maintaining the credibility of science requires both responsible journalism and strong research integrity. Journalists must accurately represent study methods and findings without overstating conclusions. Their responsibility is to avoid overinterpretation and resist generalization from studies that cannot be generalized.

Researchers, on the other hand, must adhere

to ethical and integrity standards – no falsification, manipulation, or citation games, and remember that public research is often taxpayer-funded, carrying an obligation to produce reliable and meaningful knowledge. Our responsibility is to provide society with something valuable and useful.

When we approach work with this mindset, our research will naturally be perceived as credible. But once we start bending the rules, we undermine the whole idea of science. Every such case erodes public trust in research. The future of research depends on our ability to maintain professional and ethical standards.

David Biggs: The Dutch Embassy in D.C. held a panel discussion on this a couple of months ago. There's been a lot of discussion lately about rebuilding public trust in science. Some suggest that science should "stop being elitist," but I think we should be careful with that idea.

In the U.S., saying "science shouldn't be elitist" can imply that anti-vaxxers or climate deniers should be accepted as just as credible as decades of peer-reviewed research, and that's dangerous. One of the reasons I trust science is because there are some elite scientists that are doing it and continually testing each other's work.

Another major issue is the dominance of disinformation platforms like Fox News which are creating a disinformation bubble that one third of the United States is living in, and you have similar disinformation sources here in Europe. I know that Germany has a couple, I've seen others that are very much funded by the Russian government for instance, or through other means. If those disinformation platforms are out there and are sold as truth and as reporting facts, I think we are all going to have a problem. So this is a problem of scale.

You can go and talk to scientists one on one; you can go to the public, you can go to state fairs and help people understand why they should trust science. That's great, but if you get five people that day to change their mind about science, Fox News has reached 4 million people that same day, and you are never able to win that battle.

So, somehow, something needs to happen with all the false, disinformation, and misinformation platforms that are selling themselves as news and truth and I don't know what that is. And I understand all of the problems with freedom of speech that we run into but at some point, there's a famous case in the U.S. that effectively says freedom of speech ends when you start putting everyone in danger with it.

So, there's a line, I think, these organizations have already crossed, and we need to start reinforcing that line and figuring out how to do that and we need to do that fast because the trust is gone with the organized monetized lying and it will continue down an ever darker road.

TAKEAWAY

Resilient science is about preserving trust in all these things: knowledge, institutions, and each other. Finding the right balance between security and openness is important to make sure that scientific advancements continue to strengthen our democracy instead of weakening it.

In the recent case where Jian Guo, ex-aide to AfD's Maximilian Krah, was convicted of spying for China. What failures in Germany and the EU allowed this, and what changes are needed to prevent similar violations in the future?

Alicia Hennig: The Jian Guo case highlights gaps in inspection and oversight mechanisms. Although the individual held German citizenship, the case suggests that background checks applied in some parliamentary or political contexts and were insufficient compared with the more rigorous screening used for positions with access to classified information. This is not an issue of nationality but rather of the political system the individual is coming from. Such checks should have been conducted more thoroughly in this case, and I hope the experience leads to stronger oversight in the future.

As for Maximilian Krah, it is difficult to assess to what extent he was aware of Jian Guo's ties or how much he cared about them. There is also an ongoing investigation into whether AfD received funding from China and Russia. Krah was not legally obliged to perform background checks, but perhaps there was also a degree of carelessness or indifference. Without full clarification regarding potential money transfers from Russia and China, one crucial piece of the puzzle remains missing, making it difficult to form a complete judgment on the case.

How can the U.S. and Europe better cooperate to investigate intellectual-property (IP) theft and prevent state or non-state espionage targeting research?

David Biggs: In general terms, the U.S. and Europe approach legal issues, including IP, differently: Europe often focuses on protecting the rights of individuals, while the U.S. usually emphasizes protecting corporations. The cultural difference complicates cooperation.

IP theft and research espionage are related but distinct issues. IP theft is usually covered by clear laws. If someone steals IP, they've broken the law. But fundamental research often lacks such protection. If your findings are taken and repurposed, what law was broken? If you hand your pre-publication data to someone and they publish the results under their name, is that a violation of the law?

China often exploits this gray area, arguing that no laws were violated. So, we need clarity – both in defining what constitutes theft and in being clear about the legal and ethical frameworks governing research.

One of the problems with the PRC is that even if you trust people you are working with, or the Chinese institutions, Chinese laws and authorities can force individuals and institutions to do things that they would not otherwise do. Researchers must enter these collaborations with full awareness of the risks and potential consequences to their research and life's work.