June 3, 2024

EXPERTS TAKE

Safeguarding intellectual property in the wake of digital authoritarianism

An Interview with
DR. REBECCA SPYKE KEISER

Dr. Rebecca Spyke Keiser is the Chief of Research Security Strategy and Policy (CRSSP) at the National Science Foundation (NSF). The U.S. National Science Foundation is an independent federal agency that promotes the progress of science and the security of national defense. As the chief of research security strategy and policy, Dr. Keiser provides the chief of NSF with policy advice on all aspects of research security strategy. She is working with and has advocated for a collaborative open research eco-system with policies that can properly protect the research from being exploited by foreign nations. In this interview conducted by Zahra Nayabi, Dr. Keiser explains the methods undertaken by certain actors to restrict the freedom of their own civilians and spread their authoritative values to other semi-democratic or developing nations. She further highlights the importance of securing the nations intellectual property as it plays a key role in hindering the authoritative nations from further developing their technologies, especially in the field of AI as it has been extensively used to suppress dissent and steal information.

Zahra Nayabi: When it comes to digital authoritarianism, the countries that are often brought up are China and Russia. Can you explain how these countries use the digital platform?

Dr. Keiser: When we think of the CHIPS and Science Act of 2022 in the U.S., we usually think about semiconductors. However, the CHIPS and

Science Act also includes countries of concern and, currently, there are four countries: the People's Republic of China (PRC), the Russian Federation, Iran, and North Korea. We are particularly concerned about the PRC and Russia because of their systematic efforts to suppress freedom of speech, change election behavior, manipulate AI, and use facial recognition technology. This comes in the form of disinformation and misinformation where we have found evidence that they are spreading false information about high-level U.S. political figures. They are spreading misinformation and disinformation about the actions of the U.S. government. For instance, the PRC characterizes a lot of activities as being anti-Asia and that the U.S. government is biased against those of Asian descent – which is not true, but this sort of disinformations spreads. Then, of course, there is the concerning news of visual recognition technology to suppress minority groups such as the work of the Chinese government to identify people from the Uyghur population so that they can put them in camps and isolate them. So, we are genuinely concerned about the systematic effort from these countries.

> **"For instance, the PRC characterizes a lot of activities as being anti-Asia and that the U.S. government is biased against those of Asian descent – which is not true, but it gets spread".**

In the CHIPS and Science Act 2022, the government aims to ensure that any entity receiving funding from CHIPS Act will enter into an agreement where it will not engage in "significant transaction" with countries of concern including North Korea, Russia, China, and Iran over material expansion of semi-conductor manufacturing.[1]

Zahra Nayabi: China has been expanding their own brand of digital authoritarianism through the Digital Silk Road Initiative. Can you expand a bit more on that strategy? In what ways can such expansion affect the international community?

Dr. Keiser: What we found is that through the Silk Road Initiative, or Belt and Road Initiative, China is providing funding, infrastructure, and equipment to countries in the Global South. Although the PRC says that the initiative is part of helping these countries develop, we have observed a trend where countries are investing in technologies like visual recognition to monitor their populations. This enables them to identify dissidents and manipulate election behavior, aligning with the ideology of the People's Republic of China. So, we are concerned with this type of influence that is happening through the Digital Silk Road Initiative. To curtail these actions, we in the U.S. believe that we need to form a positive beneficial international collaboration with these countries, and we are working very much in establishing good and beneficial research collaboration with countries in Latin America and East Asia so that we can counter the level of digital authoritarianism that is coming through the Digital Silk Road Initiative.

1 William A. Reinsch, and Thibault Denamiel, "The CHIPS and Science Act Guardrails' Implications for the U.S. Trade Agenda," Center for Strategic and International Studies, April 13, 2023, https://www.csis.org/analysis/chips-and-science-act-guardrails-implications-us-trade-agenda (accessed April 26, 2024).

"Although the PRC says that the initiative is part of helping these countries develop, we have observed a trend where countries are investing in technologies like visual recognition to monitor their populations. This enables them to identify dissidents and manipulate election behavior, aligning with the ideology of the People's Republic of China".

Zahra Nayabi: Due to the open and globalized commercial domains, foreign countries can take advantage of algorithmic manipulation to manipulate and influence information environments. Can you explain more on how algorithmic manipulation works? Can you also give an example?

Dr. Keiser: What we found is that there exists multitude of manipulative tactics at play, particularly in the realm of digital platforms. News reports that appear to be from legitimate sources are spreading misinformation and disinformation, often targeting high-level actors. For instance, there has been news reports about the U.S. ambassador to China, suggesting that he is inciting and encouraging violence within the PRC with his actions, which is not true at all. Additionally, we are also finding out that Twitter feeds uploaded by the U.S. embassy or the PRC over informative content are swiftly shut down. Finally, another worrying trend that we are addressing in the US involves the attempted acquisition of large database containing personally identifiable information about the U.S. citizens by the PRC. However, the intent behind acquiring such data and how it might be used remains uncertain, but it still poses a serious threat to privacy and security. These are genuinely concerning activities.

Zahra Nayabi: On November 9, 2016, the U.S. formally accused Russia of a campaign of cyber-attacks against organizations tied to the Democratic Party ahead of the November 8th presidential election. Alongside that, Russia was also accused of information wars to destabilize the Baltics. Can you explain in what ways Russia uses information to destabilize nations?

Dr. Keiser: To begin with, it tries to polarize the public by spreading disinformation and misinformation followed up by flooding digital platforms so that when somebody signs up for Twitter feed, or some other social media, they would be bombarded with information that is incorrect. For example, in the U.S., messages are amplified to suggest that the government is taking actions to restrict the human rights of its citizens. Take the controversial right to bear arms amendment in the U.S. as an example. We have been finding evidence that the Russian hackers are spreading information that the U.S. government is going to cut off the access to firearms. This type of misinformation, alongside other tactics, is being used as a tool to sway the populace to vote for certain candidates rather than the others. This is extremely concerning and polarizing, which is something that deeply troubles us.

Zahra Nayabi: Moving away from this topic, China has regularly been accused of intellectual property theft, combining that with the race to become a global leader in AI. How does such behavior affect the U.S.' global leadership?

Dr. Keiser: In the United States, it is crucial that we collaborate with our like-minded partners internationally to make sure that we continue to

uphold leadership rooted in the fundamental values that have fueled our innovation and maintained our position as a global leader. This includes funding research and doing research based on competitive advantage and merit-based competition, which we must continue to do.

Attempting to restrict certain fields like AI would only serve to benefit our competitors because the way that research works is that we must openly publish research in areas like AI so that other researchers can take that information and challenge it and improve upon it. That is how innovation happens. So, I think that the way to succeed in this competition is to keep our values open even in the fields of AI. At the same time, we must realize that because we have competitors who may exploit this openness for unethical and harmful purposes, we must therefore implement safeguards.

> **"Take the controversial right to bear arms amendment in the U.S. as an example. We have been finding evidence that the Russian hackers are spreading information that the U.S. government is going to cut off the access to firearms. This type of misinformation, alongside other tactics, is being used as a tool to sway the populace to vote for certain candidates rather than the others."**

These safeguards involve educating and advising our research community to assess collaborations wisely. For example, if a potential collaborator is associated with or is a member of a foreign entity that is part of military and civil fusion and is doing things for military purposes, we must guide the U.S. researchers, or the like-minded researcher, to understand that research in something like AI might be used for concerning purposes. Consequently, maybe they should not collaborate with that military-related researcher, but rather collaborate with others who are not associated with non-military entities. With such measures, we can keep this system open, and it is working well.

I am excited about the establishment of SECURE. NSF is funding it, and it is going to be used to serve the research community, providing them with the avenue to raise questions that might concern their collaborations. It is an exciting project and I think that other countries such as the UK, Denmark, and the Netherlands are also taking similar steps to establish these kinds of centers to support their research community.

SECURE or CyberSecure is a platform that provides organizations and companies with a security framework customized to their needs. CyberSecure, for example, provides feedback on a company/organizations' existing policies using AI technology. They also have a policy builder function, which helps generate policies on demand.[2]

Zahra Nayabi: How does AI affect the authoritative nature of China's digital world?

2 NSF, n.d., "NSF CyberSecure," National Science Foundation, https://www.nsf.org/digital-solutions/nsf-cybersecure (accessed April 26, 2024).

Dr. Keiser: In China, citizens have long had limited privacy, and with AI, their privacy have been further diminished. The widespread use of AI to monitor Chinese citizens is deeply concerning. Surveillance cameras in many neighborhoods track individuals' movements, raising fears of even greater restrictions on the freedom of speech. If citizens voice their discomfort or dissent, AI can be used to target and penalize them.

Furthermore, AI is already being used to financially restrict the citizens through the social credit system, whereby those with higher credit scores are granted privileges in comparison to those with lower scores who face severe restrictions. For example, citizens who are found to voice their discomfort against the government had their finances and their travel ability completely cut off. While the government considers these measures protective, in reality, they prevent citizens' freedom.

Zahra Nayabi: There have been reports of China creating a web of techniques whereby they use various methods such as intelligence operation, corporate investments, and transactions to gain intellectual property. Has there been any diagnosis for such a complex web of techniques?

Dr. Keiser: I liken these techniques to peeling an onion, each layer revealing a different aspect. So, one layer that we are focusing on is financial transactions. A recent Wall Street Journal article highlighted the money flowing from countries like the PRC into U.S. universities, often with the aim of exerting negative influence, extracting intellectual property, and to taking talent from the U.S. universities to the PRC. To address this, we are focusing on implementing measures to enhance transparency into these financial flows, such as through the CHIPS and Science act. Universities are now required to report on their foreign financial transactions from countries of concern to NSF. Therefore, the system promotes more transparency in that regard.

I think that one of our key challenges is that we have open university campuses, which allow for unrestricted access. To address this, we are implementing NSPM 33, which is a presidential directive focused on research security. It mandates US universities to establish an international travel policy. Many universities currently lack this capability, so raising awareness and implementing safety measures are priorities.

The five key areas addressed in the NSPM 33 policy are:

1. *Disclosure Requirements and Standardization*
2. *Digital Persistent Identifiers*
3. *Consequences for Violation of Disclosure Requirements*
4. *Information Sharing*
5. *Research Security Programs*[3]

When it comes to businesses, I think that most of the companies have these safeguards already in place, but we are also worried about smaller businesses and smaller companies that might not have these kinds of safety measures. Hence, the SECURE center is working with providing information and services to small businesses and universities as part of the program. It is an ongoing effort, but I think that through some of these types of action, hopefully, we will be able to make a little

3 National Science and Technology Council, "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-supported Research and Development, 2022, Subcommittee on Research Security and Joint Committe on Research Environment, https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf (accessed April 26, 2024).

> **A recent Wall Street Journal article highlighted the money flowing from countries like the PRC into U.S. universities, often with the aim of exerting negative influence, extracting intellectual property, and to taking talent from the U.S. universities to the PRC. To address this, we are focusing on implementing measures to enhance transparency into these financial flows."**

bit of dent in safeguarding our research ecosystem.

Zahra Nayabi: A lot of efforts have been made on China and China's attempts at intellectual theft, or even, let us say, misinformation and disinformation. However, it is not only China; there are also many actors who do this for their own advantages. Instead of focusing on specific countries, should these programs not focus more on general?

Dr. Keiser: Yes, we make a conscious effort not to fixate on individual actors because, realistically, we cannot control their actions or those of other countries. Instead, our focus lies on actionable steps that we and our researchers can take to safeguard the system. It is about making informed and prudent decisions.

By educating and informing the public, we empower them to discern between truth and falsehood, providing guidance on recognizing signs of misinformation or disinformation. We also offer strategies for protecting intellectual property, acknowledging that we cannot control external actors. This approach benefits the entire system, and other countries share a similar perspective. I am hopeful that collective efforts will lead to improvements.