CARNEGIE-TSINGHUA
CENTER FOR GLOBAL POLICY

Transcript

CHINA IN THE WORLD PODCAST

Host: **Paul Haenle**
Guest: **Tim Maurer**

Episode 92: Cyber Norms in U.S.-China Relations
September 18, 2017

Haenle: Recently I had the opportunity to sit down with my Carnegie colleague Tim Maurer, fellow at the Carnegie Endowment and co-director for one of Carnegie's newest programs—the Cyber Policy Initiative. At Carnegie, Tim's research focuses on cyberspace and international affairs—namely cybersecurity, human rights online, internet governance, and their interlinkages. Prior to joining Carnegie, Maurer was the director of the Global Cybersecurity Norms and Resilience Project at New America, and head of research at New America's Cybersecurity Initiative. Tim has spoken extensively on cybersecurity issues at the United Nations, and he helped to develop a global cyber definitions database for the chair of the OSCE [Organization for Security and Co-operation in Europe]. During our podcast conversation, Tim and I discussed the growing importance and intersection of cyberspace and international relations, and the potential for cybersecurity to undermine the stability of the international system. I hope you enjoy my conversation with Tim Maurer, and be on the lookout for Tim's newest book, entitled *Cyber Mercenaries: The State, Hackers, and Power*, to be released in January 2018.

And if you like [the] China in the World podcast, please be sure to leave us a rating and comment on iTunes; and of course, head to [the] Carnegie–Tsinghua website for more work from all of our scholars.

Tim, before we delve into issues I wanted to just start by asking you to talk a bit about this new program at the Carnegie Endowment, which you were brought on last year in October to help build. What's the focus of the initiative, this new cyber initiative? What are the aims? What are your goals for it? And how is this unique for Carnegie?

Maurer: Sure, and thanks for having me today, Paul. The Carnegie Cyber Policy Initiative focuses primarily on global cybersecurity, and it grew out of the Nuclear Policy Program at Carnegie, which has been focused obviously on nuclear policy and the stability of the international system. Out of that kind of sentiment, Carnegie made the decision to also look at cybersecurity. As we've seen in the last few years its obviously grown in terms of the topic, but also risen on the agenda, and it's clear now that cybersecurity has the potential to undermine the stability of the system. So, we are [very] much looking at this from the perspective of: one, how does cyber insecurity undermine the stability of the international system, and what can we do to actually increase stability and work with governments to potentially develop some rules of the road in supporting the ongoing process for that.

Haenle: And you said [that] it grew out of the nuclear policy program at Carnegie—George Perkovich, Eli Levite, well-known names in the nuclear field. Is there a thought that—looking at cyber in the future in terms of setting up norms and rules and regulations, regimes—that there are things we can learn from our experience in arms control in the nuclear policy world?

Maurer: Definitely. And actually one of our main projects right now is working with U.S. Cyber Command on updating the cyber analogies book, which focuses on [the] kind of analogies we can make to other security fields; and this includes the nuclear field. And if you look at the international processes in the last few years, a lot that of that actually emulates what we saw during the Cold War. On the one hand, we have the establishment of hotlines between countries, very much like what we saw during the Cold War after the Cuba crisis. A lot of discussion about escalation dynamics that mirrors the discussions of the Cold War. And a final point on that, a lot of people actually compare where we are currently with regard to cybersecurity to the discussions

of the nuclear space in the 1950s. There are obviously limitations to that analogy—cyberspace and the internet [are] very, very different in many ways as well—but in terms of process and how the field has evolved, there are also a lot of things we can learn.

Haenle: [A] very new field and a lot of work to be done, so we're glad you're at Carnegie as part of this new program. I want to provide our listeners [with] some context on this topic, and wanted to ask you if you would just define cybersecurity for our listeners; introduce, if you could, the policy aspect of cybersecurity, and how cybersecurity is addressed in international relations.

Maurer: Let me start with a technical definition. If we look at the standard by the International Standardization Organization, they would define cybersecurity as anything that undermines the availability, confidentiality, or integrity of information. That's the technical term. Now if we look at the political level, then you quickly get into the political negotiations. Cybersecurity, by the U.S. government, and most European or western countries, is defined more from the network security aspect—so much more technical focused on the actual infrastructure. The Chinese government and some other governments, like the Russian Federation, are pursuing a broader definition of cybersecurity. They actually use the term information security usually—that includes questions of content and not specifically just the technical aspects. And that's part of the challenge of the international—

Haenle: What else besides content? I mean, sovereignty…issues like that?

Maurer: That as well, and it's also more with a domestic focused agenda than the more international external focused agenda of the cybersecurity discussions.

Haenle: More focused on challenges…perceptions of challenges to their own domestic security?

Maurer: Exactly, yes.

Haenle: So, let's talk about U.S.-China. You're here in China, and obviously the Carnegie–Tsinghua center focuses on China. Over the past few years, the disagreements between the U.S. and China on cyberspace have come to the foreground. [In] 2014, I believe it was, we had the indictment of the five PLA [People's Liberation Army] officers. And then in the leadup recently, in September, to the state visit to the United States by Xi Jinping of course, there were U.S. threats of sanctioning, which they brought Meng Jianzhu [孟建柱] to the United States, and they—the U.S. and China—reached an agreement during the state visit. It has resulted in an agreement that, and I'll read from the language, that neither China nor the U.S. would conduct or knowingly support cyber enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. This is the language that came out of the state visit. I think people were frankly surprised that the U.S. and China were able to come to this agreement, but of course President Obama, during the press conference, said we'll have to wait and see whether actions follow words. There's been high level working groups set up that met in December; and just recently, here on the margins of the S&ED [U.S.-China Strategic and Economic Dialogue] here in Beijing, they announced that progress is being made. But give us a sense, if you could, for where

things stand in this regard. What kind of progress is being made? Have we really seen a reduction in this kind of activity? And how do you think we'll see things going forward?

Maurer: What's interesting about this space is that, in addition to the official statements by governments, we actually have additional information provided by private security companies who have their own threat intelligent units who track different actors. And some of them have —

Haenle: These are like Mandiant, and others like this?

Maurer: Exactly. And some of them have reported that there has been a decrease in activity. I think a week after the statement, one company reported that there had not been any decrease in the activity. I think President Xi might still have been in the air, so I think that was a little early. But that is interesting in that you have an independent source of information, and some of that has suggested that the activity has decreased. Now, is that going to be sustainable? I think that is a big open question. The Chinese government is very large, the bureaucracy is fragmented, there are different interests at play. And the language itself is also open to interpretation. I mean, what is commercial advantage has obviously been a big contention between the two countries. But it is also very clear, and I think this led to the agreement, that the pressure rose and that there is a significant constituency in the U.S. that, after the OPM [Office of Personnel Management] hack, felt—enough is enough, and something needs to change. And a final note on that —

Haenle: So your perception is that the OPM hack really led to the U.S. pushing this issue, to the threat of sanctions? That it was, that that really had a pivotal part?

Maurer: I think it definitely increased the pressure. Even though it was more perceived to be a political espionage case, it was perceived in the broader context —

Haenle: Because of course, General Clapper basically implied that it was fair game.

Maurer: He did. And I think he was envious and said even that had the U.S. had a similar opportunity they would have done the same. But what is interesting about the agreement is that it showcased a will at the highest level of government—that this is something the two states wanted to make progress on, and actually agree on language, rather than have it escalate further. And I think the working groups are essential for that, in actually having this conversation continue and having the processes in place for when there is a new incident—what information should be provided by each side. And I think what's even more important moving forward, [is] that these working groups won't be suspended even if there is a time of heightened tension; unlike back, two, three years ago, when the working group that had been set up got suspended after the indictments, which is understandable from the dynamic. But, I think, given the importance of this topic and how much [this] concerns both sides, I think it is important in the future to make sure these working groups and the process stays in place, because that will help us to deescalate if necessary and to manage that situation.

Haenle: Now coming out of the state visit—I noticed that in the G20 there was language in the statement coming out of it that was similar to the U.S. and China agreement. How did that

develop? And what are the implications for that, given that the G20 is obviously more than just a bilateral agreement?

Maurer: Yeah, that is really interesting; and I think sheds some light on how the broader global discussion about cyber norms is proceeding, because there is a general discussion going on in the international community for what rules of the road should govern cyberspace—and this includes espionage, but also includes how conflict will play out. And you saw the initial bilateral agreement between the U.S. and China, which was followed by a similar agreement between the U.K. and China shortly thereafter. And that then eventually led to the agreement between the heads of states in the context of the G20 and the statement. You saw something similar happen three years prior, where the U.S. and Russia agreed to a bilateral agreement to essentially use the hotline between the two countries and the confidence building measures, and then the U.S.-Russian agreement then led to an agreement in the context of the Organization for Security and Co-operation in Europe. So, a very similar dynamic of first bilateral agreement between two of the major players, which then [leads] into a broader framework. And this has been part of the broader strategy and process for developing and understanding among the international community at large.

Haenle: Thank you for that. So on this global cybersecurity agreements, you mentioned [that] China-U.K. and China-Germany are also publishing similar accords. At the U.N., this group of governmental experts' report, which came out in 2013, proposing norms in international cyber activity, and this was agreed to by 20 governments, including China and the United States, and this build on an agreement in 2013, a landmark agreement report that provided greater detail outlining several norms for cyber diplomacy. So we've had some diplomatic progress. But there are still doubts concerning the extent to which these agreements can be implemented. Can you talk about these doubts? Tell us what the outlook for 2013 looks for in this space and going beyond.

Maurer: Yeah, sure. And I think here, the diplomats—from a diplomatic perspective—the GGE [U.N. Group of Governmental Experts] report has been a great success. If you talk to the international lawyers, they will give you a very different analysis. They will point out that, first of all, it's a group of governmental experts meeting through the first committee of the general assembly—so it's not the first committee of the general assembly that has passed a resolution, it's a report by experts from 20 countries that then submit that report to the first committee—and even the general assembly resolutions are usually considered soft law. So it's not even a general assembly resolution, so it terms of under existing international law, this agreement doesn't really have any standing. And the norms themselves, it says explicitly in the report, are voluntary norms. So from that perspective, they're more of a political statement than anything else. That doesn't mean though that they can't develop a life of their own, because the hope is that, on the one hand, these norms will disseminate across the international community and they'll be taken up by other governments and that they will eventually then become absorbed. But the big question is how do you verify and enforce them? And this is an area where there is a lack of transparency, partly because so much of it is taking place in the covert and classified space. But going back to my initial comment, this is where it's a fascinating security field because you have a lot of private sector companies that are engaged in this as a third party, that are providing more information that wasn't otherwise available.

Haenle: A lot more work to be done in this field. I understand that you'll be coming back to China again given your work with this new cyber program at Carnegie, and we would like to have you come back to the podcast. We appreciate you joining us today and welcome you to the Carnegie Endowment, even though you've been here since October. But thank you very much for doing the podcast with me today.

Maurer: Thank you, Paul. And I look forward to coming back.

Haenle: Thank you.

That's it for this edition of the Carnegie–Tsinghua China in the World podcast. I encourage you to explore our site and see the work of all our scholars at the Carnegie–Tsinghua Center. Thank you for listening, be sure to tune in next time.