The Cyber Sphere—The Hidden Variable of International Relations: In Conversation With Professor Nazli Choucri

Enya Gu

Enya Gu is a Staff Writer at JIPP and the captain of Lincoln-Douglas debate at Nashua High School South in New Hampshire. She has received regional and national awards in several events at the Technology Student Association competitions and was a Bank of America Student Leader in 2021. Enya is also the editor for many comic and novella publishing groups that have garnered over 2 million views. In her spare time, Enya loves to learn about policy issues, international and domestic.

Nazli Choucri is a Professor of Political Science at the Massachusetts Institute of Technology. She focuses on "computational social sciences in the areas of international relations and cyberpolitics—with special attention to sources of conflict and threats to security on the one hand and strategies for sustainability and global accord, on the other." Choucri has authored or edited twelve books and directs the Global System for Sustainable Development (GSSD).

What drew you to your areas of expertise, specifically cyberspace and International Relations?

Cyber didn't exist at all in the 1970s and 1980s. I think what got me into that was computational social science. There was, at that time, a movement towards quantitative international relations, and they were beginning to use computer programs to analyze data. For my PhD thesis, I focused on content analysis of speeches of three leaders from three countries that were not aligned in the Cold War to apply quantitative analysis to their words and their expressions. But the focus was on the individuals as leaders. It gradually became clear to me that international relations, which was what I was interested in, is about countries, not just leaders. And so, from there, with the guidance of my professor and the work of the group at the time, we started focusing on how to distinguish between countries in a way that makes sense.

What were some of your early findings, and what's next?

The basic idea is that there are only three variables that shape what the country can do, what the country is, and whether it can move out and do things internationally or not. The variables are (i) the people, (ii) the resources, and (iii) the technology. But they're not additive variables, they're interactive.

For example, if you look at China now, and compare it to China in the 1950s, not only did the population grow along with everybody else', the technology skyrocketed. If we compare Korea today with Egypt today, Korea, technologically, is very far ahead. In 1950, they were both at the same level.

Next came the issue of distinguishing between countries. But what we really want to know is, what is the propensity of a country to expand outwards? Quantitatively, we could figure this out. But around the 1980s, two things became clear. We were polluting a lot—the environment became important. At the same time (but we didn't notice it), the cyber domain—what we now call cyber, the digital world itself—was also developing.

In particular, the internet did two conflicting, competing things. It was available to everybody (just about) to level the playing field. But there were no "rules of the road." For example, when driving, if you run a red light, you'll get pulled over, but there's nothing like that for the internet. Now, we have words like malware, etc.—which is very exciting, but it's going to be your problem. You guys are gonna have to figure out the rules of the road.

I think that the next really big thing in this question is, what are we going to do about developing rules of the road for the use of AI (artificial intelligence)? It's a technology that can be used by an individual and by a country, for whatever purpose. Think about airplane travel. If the pilot takes off whenever he wants to and whatever route he wants to, you can see the mess it would make. For AI, we're going to have to develop a similar framework of rules. And it's international relations—not just the specific violence/conflict side of it, but we're *all* affected by it. It's in our common interest to have some kind of rules.

Additionally, privacy is a big question: you want to make sure that not everyone has easy access to you. MIT has VPNs and so forth, but it's internal to MIT. I am very conflicted about privacy—in other words, I think it's a good thing, but I don't think it can really exist. But then if it can't exist, is there a fallback position? Your generation will see. What is really kind

of interesting is that my generation, which did not grow up with the Internet, is trying to make rules about all this for the next generation.

In your book *International Relations in the Cyber Age: The Co-Evolution Dilemma*, you say China, the United States, and India have the highest lateral pressures, which are defined as "the propensity of organized entities to expand behavior beyond established boundaries." How can lateral pressures be mitigated by other states?

A key question is, are patterns of lateral pressure in the physical world similar to what they are in the cyber domain? For some countries, like Saudi Arabia, they are physically much higher: in the cyber domain, you can't really see them. But there's a group of countries that are high on all three. I think that what we want to prevent or mitigate is the propensity of expansion in their interaction. Expansion always leads to competition of some sort—my trade is better than your trade, or we have more troops overseas than you do. So trying to anticipate and modulate the possibilities of hostilities is really, really important. But this is something that you can't do overnight; you have to do it sustained over time. And meanwhile, most countries believe that they have to respond immediately to something—they've got to send troops immediately, or we have to do something immediately. And that takes priority.

In your world, there will be more multiple major powers; not 100, but maybe three or four or five big ones, like India, China, and the United States—whatever happens to Russia, maybe something like Brazil. Not equal, but enough to make demands. I think that the structure and restructuring of entities in the world is a far more important issue than liberalism vs. communism vs. etc. And then, what does cyberspace do? Does it help? Or does it hinder? I see that domain simultaneously as a power domain and a capability domain.

So nuclear weapons supposedly serve as deterrence to conventional attacks. Do you believe that the cyber world could do the same in the future?

Actually, I do. It could cause a lot of harm with very little investment. But at the same time, we know that countries or people (and not just countries) are using those tools for financial gain.

In the book [*International Relations in the Cyber Age: The Co-Evolution Dilemma*], there's a comparison between how deterrence works in the old world and how deterrence can work here. And so we're in the middle of the experiment now. Can the United States deter Russia? Can we deter Russia through cyber tools? We also don't know what the United States is doing. The Department of Defense doesn't say, "Well, today we penetrated…" So we don't have a complete real sense of what's going on. The interesting part would be can cyber deter a China or an India? Can cyber attacks lead to a country warring where people might die? I think probably not, but maybe in some instances.

But I do think that there is vulnerability now. Everybody is vulnerable to critical damages in their critical infrastructure. If the water system here erupts—we may be able to do without electricity for a while, but we do need the infrastructure of water to continue. So my answer to your question, can cyber deter? I think yes, but I don't have the data. So maybe the research question should be, how can cyber deter? How could it be done?

I remember that recently, when the India/Pakistan dispute seemed like it was drastically escalating, the Indian government shut down internet access in Kashmir. If there were to be more conflicts in the future, conventional or otherwise, do you think that countries would start targeting infrastructure like technology and the internet?

Absolutely, yes. I don't like it. But yes. Can they sustain it? And who will retaliate? I think we can predict it will happen. What I can't predict is, what's the reaction? Or the reaction from an ally? Even if the reaction is nothing, that gives a signal to somebody.

Do you think countries are prepared for this?

No, not even the United States. Maybe China's a big exception. Because—and that's not taking into account theories of international relations—in general, the leadership, and maybe the society, has a long term view of things. So I wouldn't be surprised at all if they were preparing. The West is generally a market much more oriented towards the immediate short term. Even though we have five year development plans, we don't have a strategic view of the globe, such as where we want to be at 20 years from now. China tends to be the only country I know that tends to be consistently thinking beyond the short run.

What are the most important steps for America to be taking in regards to the cyber sphere? What should the United States be focusing on?

Well, I think the United States should be thinking about a global accord on the conduct of behavior in the cyber domain. Some countries have their own cyber laws, but I don't know of any international law.

I think the United States should take the high road and say the time has come: we should all convene and think about how to frame a general approach. We will have companies represented, but it's a matter of sovereignty, and it is a matter of security for individuals and for the globe—and I can write the speech for this. It's not going to cost the US anything except for maybe some time of its representatives. There are lots of pockets in the UN and elsewhere that are beginning to talk about this, but no country has taken the initiative and said it. There are some efforts, like the International Telecommunications Union, but I think we should be moving towards an accord and then hopefully international law comes out of it.