Intersect, Vol 16, No 3 (2023)

Interview with Professor Amy Zegart

Morgan Cortina
Stanford University

Amy Zegart is a professor of Political Science at Stanford University. She is also a Senior Fellow at the Freeman Spogli Institute for International Studies as well as a Morris Arnold and Nona Jean Cox Senior Fellow at the Hoover Institution. Professor Zegart researches U.S. intelligence, cybersecurity, emerging technologies and national security, and global political risk management, focusing on demystifying common misconceptions surrounding the intelligence community and analyzing the ways in which intelligence institutions operate. Through her Spies, Lies, and Algorithms class at Stanford University as well as her various publications in The Atlantic, Professor Zegart is a revered author, professor, and researcher.

Her publications include Spies, Lies, and Algorithms, Political Risk: How Businesses and Organizations Can Anticipate Global Insecurity, and Spying Blind. She has worked with a variety of authors such as Condoleezza Rice and Herb Lin.

Professor Zegart attended Harvard University for her undergraduate education and obtained her Master's degree and Ph.D in Political Science at Stanford University.

MC: Can you tell me a little bit about your background and expertise in the field of national security and intelligence?

AZ: So, I've been looking at intelligence issues now for almost thirty years. It started with my doctoral dissertation where I looked at the creation of three organizations: The Joint Chiefs of Staff, The National Security Council, and a little agency called The Central Intelligence Agency. And that organization fascinated me back when I was a grad student, and I've been hooked on intelligence ever since.

MC: I've had the pleasure of taking your Spies, Lies, and Algorithms class this quarter, and I feel like we've learned so much about both the benefits and shortcomings of national intelligence institutions. I'm curious to hear about what you think are the biggest challenges national agencies face today and how they could possibly be addressed.

AZ: Well, first let me just say it warms my heart that you said you've learned about the benefits and the challenges, because one of the goals of this class is to provide a realistic and thoughtful perspective about agencies that most people don't know anything about. There's a lot of myth and misperception about American intelligence agencies, in particular, so that's a really important goal of mine: to demystify but also to have a balanced perspective.

In terms of the biggest challenges, I think the fundamental challenge of intelligence agencies is their inability to adapt fast enough to the threat environment. This is a theme, as you know, that has run throughout the class. Intelligence agencies are charged with preventing strategic surprise. They have to be able to see over the horizon to keep the United States out of wars, out of conflicts, to anticipate dangers before they arrive at our shores or affect American interests. That's a really hard job, and it's getting harder because of this convergence of emerging technologies. Adaptation is always hard, but it's even harder today because the basics of intelligence are fundamentally challenged. Who's a customer? People without security clearances are customers. Who can collect and analyze intelligence? People outside of the government now can collect and analyze intelligence. What's the threat landscape? It's more complicated than it has ever been. So a hard job is now even harder thanks to emerging technology.

MC: With the changing cyberspace landscape and the consistent cyber threat North Korea specifically poses to the United States, do you think that institutions will be able to address this?

AZ: That is a really hard and complicated question. It depends on which institutions. I've been following and studying cyber for a while now because it's really intelligence-adjacent, and from the government perspective, we've seen a big shift. There has, in the past, been a lot of talk about cyber deterrence: 'We have to stop the bad guys from getting into our systems to begin with.' Cyber deterrence doesn't work, or it doesn't work very often. So now what we're hearing is a shift in thinking from The White House, and I think it's a good shift in thinking: to cyber defense and cyber resilience. The question isn't 'is my company or organization going to get attacked?' You are. The question is 'can we recover from an attack?' Is an attack crippling or is an attack something where we're resilient enough that we can continue our operations?

And so, that shift in mindset is changing how the government is interacting with the private sector, and it's also changing how private sector organizations are thinking about their own cyber security. Ultimately, the government can only do so much. We're on our own in cyberspace, and so we have to figure out ways, systematic ways, that critical infrastructures like power, water, and other things that keep the country going can operate, even if North Korea launches a cyber attack.

MC: What do you think about the state of the communication between the public and private sectors? I know that there have been a couple of initiatives like DreamPort or the zero-trust mentality, but I wasn't clear on if it was working or not. And if they aren't adequate enough, what are the steps necessary to resolve this?

AZ: I think that what we often see with the government is asking the question, 'Is it working?' The answer is almost always: progress is being made, but we still have a long way to go.

MC: As politicians would say!

AZ: That is definitely true in cyber, as I'm sure you really appreciate from having read so much about cyber. So, yes, there is this DreamPort and there are new capabilities for the National Security Agency (NSA) and the

Department of Homeland Security (DHS) to better talk with the private sector.

To me, one of the most interesting and important developments, which General Nakasone (the head of Cyber Command and the NSA) talked about when he came to class, was that cyber used to be a one-way street. The government would come and say 'tell us all of what's happening with you in cyber' to a company, and would give nothing back. Now, there's a two-way sharing of information between people in the government that know a lot about what's going on in cyberspace and potential victims of cyber attacks. It's that two-way sharing that's going to be crucial for securing cyberspace better.

MC: That's a great point. I remember reading about how there's an increasing number of cyber attacks these days and they're incredibly difficult to stop.

AZ: Right, and no one's going to stop North Korea from attacking us in the cyber sphere.

MC: Absolutely. Shifting gears a bit, we've talked a lot about shortcomings in intelligence and I know that there's a lot of work to be done within these institutions. But I would love to ask, in your research and experience, have you come across any noteworthy examples of successful intelligence reforms or organizational changes that have enhanced the national security capabilities and overcome these shortcomings?

AZ: The short answer is yes. One example is after 9/11, there was the creation of an organization called the National Counterterrorism Center, or NCTC. The main challenge there was, 'how do we coordinate information-sharing better and faster so that we can pursue active terrorists before they strike on American soil?' And NCTC was the answer to that. It brings people from across the different intelligence agencies and they work collaboratively together. They've gotten better computer systems as well, and so NCTC is seen as a shining example of success.

A second success story, still being written, is CISA, the Cyber Security Agency in the Department of Homeland Security. This is an organization that was just created a few years ago, about protecting presidential elections from foreign interference and vote tampering. That organization's gotten a lot more robust. Its leader, the director, Jennifer

Easterly, is a really charismatic leader. She's gone a long way towards making cyber cool, which is a big part in attracting talent. For example, a lot of Stanford students have worked for her. So I think that the organization has come a long way. One of the things which we've talked about in class is that there's a natural and understandable distrust in the U.S. government when it comes to things like data protection and cyber security. There have been some dark chapters in American history. As a consequence, many people are uncomfortable if the NSA comes knocking on their door saying, 'We're here to help.' But CISA and the Department of Homeland Security don't have that baggage. So when Jen Easterly says, 'Hey, I'm from the government. I'm here to help you in cyberspace,' people are naturally more trusting and willing to work with her. And I think that's really important.

MC: That was actually a perfect lead-in to my next question, which was how can the intelligence community effectively balance the need for privacy and civil liberties while dealing with the imperative to protect national security in this increasingly interconnected, technology-based world?

AZ: There's always an enormous and important tension between achieving security and protecting privacy and civil liberties. That is the natural tension when secret agencies are operating inside democracies. Where to draw the line between the security part and the privacy and civil liberties part is a constant challenge. It's getting harder because so much information is flowing on the internet anyway, so how is it that Google knows more about me than my own government? And how is it that China can learn much more based on data that they can access about American citizens than our own government to keep us safe?

On the other hand, we don't want the government to have access to everything. There are good reasons as to why we have these protections in place. Figuring out how to draw the line and strike the right balance is crucial. Congress plays a crucial role in this process because nobody really sits at the center of getting classified information on the one hand and interacting with the American people in an open way on the other hand. No one is in a better position to do that than people elected to Congress. When we talk about oversight, I think that's a crucial function. But I think that Congress hasn't done a very good job, for the most part, of fulfilling that role.

MC: Do you think that there's a risk of privacy and data being overlooked by politicians due to more heavily publicized issues in politics, especially due to the extreme polarization in government?

AZ: I think polarization is always a challenge. Politics should stop at the water's edge, but it often doesn't. So we see this infecting how people view U.S. intelligence agencies, for example. But I think there's something else going on here. The European Union has a data privacy protection law that's very robust. Now, big tech companies don't like it, but they have to follow it. There is no data privacy law in the United States. So let's start there. The privacy of our data needs to be protected from a whole host of actors, including actors that want to monetize our data, and we don't know how they're using it. They can sell it to third-parties without our knowledge or consent because you sign that user agreement form and who has time to read all of those? So let's start with the fact that we haven't been able to pass a basic data privacy/protection law in the United States that would then set guard rails for what companies can and cannot do. So I think that's a crucial need. One of the reasons we haven't been able to do it is with our classic American political system, there are opponents to that, and those opponents are big tech companies that have huge financial incentives to fight legislation like that.

MC: Absolutely. Looking ahead, what trends or developments do you see in the field of national security and intelligence and, if there are any, how should policymakers or intelligence experts prepare for them?

AZ: I think emerging technologies are going to be increasingly crucial for intelligence agencies, both to understand and to use. What that means is that they're going to have to think about talent differently. They're already starting to. But there's a need to get talent in the door that is technologically literate and there's a need to get talent in and out of the door, going in and out of government and the private sector. The locus of innovation has moved from the U.S. government to the private sector. Many of the things that we take for granted that are amazing scientific innovations—GPS, cellphones, the Internet—were invented by the government. Crucial technologies—micro-processors, the Arpanent (precursor to the Internet), GPS satellites—exist because of government funding and government innovation. But now that script has flipped, and the big innovations of society today are not invented by the government, they're invented in the private sector. This means that you have to be able to adopt technologies inside the government and you need people who are literate in both government and private sector worlds. That workforce needs to be more fluid and move in and out. In your generation, I can't imagine most of your classmates thinking, 'I would love to work in the government for the next thirty years of my life.'

MC: I can't say that I've heard anyone say that in my time at Stanford.

AZ: But you might be interested in working in the government for a couple of years, and then going to Google or a startup, and going back and forth. That's the model that the intelligence community has to adopt, and that's a very hard change because it's never had to do that before.

MC: Do you think that the shift from the government to the private sector in terms of technological inventions is causing a rift between the two? Is it getting harder for the two to communicate and for the government to regulate such technologies?

AZ: I think, in many ways, it can't be regulated in the same way. AI is born "open," it wasn't born classified. Nuclear secrets were born classified. The government could control the spread of how to make a nuclear bomb from the very beginning of that technology. We don't live in that world anymore. Synthetic biology or artificial intelligence, these are all technologies that are widely available and widely distributed. If the government thinks that it can solve technological problems by restricting technologies alone, that approach is doomed to fail. And so there has to be a different way of collaborating and understanding what's going on. Not just in the private sector, but in universities as well.

MC: I mean, computer science is so big here at Stanford, so I think that speaks to your point of starting technological literacy early on. On the topic of AI such as ChatGPT, how do you assess the role of these kinds of technologies in shifting the narrative of cyberspace? Do you see it changing for the better or for the worse?

AZ: I'd like to be optimistic, but I am naturally a 'dark corner of the room' kind of person. I gravitate towards thinking about the risks and downsides of technologies while understanding that there are tremendous upsides to technologies too. So with ChatGPT in particular and generative AI, I think the near-term likelihood is that deception is going to get even worse. One of the big changes over the long arc of history is that deception has gone from being a tool that elites used to trick elites in the deception of warfare—'I want to convince you that my army is moving South when in fact it's moving North'—to tricking masses with the Internet and AI in particular. Russian trolls can pose as Americans on Facebook and deceive millions of Americans. And what does ChatGPT do? It makes that even more possible to do, more believable to do, at scale. I'm really worried about manipulation of narratives, polarization of societies, generated either domestically or by foreign actors with the click of a mouse. Or utilizing ChatGPT to make things sound much more realistic than they have been in the past. So the near-term risk of deception influencing geopolitics is very high.

Long-term, it's hard to know. I'm sure you've played around with ChatGPT, and it has a lot of problematic qualities. My concern is that these models are in the wild before the creators have any systematic idea of the risks of these technologies and how they can go wrong. They're confidently wrong and deceptively wrong. I'll give you an example, one that I mentioned in class. I asked ChatGPT to name five things that I had written. It returned five things, only two of which I had actually written. Three of them, however, were so believable with titles and arguments and sources, that I wasn't sure whether I had written them and had forgotten whether I had written them! It was wrong, but it was deceptively wrong. I'm really worried about that too.

MC: That has definitely happened to me before, where I think something looks right but with a second glance, it is completely wrong.

AZ: And you don't have a sense of what confidence to have in that assessment. Even the citations can be completely made up. So I am concerned that this new technology has gotten out of the gate before people really understand its limits. I'm sure that's often the case. But given the temptation to use it as a substitute for human judgment, I am concerned about the future of ChatGPT.

MC: To your mention of deception, do you think that we should increase international cooperation and information sharing among intelligence agencies across the globe and how do you think we can achieve that? I know that there's a certain amount of distrust as well that could pose a challenge.

AZ: Well, I think that we need to think about data as a vital resource and increase the sharing of trusted data flows across countries more than we have in the past. Note that I said trusted data flows, not among democracies. So we need a broader coalition than just democracies, and there are like-minded countries that believe in rule of law and cyber security and protecting data, making sure that your data is authentic, has integrity, and is available to the people who need it. Because that is such a powerful force for trade, economic growth, and national security, we need a broad coalition of the willing to think about, 'How do we have digital free trading agreements involving data?' This is something that I know the new state ambassador for cybersecurity, Nate Fick, is really interested in. So not just intelligence sharing, though we need to do more with that too, and we've seen a lot more intelligence sharing because of the war in Ukraine. We need more intelligence sharing with other countries. We need more intelligence sharing with the public, so declassifying intelligence as a way to galvanize support. And we need more collaboration when it comes to data and algorithms among like-minded countries.

MC: Yeah, I was reading a little bit about that in terms of North Korea's cyberspace capabilities. In some cases, if we had just connected with other countries, we would have been able to link cyber attacks and better predict them. For my last question, I wanted to take note of your various publications such as Spies, Lies, and Algorithms as well as Bytes, Bombs, and Spies, both of which we've had to read for class. They've significantly deepened my understanding of the intelligence landscape, and I really look forward to exploring more of your works. So I'm curious if you have any upcoming publications or areas of research you plan on exploring in the future.

AZ: I'm noodling at the very beginning of another book. I'm in my 'let's let it marinate over the summer' days. I'm really interested in the changing sources of power. If we think about it, for most of history, the sources of national power were tangible objects like land. What territory did you hold? How fertile was the farmland? What waterways did you control? What military assets did you have? So they were tangible assets controlled by governments. But increasingly, the sources of national power are intangible assets such as data and technology that are not controlled by governments. I'm really interested in exploring this question about where power comes from and what happens when the distribution of power changes within a country, not just between countries. I don't know what the puzzle is yet that I want to examine or how I want to approach it, but I'm going to dig more deeply into history. What can we learn from ancient times? What can we learn from the period where the Dutch, for example, were settling in New York and it was really led by a corporation and not a government? How did that work? Are there lessons that we can learn from history that are applicable today? That's my summer project.

MC: That sounds like an amazing summer project. I will be on the lookout for the book when it comes out. Thank you so much for taking the time to speak with me today—I have truly appreciated your insights and thoughtful responses!