Peter:

Hello, and welcome to Policy 360. I'm your host this time, Peter Feaver. I'm a professor of political science and public policy. And I also run the Duke program in American Grand Strategy. My guest today is Jared Cohen. Jared is the founder and CEO of Jigsaw, the tech incubator created by Alphabet, the parent company of Google. He is also the chief advisor to Alphabet's executive chairman, Eric Schmidt. Previously, Jared served as a member of the Secretary of State's policy planning staff, and thus as a close advisor to both Condoleezza Rice and Hillary Clinton.

I should also say he's an old friend, and one of the more far seeing futurists that I know. Jared has a long standing interest in international security issues, including counter-terrorism, conflict resolution, and the politics of the Middle East. He's traveled to more than a hundred countries, including Iran and North Korea. And has conducted interviews with members of various extremist groups, including Hezbollah, Al-Qaida, the Taliban, Al Shabaab, Somali pirates, and more recently, failed ISIS recruits. A fascinating resume and an even more fascinating individual. Welcome to Policy 360, Jared.

Jared:

Thank you, Peter.

Peter:

So let's just dive right in. You've said that the world "is in a perpetual state of cyber warfare". What did you mean by that?

Jared:

We're at a point now where the advent of technology has happened. The access revolution is constantly evolving, but the ubiquity of technology is upon us. And what that means is many states and entities have harnessed the power of cyber capabilities to perpetuate some of their nefarious objectives. The result of that is some of the obvious, invisible cyber warfare that we see. But every time you get one of those phishing attacks in your inbox, every time you find malware on your computer, when you worry about bringing your laptop or your phone to a particular country, that's because if you're online, you're essentially living in this digital war zone. And if you're living in an actual war zone, think about the precautions that you would take, helmets, flak, jacket, paying attention to what's around you. We now find that we're in the same situation online, and we have to take care of ourselves. We have to be vigilant. We have to make sure that we're protected.

Peter:

This sounds like a problem for states, created by companies. Is this something that the companies can help us solve?

Jared:

I would say it's a shared responsibility. So the companies have transformed the topography of the world in the sense that they've made the world even more digital than it is physical. In the sense that all of us have many more versions of ourselves online than the one version of ourselves that's walking around offline. And so the digital world is in fact much bigger than the physical world. But all of the same sort of human interactions and human precautions, the good, the bad, and the ugly, it all exists there as well. And so I think what we need to do is not look at the online world as some sort of separate place. But we need to look at it as an extension of all the things that we do in the physical realm.

Peter:

Well, let me begin with a question about something you did in the physical realm, where you traveled around the Middle East. This is when you were very young, just out of college. And you traveled in many of these countries and got an insight into the mindset of the next generation. And you came back and told the U.S. Government that we were missing some big things. Just tell us what you saw then, and how that led to some of the things you're doing today.

Jared:

Yeah, well, you've known me for a long time, Peter. As you know, I was an obnoxious 22 year old who had this sort of naivete. It was a combination of naivete to traveled to these places, and sort of typical 22 year old hubris to think that I had something to say as a result of having been there. But Woody Allen has a great quote where he said "80% of life is showing up". That's essentially what I've tried to do in my life. Which is I'm blessed with curiosity in the sense that I'm a very curious person, and I allow myself to take risks to pursue those curiosities. And more often than not, that's involved looking at a map, looking at a set of issues, being curious enough to find a way to get there, and kind of going without a plan and just talking to people.

And I find oftentimes in traveling, especially as a young person, the less structure, the less of a plan, the less organized it was, the more interesting. Because I always ended up going with one set of hypotheses and research objectives, and leaving having studied something completely different. So when I went to Iran in 2004, I went to interview opposition groups and reformers. And it turns out as an American at that time, traveling in Iran, that research project gets blown up pretty quickly. And so I ended up just spending time with young people. After leaving the country, realized that I'd gone to the country to study the wrong opposition. Right? That in this country, that at the time had 70 million people, the real opposition was the 67% of the country that was under the age of 30.

And what was fascinating, and we take for granted the trends around technology. Back then, nobody was talking about Arab Springs and tech oriented revolutions. And these young people were just using technology to organize, to do things they weren't allowed to do. Mostly social and recreational. And I left Iran feeling one day, this is going to matter in some political moment. One day, politically, something is going to happen. And they're going to realize that they know how to do a bunch of things that the adult leadership isn't necessarily aware of.

And so, I sort of left my time in Iran and Syria and elsewhere, and you were at the White House at the time. And you remember, I had come back to Washington, and Dr. Rice was my mentor. And so she was always gracious enough to see me. But you were also gracious enough to see me. And the lesson that I learned there was twofold. If you're curious and you go explore something that most people haven't had a chance to see, it turns out that there's a lot of people who are curious about the findings. Two, it's amazing what you can get and who you can meet with if you just ask.

Peter:

Well, this led you to an interest in the intersection of digital technology and foreign policy. And you played a key role in advancing the State Department's engagement in that area. But then you left the State Department and helped stand up a new effort at Google, to develop new tools that would be at the interface of politics and technology. So talk a little bit about the mission of your current company, Jigsaw. And maybe one or two of the new products that, that your research has helped create.

Jared:

Yes. So Jigsaw is an entity within the Alphabet structure, which is Google's parent company. And our mission is very simple. Which is we're trying to build technologies that address some of the toughest security challenges around the world. And as technology becomes ubiquitous, all of the toughest challenges of the physical world are increasingly spilling over online. Which is making the complexity of these challenges far greater. We went from looking at security threats that were largely sort of deployed by criminals and hackers to security threats that are now deployed by many more state actors at scale. On the one hand, that's horrifying. On the other hand, from a technical perspective, these are real engineering problems that our engineers are excited to work on.

We have a philosophy that every product we build starts with an insight from a user somewhere in the world who lives in one of these geopolitical hotspots. And if the technology associated with trying to address their problem is interesting enough, we will build it. And our fundamental philosophy is, we believe that we can help address some of these tough international security issues and do well by the business at the same time. That can be... Yes, of course, that can be making money. But more often than not, it's about advancing the technology. And if our starting point is helping these users, these sort of users in distress, and we can advance the technology at the same time, all the better.

So examples of what we've built. We've built a sophisticated DDoS protection service. A DDoS attack is when a website is overloaded with nefarious traffic, to such an extent that it essentially knocks the site offline. We've built a DDoS protection service that we offer for free to any website in the world serving human rights content, election monitoring content, or independent media content.

We just built a technology called Perspective to address what is probably the most universally understood problem on the internet. Which is the decline of civility perpetuated by the trolling problem. Trolls are obnoxious people online, who are obnoxious at scale. And what the product does is it uses machine learning to facilitate better conversations online. So we have a massive data set that we use as training data.

And then we've built a toxicity model where we can, any publisher or platform can run their comments, or their discussions, through this technology. And they receive a score zero to 100 of how toxic that language is. And then they, as the publisher or platform, determine what to do with that score. So in some cases, they allow the user themselves to turn the volume up or down, depending on what they have an appetite for that day. In some cases, they use it as a way to facilitate better moderation tools. And some are experimenting with using it as a sort of author tool where they're sort of betting on the fact that many people who write obnoxious things, maybe you don't realize how obnoxious they are. And it's like a hint and assist model, where you can spell check your toxicity.

Peter:

That's great. So if I'm writing something, and this thing is operating in the background, it can say, whoa, you are scoring, what? A 60 on the toxicity scale. Is that what you intend? And if I intend, I still press send. But if I thought I was being nice, then this allows me to fix it. Is that-

Jared:

That is precisely right.

Peter:

And on the other side, if I'm feeling tough that day, I can open the [inaudible 00:10:09] and say, throw every negative comment at me. But if I'm feeling fragile, then-

Jared:

Precisely.

Peter:

Of course, the danger here is that what you consider toxic might be my political views, or vice-a-versa. So how does it protect against that kind of bias?

Jared:

So we at Google are not, or Alphabet, are not determining what's toxic and what's not. The annotations come from a combination of preexisting data sets from a place like the New York Times and elsewhere. And then, a collection of aggregated data sets from other sources that we then crowdsource with accredited annotators to ask the question, which of these comments are toxic? And the way we get around machine learning bias, and you should never declare victory on machine learning bias. We're constantly iterating on it and working on it. But we have a ratio of 10 annotators for each comment. And the annotators are, as you can imagine, geographically, socioeconomically, gender-wise, et cetera, as diverse as possible.

And the way we define toxicity in this case is, this comment is likely to cause somebody to leave the conversation. The reason we started with a toxicity model, so a toxicity measurement tool, is there was actually greater inter annotator agreement on what constituted a toxic comment than what constituted a personal attack, something obscene, something off topic, something unsubstantial, something that was harassment, something that was hate. Which was actually a little bit surprising to me. But it turns out that people are able to recognize the type of comment that would cause somebody to leave the conversation.

Peter:

Interesting. Well, when you do develop the technology that tracks stupid comments, I will, I'll certainly buy that one. Of course, the news these days is all about the way the Russians appear to have interfered with the 2016 campaign, taking advantage of their own digital tools to do so. And that raises serious questions about the integrity of our electoral process. And is there something that Google Alphabet can do in that space that would promote the people's confidence in elections?

Jared:

Yeah, and I would say, there's a lot of focus on the Russians. But tactics are tactics. And they're kind of state agnostic. And once they're out there, any state can use them. So it ends up, in some respects, being metadata. Which state was responsible for it. We have developed an understanding of what types of tactics a state can use if they want to "hack an election". Now, the problem is, when we say hack an election, it means different things, depending on who's talking, right? So, some people are talking about hacking of the machines. Which is why the Dutch with their election said they went to all paper balloting. I don't believe a state, if they wanted to hack an election, would try to do anything significant on the machines.

I think that they might do a little bit on the machines to try to create a little bit of chaos, and maybe foster a Florida type, a Florida 2000, type moment. But it's hard for me, the attribution is too easily discovered in that case. And I also don't think... There's a lot being made of fake news. You know, fake news to me, is a catchy term to describe what is one slice of the problem. And you're talking about manufactured information that is deployed for somebody sort of receiving it on the other side, to essentially believe a falsity. And I don't think that works as effectively as people think it is. And it's very glossy.

And if I were one of these countries that was trying to hack an election, I would be thrilled that everybody's talking about fake news. Because it means that they're not talking about the tactic that one would use if they did want to hack an election. Which is, essentially launching a digital insurgency. Which is the commandeering of actual identities, and then building accounts around them, and supplementing that with manufactured identities and automated identities that all create the appearance of being scattered throughout the world, representing different interest groups that then all follow each other.

So they then all look influential, defined by how society describes influence, which is how many followers you have. And then a state would have an army of trolls representing these different interest groups, all of which look influential, and all of which look like they belong in the conversation. And they would deploy them against various topics that were trending to try to hack the conversation.

Peter:

And is there anything that Alphabet can do in that space?

Jared:

I mean, I think the problem needs to be better understood. It's clear that there are state sponsored efforts to hack the discourse, and hack the conversation. And I find myself asking like, what's the lever of change here? I think the lever of change is detection, right? Which is, how do you, when you're participating in a conversation, are there signals that can be pointed to? Are there signals that can emerge, that indicates that this isn't so and so from Arkansas. This is so-and-so sitting in Beijing. Who might look like this person in Arkansas, who's a Trump supporter, or a Bernie Sanders supporter. But in fact, it's not.

So if we can understand the signals, we can potentially explore detection tools. We are so far from that. Because I think that understanding the problem is the first part. And then this is happening across lots of different platforms. So a solution really requires an industry-wide approach to this, right? You have many, many digital platforms where the conversation is playing out. And unless you do something comprehensively across all of these, it will be a very difficult problem to address.

Peter:

Well, addressing difficult problems is what I've seen you be doing for the last 15 years. And so I'm confident that you'll be working on this. And if anyone can advance the ball, I think you and your team will be them. So thank you very much for joining us, and joining me here on Policy 360. Our guest today has been Jared Cohen. Jared is the founder and president and CEO of Jigsaw, the tech incubator created by Google. Jigsaw is a subsidiary of Google's parent company, Alphabet. Jared coauthored his latest book, 'The New Digital Age: Reshaping the Future of People', with Google executive chairman, Eric Schmidt. And it was a New York Times bestseller. Well done. Jared is on the Duke campus today as a guest of the Duke University program in American Grand Strategy, the political science department, and the Sanford school of public policy. Until next time, I'm Peter Feaver