Cyber Threats and Cyber Policies

Interview with Dr. Peter W. Singer
New America Foundation

What are your main concerns regarding cybersecurity currently?

There's so much happening from new technology and new dilemmas, but unfortunately, there's something I just can't get past, which is that we just had the most important cyberattack in history, and a large part of our political system just wants to whistle by and forget it. We had Russian cyberattacks on a wide variety of American political organizations, individuals of both parties; as well as non-governmental groups, from think tanks to universities, to governmental sites like the Pentagon email system. This was not a one-off event. They were identified by five different cyber security companies as Russian in origin and also officially identified by the U.S. government as such. Also, belatedly and begrudgingly, the attacks were admitted by the current U.S. President to have been Russian in origin.

Yet not much has happened in reaction to this, other than the stop gap sanctions put into place by the Obama Administration, which are at risk of being lifted by the Trump Administration. This is big. It's not just a campaign that's hit the U.S., it has also hit multiple allies of ours, and it's ongoing. So again, there are lots of other things that we can talk about in this space, but it's hard to ignore that many people want us to ignore this cyberattack.

After the attacks, Senator McCain said, "the American response was totally paralyzed." What should be done to better thwart and respond to these kinds of attacks?

It is interesting that a number of congressional leaders, not just Senator McCain, but both the Speaker of the House and the Senate Majority Leader attacked the Obama Administration responses as too little, too late. They were quick to make that criticism, and, quite frankly, they were right. But a test of their sincerity is whether they will back these words with actions by turning these sanctions into law and strengthening them further. The important part of turning them into law is that it makes it harder for Trump to set them aside, as both he and his aides have made clear they'd like to do. Strengthening sanctions could aid restoring and bolstering deterrents in this space. If Congress actually acts, it would show Putin that the party of Reagan and Eisenhower is willing to stand up to Moscow rather than shower it with praise.

So, what else can we do? It's not about punishment. It's about seeking to find pressure

> *..we just had the most important cyberattack in history, and a large part of our political system just wants to whistle by and forget it.*

points to influence future action. The overall weakness of the Russian economy as well as its oligarchic structure, are choice leverage points. It is notable that the U.S. is being bullied about by the world's thirteenth largest economy and falling. Russia's economy is the equivalent of Spain. Targeting financial assets of Putin and his allies, particularly those held outside the country in real estate and tax shelters, would be something I would expand. Outing these assets should also be the target of activities beyond sanctions. One of the things that authoritarian regimes fear is what they try to ban discussion of. The Russian regime's anger at the publication of the Panama Papers, which show just a very small portion of where its money was hidden around the world, reveals an area that could be exploited further.

The same twin goal of outing and defanging networks should also be applied to the financial and digital infrastructures that have been used to conduct these attacks. By outing them, you make them harder to operate in the future. But there's an important caveat here. It's not just about hitting back. You also can and should build up resilience, the ability to shrug off future attacks. This is known in deterrence theory as "deterrence by denial", that by making attacks less beneficial to the attacker, they are made less likely. What's important about building up our own resilience is that this would be of benefit not just against Russia, but any attacker, whether it's other high-end threats, like China, to low level threats such as cyber-criminals.

There are also all sorts of things that we could be doing better in building our resilience and almost all of them are non- or bipartisan. An example was, after the OPM breach, the Obama Administration identified a series of best practices from business that could be brought into government to aid cyber security. Best practices from business? That feels like a nice Republican talking point. Congress should be making sure that these things are actually being implemented. Another example would be, towards the end of the Obama Administration, there was a bipartisan commission of experts that sent out a series of action items. Again, bipartisan. Now, put those into place. Some people will say they want one or the other of these things. No, you do both. There's a lot more that we could do here. But, for the most part, significant parts of our political bodies are whistling past it.

A few years ago, China was perceived as the largest cyber threat to the U.S. Has that abated?

It depends on how you define largest. What gained such interest was a massive and in-your-face campaign of intellectual property theft that was targeting everything from government research institutions to private businesses. It occurred from the area of defense to soft drink companies, furniture companies, you name it. This was raised at the highest levels with China right before the bilateral meeting a year ago, and it was made clear that if it continued at that level, it would sink the upcoming leaders' meeting and sour American-China relations. Reportedly, the scale of that campaign, the in-your-face nature of it, has gone down. There are some other things going on within China, from reorganization of how its military and government conduct these operations to anti-corruption campaigns, that have been tied to that decline as well. So, the bottom line, by most accounts, is that it's gone down, but not disappeared.

However, this is a tool, a leverage point in China's back pocket that it could bring them back if it sees relations sour. As an example, President Trump placed a pretty inflammatory phone call and series of tweets related to Taiwan right after he won the election, whereby Beijing sent signals of its displeasure by doing things such as kidnapping an American robotic submarine in the South China Sea and sending bomber flights around Taiwan. There's a similar response in their back pocket, which is to ramp back up the level of cyberattacks.

Let's switch to cyberterrorism, a topic many people are concerned about. For example, potential threats to infrastructure. Do you think those general fears are perhaps overblown?

Yes and no. The narrative of cyberterrorism is something that has had an outsized influence compared to the actuality of it. And let's be clear here. There have been over 50,000 mentions of "cyberterrorism" in some way, shape or form. But, there have been zero actual incidents of it, according to the FBI definition of cyberterrorism. Cyber terrorism is not terrorists using the Internet; it is actually using it to cause physical damage, death and destruction. If spreading propaganda was terrorism, a terrorist sending a letter would be "postal terrorism." But no, it's the terrorist sending the letter bomb that makes it postal terrorism. Right? Same thing here. So we've not actually seen any incidents of actual cyberterrorism yet despite all the stories.

This doesn't mean it is not a risk. It doesn't mean that it won't happen. It will. It will happen because of the clear interest in it and the lowering of barriers to entry, particularly as we move more and more to the Internet of Things, as we expand from using smartphones and laptops to also using smart cars, smart power grids, and smart medical devices. It's not just that the landscape of potential targets grows from roughly the 7 billion things that are linked up to the Internet right now, to the 50 billion things that are going to be online in a couple of years. It is also that, when you attack and gain access to "things," like a car, like a power grid, like a refrigerator, you can cause physical change in the world. Therefore, different kinds of risk are created than if someone stole your email. If you can pump the brakes of a car remotely, it's a lot different impact than being able to steal the financial information of who bought the car. The point is, there is a very real risk here. But again, too much of the discourse has been stuck on "cyber 9/11" and "cyber Pearl Harbor" bumper stickers that haven't been all that helpful.

On a lower scale, do you think that not enough attention is being paid to simpler cyber security risks that are potentially encountered with everyday activities, things like phishing, shoulder surfing, human factor risks?

Clearly we would be in a much better space if we just had a minimal level of cyber hygiene. By saying "we", I mean everything from individuals to national security at-large. The breach at the DNC is a great illustration of this, the "what if" that could have taken us in a very different history. But what I find fascinating is that we still don't teach these cyber security basics the way we should. And this applies again everywhere. For example, business executives regularly make cyber security decisions, everything from their own individual cyber hygiene to making decisions for their company on how it's going to invest in their space. Yet, MBA programs don't teach it the way they teach courses in ops, org behavior, finance and the like. Where if you're in an MBA program, even if you're not going to go into ops, or if you're not going to go into accounting, you still get the basics. We don't get the same coverage for cyber security, even though it will be a manager's responsibility.

This is important all the way down to our kids, given the massive amount of time they spend online. But, for the most part, we don't teach them how to protect and secure themselves online.

I like that notion of hygiene as a parallel. It's something that everything from parents to schools teach, because it's both protective of those that you love, but it's also protective of society at-large.

How do you see cyberwar capabilities affecting future conflicts?

It's not just the future; it's the reality of present day conflict. Just look at Russia versus Ukraine or ongoing events in Syria and Iraq. There is now a conflict that's played out not just on land or in the air, but also in cyberspace. What's interesting about it is, as the Russia/Ukraine episode reveals, is that the most consequential cyber parts of the conflict can happen before the real physical conflict begins. To put a little more flesh on that, Russia owned, both literally and virtually, Ukraine's communication networks before the first troops crossed the border. Because Russia did, it was able to have an almost paralyzing effect on the Ukraine in the first couple of days of the conflict. It was able to control and restrict the flow of information.

What we've seen in the Syrian and Iraq Wars is everything from online recruiting and propaganda to using cyber means to gain intelligence for use in physical targeting – "Where is someone actually located in the world, so I can drop a JDAM (Joint Direct Action Munition)." Cyber has become a front in much the same way battles in the air did a hundred years back. That will be the case moving forward, whether the adversary is a military actor or a state actor.

What about criminal activity through avenues such as TOR, the darknet?

There's a very active and vibrant ecosystem that supports criminal activity. Some of it is happening in dark markets and some of it happens quite out in the open. There are two projects here [at New America Foundation] that are interesting. One looks at how these criminal marketplaces operate in the dark web. What we found is fascinating but also a bit unsurprising; like in regular crime, they often center around language. For example, Russians tend to work with other Russians, Indonesians with other Indonesians and the like. There's a global marketplace but it actually breaks down into little subsets. Like other markets, there's lots of specialization, so it's not one person who does all things, but one person is very good at one particular role, and you bundle these different skill-sets together if you're conducting a campaign.

But again, that isn't just happening in the dark. It's actually happening in the open. There's an interesting study from a couple of months back concerning cybercrime advertising on Facebook. For example, you can go on Facebook right now and find forums for everything from botnets to rent to buying weapons in the Middle East.

We started out touching on legislation. Providing legislation that can handle rapidly evolving and expanding technologies is quite a challenge…

The challenge is that it's not the technology; it's the politics of it. There's a wide range of things that could be done that are politically difficult to accomplish right now. For example, creating legislation requiring companies to meet NIST (National Institute of Standards and Technology) standards and the like.

Where I see one of the more interesting parts of this moving forward is going to be the cyber insurance marketplace. What can government do to encourage its growth, which would allow more marketplace solutions? And one that would be more flexible and dynamic, where insurance companies are going to be able to figure out what they think is best for their coverage, and then companies are incentivized to meet that. I think we'll be in a much better place if we can create more incentives for building out this marketplace. There's lots of discussion about those incentives, but that to me is where we'll see more coming together than just government saying, "This is required." I'd love to see certain things required in terms of standards and insurance, but that's not politically going to happen right now.

There's a similar question around the issue of information sharing, and that, again, is not a technical question. It's more a question about liability. I think we've gotten better but there's still a ways to go.

Peter Singer is a strategist and senior fellow at New America. The author of multiple award-winning books, he is considered one of the world's leading experts on 21st century security issues. He has been named by the Smithsonian Institution-National Portrait Gallery as one of the 100 leading innovators in the nation, by *Defense News* as one of the 100 most influential people in defense issues, and by Foreign Policy magazine to their Top 100 Global Thinkers List. His books include *Corporate Warriors: The Rise of the Privatized Military Industry; Children at War; Wired for War: The Robotics Revolution and Conflict in the 21st Century; and Cybersecurity* and *Cyberwar: What Everyone Needs to Know*, which was named to both the US Army and US Navy professional reading list. His most recent book is *Ghost Fleet: A Novel of the Next World War.*

Singer is a contributing editor at *Popular Science* magazine and the founder of NeoLuddite, a technology advisory firm. He has worked as a consultant for the US military, Defense Intelligence Agency, and FBI, as well as advised a wide-range of technology and entertainment programs, including for Warner Brothers, Dreamworks, Universal, HBO, and the video game series Call of Duty, the best-selling entertainment project in history.
He is a member of the US State Department's Advisory Committee on International Communications and Information Policy. His past work included serving as coordinator of the Obama-08 campaign's defense policy task force, in the Balkans Task Force at the Office of the Secretary of Defense, and as the founding director of the Center for 21st Century Security and Intelligence at The Brookings Institution, where he was the youngest person named senior fellow in its 100 year history.