Defending Digital Infrastructure

An Interview with
The Honorable Will Hurd, U.S. House of Representatives

The Hon. Will Hurd

EDITORS' NOTE *Congressman Will Hurd attended Texas A&M University, where he majored in Computer Science and served as Student Body President. After college, he served as an undercover officer in the CIA in the Middle East and South Asia for nearly a decade. Upon leaving the CIA, he became a Senior Advisor with a cybersecurity firm. He was also a partner with a strategic advisory firm helping businesses expand into international markets. In 2015, Hurd was elected to the 114th Congress and currently serves on the Committee of Oversight and Government Reform and chairs the Information Technology Subcommittee. He also sits on the Committee on Homeland Security and is the Vice Chair of the Border and Maritime Security Subcommittee.*

Will you talk about what interested you in public service and what do you tell young people about the importance of it?

It started with my interest in going to the CIA. I thought it was going to be a great way to serve my country in exciting and dangerous places. It was a great opportunity to work on the most important national security issues of the day.

The whole reason I ran for Congress was to be a leader on national security. The reality of being able to deal with some of the most challenging issues our country faces and doing it in a really difficult environment is very alluring.

If someone likes solving problems and puzzles, public service is a great way to do that and to be able to give back to our communities that we get so much from. We live in the greatest country on the planet and to be able to give back to a country that has given us so much is important.

For young people, it's not only about the intrinsic value they get from public service but we also need bright minds solving some of these hard problems, and it really is something I encourage people to do.

Do you have to work towards educating members of Congress and others about the need for legislation surrounding issues like cybersecurity?

People definitely understand the need and that is good but, in terms of how to fix it, that is where the education piece comes in.

Some of my colleagues believe that the direct-messaging function within some of our popular social media apps is considered the dark web. These are some of the basic understandings that need to be corrected.

This is where the private sector can play a role in explaining how some of these tools work and operate. We still have people in the Senate that haven't sent an e-mail yet.

I have, however, been surprised by the number of my colleagues that have come to me and asked for basic explanation on a number of these topics. People recognize the importance of this, and they also recognize that the private sector and the public sector have to work together to defend our collective digital infrastructure against adversaries.

One concern we hear within the private sector is about data collection and sharing of information. How critical is it to secure that platform for sharing information and for Congress's relationship with the private sector to be as open as possible?

The public sector needs to understand the global environment in which the private sector operates, and that many of our top companies have to deal with.

American companies are feeling pressures overseas from regulators and foreign governments, and much of that stems from a misperception about the relationship between the private sector, law enforcement, and the intelligence community.

Many of these foreign governments are using that as an excuse to take protectionist stances against American technology companies overseas.

It's important for us in the public sector to understand that things we do can add pressure to some of our top companies overseas, so there has to be a level of transparency.

As an example, many of our top financial service companies know where the next wave of malware is going to come from and how it is going to attack our financial system. I want to create collection requirements to get those assumptions to the U.S. law enforcement intelligence community to improve their collection of intelligence. Then we can get that intelligence back into the hands of all of the private sector so they can have a leg up on the next wave of what's coming. That is where we need to take information sharing to the next level.

Despite the circus atmosphere in Washington that comes across through the media, some good has happened. An example of that is the Cybersecurity Act of 2015. I believe it should have been passed eight years ago but at least we got it passed. There are liability protections in that legislation to ensure sharing between the private sector and government, and that sharing among different sectors is important.

We're scrubbing PII information at the business level. Then, before it gets to the government, we're scrubbing it twice to make sure we're protecting civil liberties – all of these things are good. That is the framework in which we can operate and establish the Department of Homeland Security's position at the core.

We can make that level of cooperation better by evaluating what information we should be sharing. The federal government should only be sharing what they can safely give, and that is information on the techniques and procedures of advanced system threats.

If we're getting that information to the private sector, it will become clear that cooperation among the two sectors is working.

When it appears that cyber-attacks are now a matter not of if but of when, is it hard to be optimistic that we can address the challenges? Is it more about how to respond or is it about prevention?

I'm optimistic because we still have the greatest minds and smartest people in the world dealing with this issue. When I was with FusionX, which is a cybersecurity firm that I helped start, we always taught our clients to operate with the presumption of a breach.

The question becomes, how quickly can a breach be detected, can we quarantine the attacker, and can we kick the attacker off the network? This is the mentality that we have to have. It's really hard to prevent anyone from getting into one's system. We have to design the network in such a way that there is a level of protection on our most sensitive stuff, but that people still have the right permissions, so this is a complicated problem.

When we leverage the power of the public and private sector together, however, we can make sure that we're able to depend on the most important digital systems. ●