Video Transcript for "Cybersecurity"

online at https://spice.fsi.stanford.edu/multimedia/cybersecurity

On-screen text:
Cybersecurity
a discussion with Herbert Lin

On-screen text:
Herbert Lin
Senior Research Scholar for Cyber Policy and Security
Center for International Security and Cooperation, FSI

Herbert Lin: The word "cybersecurity" made it into an Oxford dictionary recently—within the last several years—which defines it as those measures that you take to make sure that a computer system is protected. Or it's the state of being protected against outside threats. It's a definition that I think is particularly narrow because it says that cybersecurity is only about defending your computer system—protecting it from outside threats and maybe helping you to recover and so on. While that's very, very, very, very important, [and] part of thinking about cyberspace and security and so on, it's not the only aspect of it.

Some other aspects of it, for example, include when—and under what conditions, if any—should you (whether you're the victim or whether you're a government or something like that) be allowed, empowered, to attack somebody else's computer system. That's much more controversial. Some people say "never." I don't say "never;" I say "sometimes." And then if you say "sometimes," then under what circumstances, and how do you know, and how do you know who you're attacking, and so on? So the topic of cybersecurity—even what's covered in that—can be controversial.

On-screen text: Who are the perpetrators of cyberthreats, and what are their motives?

Herbert Lin: There's a whole stream of bad guys. There's a very, very wide range. It starts out at the low end [with] people who just investigate computer systems for the fun of it. Computer systems that they're not authorized to use. Computer systems whose unauthorized access is forbidden by law, so it counts as a crime. But they really just are curious about it, and they want to play around with it just because it's fun or [they're] curious.

There's also another set of criminals for a wider set of people who want to use cyberspace as a way of robbing you. Of stealing your money. And there are of course all kinds of interesting ways of taking advantage of cyberspace to steal money. That's where our money is. You probably bank online; I probably bank online. You know, credit cards and so on. The idea that I would use cash for a transaction now—that's a very quaint notion. Very few people use cash. And so, since money now lives in cyberspace, that's where the crooks go. And there's a lot of financial motives to be doing that.

You can be a small-time criminal in cyberspace and get a little bit, or you can be a large-scale criminal in cyberspace and get a lot. By "you," now, I mean not just you, but it could be you and your friends, you may have a small group of people, or you might join an organized crime ring. Organized crime is getting into this stuff. You can be a transnational crime ring, which operates across national borders. It can even be a crime ring associated with a national government that does hacking for profit. There are many reports, for example, that come out of the U.S. intelligence community, and North Korea does this. They sponsor hacking teams, and their job is to steal money for North Korea. So there are all kinds of ways of taking advantage of…many actors who take advantage of cyberspace as a way of stealing money.

There's still another set of criminals, or bad guys, if you will. Cyberspace is also a domain of national competition. So, for example, we have secrets that we put online because it makes it easy for us to work with them. But of course if you put them online, that means they're vulnerable to somebody else.

Well, what kinds of secrets? One kind of secrets are the intellectual property secrets. These are things like the blueprints for the next car that we're going to make, or something like that. And somebody wants to steal them. Well, is that for money? Sure, that's [for] money, but now it's starting to get into more "a nation tolerates that," and "this is economic espionage," and so on. So it has to do with money, and it is criminal under our laws, but this is a different thing than just the plain old theft of money.

And then there are the things like national defense secrets. And if you steal those… If Country A steals them from Country B, Country A isn't trying to make money off of that; it's trying to learn about Country B's national defenses. And if they are competitors or adversaries, that might give Country A an advantage over Country B. And of course Country B does that to Country A, as well. So there's all kinds of things that nations can and do do to each other to steal information for security purposes.

They also can use cyberspace as a way of destroying stuff. For example, we have an electric grid that's largely computer operated. Can some bad guy [or] some other nation come in and destroy that power grid? That would be a bad thing if they did that. It's the same access, but now they're mucking around in cyberspace for different purposes. It's not just stealing information; they're doing it to actually cause serious damage.

And, by the way, they're not the only parties interested in that. Who are some other groups? Well, we talked about criminal groups—transnational criminal groups who want to steal a lot of money. Well, there are also other transnational groups called terrorist groups. They're not financially motivated so much as they are ideologically motivated. And they have interest in doing bad things to nations, too, through cyberspace.

And yet another threat coming out of cyberspace is not just the hacks on our computers, although those are bad enough. Hacks on computers, the way they're successful, is that they're taking advantage of flaws in the information technology that we all buy and that we depend on. But in recent years—last year, for example—we have seen evidence that the bad guys, like Russia, are using information technology and the Internet in the ways in which it was exactly designed for to do us harm. So this is the hacking of elections, for example. And it's not that they go in and change the votes in electronic voting machines. That's penny-ante stuff. What they're doing is they're using the Internet to spread propaganda. And they're getting lots of people to believe it. They're hacking elections *that* way. They're creating discord in society. They're tearing us apart. So that's why you have reports that Russia is funding both sides—"Black Lives Matter" and "White Lives Matter," metaphorically. And they say, "Let's see you guys fight." They amp up the volume; they amp up the tension. This is clearly a bad thing for us. But they're doing it in ways that are entirely legal. Nobody knows how to deal with that.

That, to me, is the real cyberthreat. It's not a cyberthreat in the sense that they're going to compromise our computers and take down the electric grid [or] they're going to take down the banking system. It's not in Russia's interest to take down the banking system. They depend on it, too. China doesn't want to take down our banking system, either. We owe them a trillion dollars; they want it back. It's not in their interest to do that. Is it in their interest to have a divided, and therefore weakened, United States? You bet it is. And so that's an interesting question—as to how that threat plays out.

On-screen text: Why don't we prioritize cybersecurity more?

Herbert Lin: Why is it so hard to get people to pay attention to cybersecurity? That's a good question. And the answer is: Cybersecurity competes against other things that we want, as well. Let me give you an example. You want your computer to be usable. That is, you don't want to be inconvenienced by it. Perfectly reasonable thing. If you had your choice, you'd never use a password. The world would be benign, and nobody would ever try to steal your money. You wouldn't ever have to use a password. You just go into your account and just deal with it, and no bad person would ever go look at it. That'd be a pretty good world. We don't live in that kind of a world. So you have to put some security on it.

I don't know about you, but I have the sneaking suspicion that most of the security I use—passwords and my cell phone for two-step authentication and all that sort of stuff—mostly gets in *my* way. Mostly *I* can't use the computer. And I have to go recover my password and I have to find my cell phone and all this other stuff. Mostly it annoys *me*. This is an operability issue, a usability issue.

The whole point of security—the *whole point* of security—is to make it perfectly usable to me and totally unusable to the bad guy. If the bad guy couldn't use the information technology at all, there'd be no problem. But the bad guy has access to it because the security technology is imperfect. It can't perfectly distinguish between the good guy and the bad guy. And of course, I, as a good guy for my own stuff…I might be doing the unwitting bidding of a bad guy. So that's a real problem, right? It's not just that the bad guy wants to access my computer pretending that he's me. It's that he tricks me into doing something that he wants. And now distinguishing the bad guy and the good guy—that's a really difficult problem.

So that's one example. People want convenience. And they want security. Guess which wins in practice. Mostly convenience. Haven't you ever seen a fire door or a door that said "Do not prop open," and it's propped open? Why is it propped open? Because it's convenient for people to do it. And it's a perfectly natural sort of thing to do. That's one example.

Here's another example. Let's say I'm a startup company, and I want to bring a new product to market. You would say, "You should pay attention to security." Any person would say, "You should pay attention to security about that." I'd say, "absolutely not." Why? Because I'm trying to put out a new product, and it's going to—I don't know—call a taxi for you, or something like that. If I really want it to be secure—if security were the top objective on that—I would just not put out the product. But that doesn't make any sense, and nobody's going to give me a startup to do nothing. So I have to have a product. It has to do something.

Security is basically the absence of problems. So what I have to do is put enough security in it to make the security problems not look like very much, and then concentrate most of my effort on developing the product. Because I want the product to be something that you'll use. Any attention that I devote to security in that environment is energy that I've taken away from product development. And you know how important it is to be the first to market. That is, if I'm the first…I mean, what I'm doing, there's a competitor working on next door. And if he gets there first, he's going to take the lion's share. I want the lion's share, so I want to get out front. I have no way of doing that if I just spend a lot of attention on security. I have a finite amount of resources, and I can't devote all of it, or even most of it, to security. I have to put in just the minimum amount; that's where my incentives are. And in limited cases, the minimum amount is zero.

So, one [reason] is that security trades off against things that we want: convenience, first to market, innovation, all those sorts of things. That's just the way the world is. So you have to find some way—if you want more security, you have to have some way of rebalancing that. And nobody's figured out a good way to rebalance it.