SECURITY NOW!

Transcript of Episode #227

Cyberwarfare

Description: Steve and Leo examine the amorphous and difficult-to-grasp issue of nation-state sponsored cyberwarfare. They examine what it means when nations awaken to the many nefarious ways the global Internet can be used to gain advantage against international competitors and adversaries.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-227.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-227-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 227 for December 17, 2009: Cyberwarfare.

It's time for Security Now!, the show that covers your security, your privacy, your online persona. And with us today, as always, Mr. Steve Gibson. He's the king of security, the man who discovered spyware, coined the term "spyware," wrote the first antispyware program, and publishes a lot of free security stuff on his website, GRC.com, along with his great program, SpinRite. Hello, Steve.

Steve Gibson: Yo, Leo. Great to be back with you once again.

Leo: This is going to be a fun - I'm very, very interested in this one.

Steve: It's a topic we have never really discussed because for a long time, frankly, I had a hard time taking it seriously. I guess it's maybe I'm too close to the topic, and it just - or it seemed like a little sort of more sci-fi than real. But we're going to talk about cyberwarfare.

Leo: Wow. So it is real.

Steve: I still, you know - it apparently is.

Leo: [Laughing] Apparently.

Steve: [Laughing] Apparently it is. I mean...

Leo: Well, it's like saying espionage is real. Apparently it is. But, I mean, until you have something, you know, somebody's actually caught...

Steve: Yeah. For example, earlier this year, in 2009, in April, it was discovered that China and Russia had both infiltrated the control systems for the U.S. power grid.

Leo: Right. I remember that. We talked about that.

Steve: Yes, we talked about it. Their stuff was found there. And it's like, oh. Well, it didn't just happen to install itself. I mean, somebody put it there. And so this is clearly going on. Now, there are all kinds of different types of attacks. I want to talk about the different sorts of attacks going on, and countermeasures. And really the reason I just chose today was that John Markoff, who has been a reporter in the tech industry for years, he's now with The New York Times, and there was a front page story that John co-reported about the U.S. and Russia having essentially opened talks about signing a cyberwarfare treaty. And as I'm reading it I'm thinking, okay. Well...

Leo: A treaty? A treaty?

Steve: Yeah, it sounds dumb to me because it's not like a nuclear arms or a biological weapons treaty, where your compliance to the treaty is subject to inspection. Cyberwarfare doesn't exist in the real world. It's something - it's a technique rather than an object. So I don't know. So anyway, we've got a lot to talk about.

Leo: Very interesting.

Steve: I think our listeners will find it interesting. And then a couple big pieces of security news. And we ended up having a success. Someone put their hard drive in the freezer and reported that. So...

Leo: Oh, that's interesting. Because we've talked about that before, but I don't know if I ever saw anybody do it.

Steve: Well, he got his data saved because we talked about it, as a matter of fact.

Leo: Oh. I love it.

Steve: Yeah.

Leo: I guess we should start with the security news, Steve, and then get onto anything else that's going on, and then cyberwarfare.

Steve: Yeah. I forgot to ask you before we began the show. I heard you, as I was watching the feed as you were getting set up, you mentioned to Dick that he won the Podcast Best of Comedy stuff.

Leo: Oh, congratulations. You won the Best Technology podcast.

Steve: Yeah? I didn't know.

Leo: This shows you how much we care about things like this. I'm glad you brought that up, Steve. You are, in fact, podcast award-winner for 2009 for Best Technology Podcast.

Steve: Yay.

Leo: Beating out all the rest, including great shows like Bwana.tv. We love Bwana. He's great. FLOSS Weekly, another TWiT show. GeekBrief, Linux Outlaws, the great MacCast, Mike Tech Show, SDR News, Skepticality, and the Naked Scientist. Security Now!, Best Technology Science Podcast for 2009. And thank you to all the listeners who made that possible.

Steve: Wow, yes.

Leo: Because it was your votes.

Steve: Yes, yes, yes.

Leo: I heard that they got eight million total votes over the several week voting period. Eight million.

Steve: Wow.

Leo: So it's a significant, I mean, this means something.

Steve: Wow.

Leo: Yeah, we won - we were nominated for nine shows, and in several categories, like yours, two of our own shows nominated. And of course I know everybody else who got nominated, too. I mean, these are the best podcasts in the country, in the world. But we won for Best Comedy Podcast, that was Dick. We won for Food and Drink, that's Munchcast. Which we're bringing back because we had actually canceled the show. We're bringing it back. If you like it that much, it's back on the schedule. We're going to start doing it on Sunday afternoons at 2:00 o'clock, right after the radio show, right before TWiT. We also won for - what else did we win for? There was one more. Oh, Best Video Podcast. TWiT won.

Steve: Very cool.

Leo: And that was a tough category. I was actually - did not think we had a chance. We were competing against Buzz Out Loud, Cranky Geeks, Diggnation, Filmriot - which is a brilliant show - Mr. Deity, NASA EDGE, Scam School, TED Talks?

Steve: Wow.

Leo: Tekzilla, I mean, these are the - I was blown away that we won that one. So I had thought, oh, there's no chance. So thank you, everybody, for all the votes. And congratulations, Steve. There is a plaque or a trophy of some kind, which we will immediately mail to you as soon as we get it.

Steve: Hey, cool. That means a lot.

Leo: I expect to see it on the thing behind you there.

Steve: That means a lot.

Leo: Well, you deserve it. I mean, heck, this is a great show. It's not the first time you've won, we should point that out, either.

Steve: Although I think wasn't the first one Best Security Podcast? Or was it Best Technology?

Leo: I don't remember. I think it was technology.

Steve: Okay.

Leo: Yeah, it was technology. They're not that granular.

Steve: Right. That's very cool.

Leo: Well done. Sorry I didn't mention this earlier. You know, it just shows you that we don't - our mind's not in that...

Steve: It's funny when you talk about the number of votes and what it means. I won - you know how the senior class in high school is, like, most likely to this and most likely to that, like, in life? I won Most Likely to Be President of Bank of America, of all things. And it's like...

Leo: Huh? And actually, these days, not such a good job.

Steve: No. And I guess that was our high school's modality...

Leo: It was like the highest award you could get.

Steve: Yeah, or like maybe you're going to, I mean...

Leo: They weren't far off. You're an entrepreneur.

Steve: But my point is that I think I was probably - the only reason was that I was the only one who was, like, written in who got, like, more than one vote. Everybody else, I mean, I'm sure there were lots of other people who people wrote in for that. But, you know, two people probably said, oh, that sounds like Steve. And it's like, okay.

Leo: That's all it takes.

Steve: It just seemed so random to me then, and even more now. So, yeah.

Leo: I think that in order to get this award we probably had to get a substantial number of votes. I know that the video category - Todd Cochran, who runs these awards, and thank you, Todd, for doing this, he was saying that the video category got I can't remember how many votes, but a ton of votes.

Steve: Oh, yeah, I mean, and listen to the competition. Wow.

Leo: Yeah. I mean, it's the best. I can't believe we beat TED Talks, Diggnation, Tekzilla, I mean, these are great shows. So thank you, everybody. We really appreciate it.

Steve: Very neat. Okay. So two pieces of news. I wanted to mention that the House of Representatives, the U.S. House of Representatives, passed a significant resolution, HR 2221 [Data Accountability and Trust Act], which is the electronic data breach notification legislation. Something similar will happen in the Senate, and then they'll be put together for reconciliation, and then the final bill will be produced, and the President will sign it. And it looks like all that's going to happen because this isn't, like, super controversial or anything.

The reason it's significant and good news, well, it's sort of a mixed blessing. Right now there are completely randomly differing state-by-state regulations which make it very difficult for companies to comply because, if they're doing business in multiple states or have any kind of presence in multiple states, and in fact if the consequence of a breach affects people in other states, then they're subject to differing regulations. So having a federal law will, and this does, will supersede state-by-state regulations.

Now, I said it was a mixed blessing. The bad part is that the FTC is the enforcement side of this. But government, financial institutions, insurance companies, nonprofits, and institutions of higher education are exempt from FTC jurisdiction. So it's like, okay, well, we're making progress, but we still have a ways to go.

The other good piece of news is that when there have been major breaches which have been publicly exposed, the stock prices of the companies responsible have been substantially hit. And of course that gives the budgets of the CTOs in these companies, or the information security officers, now some more leverage with their boards, saying look, we need a budget to do what we know how to do in order to prevent us from getting a black eye if we disclose private information publicly by mistake. So that ends up, you know, in general we're moving forward, which I think is certainly good.

Now, the dark side this week is that a lot of attention is finally coming to, and that's a good thing, to a really bad SQL injection attack. I've seen reports that talk about as many as 1.2 million sites being infected, although to get to that number you need to use various sort of primary domains for the attack. The one that's most well known, and people can see it for themselves, as I had you do before we started recording, Leo, if you put into Google, you just Google "318x.com." Don't click on anything. Don't go to the sites. What this is doing is this is Google having found instances of sort of the fundamental domain of the attack.

We've done a discussion in detail of SQL injection attacks before, so I'll just summarize it by saying that an SQL injection attack is a means by which malicious parties can inject some text of their choosing into an unwitting website. For example, unfortunately, the SQL or "sequel" database is often on the back end of a web server. So the pages are being presented as a consequence of data stored in the database. Which means if you change what's stored in the database, you change the presentation of the website.

Now, databases are, for example, often behind forum systems, where you have a user-interactive forum. Or they can be behind wikis, for example, where again you've got essentially malleable web content. The problem is that it is certainly possible to secure these; but it is much easier, as is always the case, for them not to be secure. And so at the moment nearly 300,000 sites, actually I think there's a number - as we're recording this, Google is reporting 259,000 instances of the string "318x.com" in sites that it just is randomly indexing.

Now, what happens is that domain appears in what's called an "iframe." An iframe is an inline frame which, when the browser rendering the page containing this encounters it, it then essentially follows that frame to wherever the frame points. Well, what the frame contains is a script tag that says SRC - short for source - equals http://318x.com/a.htm. So that does two things. It loads, when that a.htm is retrieved from the domain 318x.com, it loads a second iframe from aa1100.2288.org, so just some random domain someone got, /htmlasp/dasp/alt.html. And then another script from some, I mean, I won't go through all of this in detail, but some JavaScript which is used for tracking.

Then that first one that I read, the aa1100.2288.org blah blah alt.html frame, it creates a third iframe pointing to another page, share.html, on the same site; loads a script from that second domain, just like a different subdirectory there. The share.html detects the browser type and writes and loads multiple browser-specific iframes which point to obfuscated script files located in the same directory. And so those further probe for the nature of what's on the client side. So, for example, it checks for MDAC, OWC10, and various versions of Adobe Flash.

Depending upon the results, then it specifically probes for known exploits, including the integer overflow vulnerability in Adobe's Flash Player, which is described in CVE-2007-0071; the MDAC connection ActiveX vulnerability described in Microsoft's note 07-009; the web components vulnerabilities we just talked about a couple months ago, described in MS09-043; the video ActiveX vulnerabilities recently described and patched; Internet Explorer's uninitialized memory corruption vulnerability. So it goes through those. And if it's able to exploit those successfully, then it delivers another file at http://windowssp.776.org/down/down.css, which you might think would be a formatting file. It's not. Down.css is actually a Win32 executable that is a variant of a known Windows 32 backdoor which is called the Buzus, B-u-z-u-s...

Leo: Of course it is.

Steve: ...trojan. And that installs a number of files: ammxv.drv under the user profiles; syesm.exe under common files; and then a bunch of things are installed in the registry, including a rootkit which prevents any of those from being seen and discovered. And the bottom line of that is that it then connects up to a server at 121.14.136.5 via port 80 to sign itself up as a trojan. And it then goes about stealing credit card and bank login information from your machine.

And this is all over the Internet, as a Google search on 318x.com demonstrates. So Windows users with unpatched systems who go to innocent sites - and again, they're not visiting malicious sites, they're visiting sites that haven't been sufficiently security aware, that have this little script tag, this iframe script tag added to them. And then, as you can see, all hell breaks loose. And you end up with a backdoor trojan rootkit installed, which then steals credit card and bank login information actively in the background.

Leo: Now, okay. So somebody who just did a search for 318x.com, sees all these sites, let's assume that some of them are still infected. And the person's running...

Steve: Oh, all of those are infected.

Leo: Well, Google's - I went to a couple, and they've been disinfected since Google did the index.

Steve: Ah, okay, good.

Leo: I mean, people, I mean, they're wising up, I guess. But assuming that it's infected, and you go there, first of all, you have to be using Windows; right? Not going to work on any other kind of operating system.

Steve: Right, because the vulnerabilities that it is exploiting, even Adobe Flash that is a cross-platform vulnerable target, it is installing a Win- it's running Windows EXEs and Windows, you know, a Windows trojan.

Leo: Although there's nothing to say that somebody couldn't embed other things on that page. But that's what we're seeing, the 318.

Steve: It's worth noting also that this is evolving over time.

Leo: Right.

Steve: From the first instance where this began to appear in November, because this thing is such a linked chain of events, the links can be changed at any time. So after, even after this script tag has been installed, it points to something that points to something that points to something. So it's very easy. And the people that have been monitoring this have seen an evolution of what this thing does over time.

Leo: Right. So, now, if I run Windows Update, and I'm updated, am I still vulnerable? Is that exploit - has it been patched?

Steve: All of the exploits which this thing attempts to exploit have been patched, yes.

Leo: Okay. So that's one way to avoid this is to make sure you keep up to date.

Steve: Exactly. And the other is to selectively enable JavaScript. Because this fundamentally is all about JavaScript. Without JavaScript there's no vulnerability. So again, if you were a person using Firefox and NoScript, where you turned on scripting selectively where necessary - although it's worth saying that the flipside is many of the sites you might visit which are infected might be ones that need scripting enabled. So you would innocently turn it on...

Leo: Ah, good point.

Steve: Yeah.

Leo: So in a way that's a way around NoScript because, hey, I want to use whatever this site is.

Steve: Yeah, I want the user forum or the wiki or whatever. And, gee, I have to turn scripting on. So you would turn it on. And NoScript does what it needs to. When you turn scripting on, it refreshes the page so that the scripts you have then enabled have a chance to come alive. Unfortunately, this thing would then grab you. If you had any unpatched vulnerabilities, you'd be in trouble.

The lesson here is, and we've talked about this often, is really do update your computers as soon as known problems are fixed because this is a perfect example. Now that this mechanism is in place, I mean, there will be lots of sites that are not attended, that will not get this script tag removed. You mentioned some you checked have been. Clearly people are informing the webmasters, hey, you've got a problem, fix this, and the webmasters do. There will be sites, in the same way that there's still Code Red is out there, installed on machines...

Leo: Forever, yeah.

Steve: ...randomly. Yeah, forever. So the problem is that until 318x.com is taken down, and who even knows where - I didn't even bother to look for the registry of that. It'd be interesting to see where it's registered. Until it's taken down, it can be pointing to anything. So the second a zero-day vulnerability appears, if there's a known exploit for it, that could get added to the list of things that this existing infrastructure checks for, and it could be very successful as a consequence.

Leo: Wow, fascinating.

Steve: So I wanted to share it because it's, I mean, it's a perfect example of a multifaceted exploit which is seeing wide-scale success, unfortunately, at the moment.

Leo: [Sighing]

Steve: On that note - on that note...

Leo: On that note...

Steve: I got a nice note from Chris Rivera. The subject was "Steve is my hero." And he said, "In a recent episode," meaning of Security Now!, "you guys mentioned the hard drive in the freezer trick. I've known about this, as well, but never had occasion to use it. Wouldn't you know my luck. My portable drive took a nosedive this weekend. This was my only backup of my kids' photos and videos. To me, this is the most important data in the world. As I plugged in the USB drive, I heard a clicking sound. I wanted to scream so loud.

"As my blood pressure was rising, I remembered you guys talking about the freezer trick. So I froze my drive and reconnected it later. It showed up, only to quickly die again. It would only run for maybe 60 seconds at a time. Without much hope, I fired up SpinRite and put it to work at Level 2 on the 320GB drive. 12 hours later, it had reported that there were no sectors bad or unrecovered. In fact, it didn't report anything at all. But I remembered you talking about how sometimes SpinRite fixes drives without anything to report. So I plugged it up to my Fedora box, and voila. I was able to copy the entire drive contents over to my workstation. You have saved me so much heartache."

Leo: That's great.

Steve: "I will never trust portable drives again. That was my third one to go bad. Each time I lost pictures of my kids. Luckily I have backups. But I've never had recent full backups, and have always lost some of the data. I am most impressed with SpinRite. Thank you so much for creating such an amazing application. I hope I will never have to use it again (I mean that in a good way). Did you write that in Assembler? Keep up the amazing job of Security Now!, Steve and Leo. Signed, Chris."

Leo: Awesome.

Steve: So happy...

Leo: It's good to know that works. I mean...

Steve: [Indiscernible] story, yes.

Leo: There's always been one of those, you know, I always thought it was kind of an anecdotal thing. But I guess it does work. It makes sense that works; right?

Steve: It really does because it's just, you know, drives are running on the hairy edge as it is. I mean, the sectors are requiring lots of correction. The reason that SpinRite is effective as a preventive maintenance tool is that it's able to go along and fix the problems before they get pushed to the point the drive can no longer fix things. But even something as random-seeming as freezing the drive just, I mean, it just changes enough that the drive has a chance to work again for, like, one last try. So it's funny, too, he mentioned external drives. I'm concerned about the heating of external drives because many of these little enclosures provide no active air flow across the drive.

Leo: Right.

Steve: And many drives are designed, first of all, they're running fast. They're generating a lot of heat. But there are good enclosures that do have a fan, that are actively cooling the drives. But drives really do not like to get overly hot. That will really hurt them. And so one of the problems I think we're seeing, I mean, these external enclosures are very popular. But be conscious of the problem of the drive getting too hot. Maybe, for example, don't just leave them on, plugged in all the time, but plug them in only while you're actively transferring data to and from them, and then unplug them so that they're not just sitting there, day in and day out, running with no active air flow across them because they really will overheat. And he talked about three of them dying on him. And it may very well be that they're just getting too hot. I see that, we see that a lot.

Leo: I wonder also if heating/cooling, heating/cooling is worse than just staying hot. I mean...

Steve: Well, there is that, too. You're right.

Leo: You don't want to expand/contract, expand/contract. It wears out bearings, there's metal fatigue, there's all sorts of issues that go along with that.

Steve: That's true.

Leo: I just - they don't - it's all magic to me. These things shouldn't work anyway. They're way - the density on these things, the speed, it just doesn't make any sense at all.

Steve: I completely agree.

Leo: Whoever thought that - Jerry Pournelle was talking about that on TWiT I think a couple of weeks ago where he, like you, like me, like anybody who'd been paying attention in the '90s, fully expected that by now we'd be using something else, solid-state memory or something.

Steve: Yeah.

Leo: I mean, spinning drives? Come on. Terabytes? You're kidding. Okay, Steve. Let's get to it. Cyberwarfare, our topic.

Steve: So when I was looking around for some specifics, I ran across an interesting interview which the PBS show "Frontline" had done with John Arquilla, who's the associate professor of defense analysis at the Naval Postgraduate School. And I'm going to share the beginning couple paragraphs of this because I think it sets the tone really nicely for this discussion. And this interview was six years ago, in March of '03. So John says:

"I came to the whole cyberwar business as a bombs-and-bullets guy. I didn't know a whole lot about computers. But when I was working for the Central Command in the last Gulf War" - which, you know, the first Gulf War - "it became very apparent to me that our biggest advantages came from what we knew and what our opponent didn't. On the spot we cobbled together something called a Joint Surveillance and Target Acquisition Radar System. This allowed us to know exactly where the opponent was and how to strike him.

"It occurred to me in the wake of that tremendous and lopsided victory of ours that much of what we did could have been held hostage to the disruption of any of those information systems. That was the beginnings of cyberwar, the idea that the vulnerability of communications could cripple an advanced army. What made it strong also made it weak. Then it was only a baby step from there to think about this happening across our entire society, commercially and socially. The crippling of information systems could have profound disruptive effects.

"What made that thought even more chilling was the notion that this power existed in the hands of a few hackers. The disruptive power of this small group was growing by leaps and bounds. This was something that we were vaguely aware of through the '80s, but really came into its own in the '90s. What bothers me more than anything else, as I look at the data each year coming out of the various computer emergency response teams, is that hackers could do a tremendous amount more damage than they choose to do. This says to me the threat is real. We need to get our arms around it before people do get serious about making costly, costly disruptions a way of life."

Leo: Wow.

Steve: And, you know, it's funny, what struck me when I read him talking about hackers could do so much more damage than they so far have chosen to do, I mean, we've talked about that often here. I've remarked that, I mean, almost quizzically that these viruses only so far seem to exist for their own sake. They're like little proof-of-concept things. They're kids...

Leo: Sure, but that's how you would do it; right? If I were a bad guy, I would do a little testing first; right?

Steve: Well, of course and that's what happens is that, you know, kids with spare time on their hands...

Leo: That's how they learn.

Steve: Exactly, they create these things. Now, I actually think that that ends up being a huge - we'll in retrospect, when we look back on all of this development of computers and networking communications, that will end up having been a huge blessing because it is these relatively innocent proof-of-concepts which have raised our awareness of the problem. I mean, that's what's created Symantec and McAfee and all the other antiviral, antimalware responses, is these things are vulnerabilities that exist in our machines where the vulnerability is being demonstrated without really being exploited. Except I would say now that we're beginning to see that change.

We know that organized crime is getting involved. And when I was talking about what this backdoor trojan does, this Buzus trojan that is using the SQL injection attack, well, it's actively hurting the people who end up hosting it unwittingly. It's stealing their credit card information and their bank logon data. So I guess we've - it's clear that we've crossed the threshold between purely benign - oh, I'm a virus, and I'm just here to replicate for my own sake - now we're beginning to see the exploitation of this. But overall, in the context of nation states employing these sorts of things, if it weren't for the fact that we had this infrastructure of monthly patches from Microsoft and the idea that our systems are porous, essentially, they are not rock solid.

Software has bugs. Bugs can be turned from things that crash your computer into things that actively exploit the porousness of our defenses. That really creates an opportunity for further exploitation. So as I was thinking about this, I thought, okay, we use this prefix "cyber," and we've talked about cybercrime and cyberterrorism, and now cyberwarfare. And it occurs to me that it's the users of these, or the attackers who are employing these things - the thing that differentiates cybercrime from cyberwarfare and cyberterrorism really is the motivation. So, for example, monetary profit I would argue would be behind cybercrime. If we decide that, like, warfare is something that nations do against each other, then they're not trying to profit monetarily. They're trying to in some way attack some other nation that they've decided they're at war with.

And in all of this case, there's this serious problem with attribution, that is, attributing the source of the attack. When we were talking earlier about the malware that was found installed in the U.S. power grid control system, there was belief that it was - that some of it was Chinese, and some of it was Russian. But of course...

Leo: You can't tell.

Steve: ...their governments disa- you're right. Their governments disavowed any participation, said no, you're crazy, it's not ours. Well, and all we have is suspicions. So there's a sort of a fundamental sort of plausible deniability about anything that's going on in this cyberspace. And, for example, even in instances - we've talked about this before - where control systems for, like, botnets have been tracked down to specific countries, well, even when we find the control computers, and they might be in, for example, China, we don't know that there's anything that's China-based about where they came from because that control computer could be under the control of a computer located in an entirely different country.

So, I mean, it's interesting. I've read articles about the fundamental problem of the Internet being this autonomous routing technology, which we've also often talked about, how a packet dropped anywhere in the world now onto a network with a given destination IP address will be picked up by the router on that network, which inspects the header of the packet, looks at the IP address, and forwards it on in the direction of its destination. It doesn't care anything about the source IP. Now, there are some filters, for example, on the ISP networks which prevent spoofing of source IP. But that's within a given domain, and that's the exception today more than the rule. In general you just drop a packet anywhere in the world into a network with a given IP, and that packet will end up at that destination, with no backtracking, no way of knowing where it came from, no authentication. I mean, it's the strength of the Internet, the resilience of the Internet comes from this.

But it is - it also is a, I mean, from a standpoint of attribution of sources of attacks, sources of any type of malicious conduct, I mean, it's a huge Achilles heel. And I can't see, having thought about this, any practical way of getting to a more secure technology without adding a massive burden to the way the 'Net works. I mean, one of the reasons it works as well as it does, it's as inexpensive as it is, it's able to grow and be flexible and resilient, is that trusting nature. If there was some sort of public key crypto where packets had to be signed, for example, in a succession of envelopes where a router would only accept a packet from another router if it was authenticated, then you could potentially have backtracking provability, but at a huge expense. The packets would grow in size. There would be this massive public key verification and signing needed at each step. I mean, basically none of it would work nearly as well as it does.

So it's really difficult to see how we get there from here. And of course the other problem that the Internet has is that to some degree the equipment that we're using are black boxes. We fundamentally trust them. We purchase them from suppliers and plug them into our networks. It says "Cisco" on the front, for example, and it looks - it's got that Cisco green paint on it, and it looks like a Cisco router. Well, we don't go in and inspect them. We don't know for sure what's there. And there have been instances of counterfeit Cisco routers coming from other countries that have questionable software installed in them, and in some cases known malicious software.

Leo: Right.

Steve: So there we have what we think is a trusted appliance. And upon inspection it turns out that this is a counterfeit. And we also have seen stories where cryptographic equipment, we talked once about how there was cryptographic equipment purchased, I think from a company in Switzerland, which upon inspection turned out to have known backdoors installed in it, and other countries were buying this on the reputation of the seller, which was stellar. But nonetheless, backdoors were discovered which would allow other nations, at the national, nation-state level, to access this data which some other nation was depending upon being impervious to decryption. So that kind of cyberintelligence, or counterintelligence, is, we know, probably also going on. We know that it has. There's no reason to imagine that it hasn't.

So it seems to me that we could broadly divide attacks into - cyberattacks, cyberwarfare - into two broad categories. There's stuff happening in the background, and there's stuff happening in the foreground. By background I mean sort of like behind our backs. Quiet, continuous, the kind of thing that is probably happening all the time. And then foreground attacks are things like bandwidth floods, like huge denial of service attacks that, you know, that attempt to swamp networks. My feeling is that those would have to be ineffective to some degree on an international basis.

For example, one has to imagine that the United States, and probably maybe all nations, have, like, a kill switch on their transnational Internet links. That is, it must be possible, for example, for someone somewhere in the U.S. government to say, okay, take us off the 'Net. Literally, you know, take the U.S. off of the global Internet. Cut our transoceanic links. Cut our satellite links. We need to be an island for a moment. It's just hard to imagine that that facility doesn't exist. Which means that flooding traffic that was coming across those links would get blocked. And so would, for what it's worth, you know, nonflooding sort of malicious traffic, which is operating in a much more stealthy, non-in-your-face, sort of just bandwidth attack mode.

On the other hand, one wonders if the bad guys, I mean, we being bad guys relative to other countries, other countries being bad guys to us in this - in a cyberwarfare scenario, if there would be other assets installed in country that could act on behalf of a nation outside of that country's borders, maybe in the event of it being cut off, or maybe using some other communications means to activate something that is sort of essentially a sleeper agent cyber thing that has been installed. I mean, the problem with all of this is its presence is potentially unknowable. It's just - it's like bad firmware installed in appliances that essentially are sleeper agents that are in country waiting to be activated and then do who knows what.

Leo: I love that kill switch idea.

Steve: Yeah, don't you think there has to be that?

Leo: I have to think that anything that we can think of at this point they are doing or have at least thought about; right? I mean, they game this stuff all the time. They are always looking at these scenarios. So I presume that they're kind of looking at ways to respond to this. And that's an obvious one, a kill switch. Big red button for the President to push.

Steve: Yeah.

Leo: Takes us offline.

Steve: As I was thinking about all of this, I mean, this whole sort of almost to me sci-fi dimension, the flipside of that is that we're becoming, thanks to the Internet, I mean, thanks to this Internet which represents this potential threat from cyberness, it's also really knit the globe together into in many ways a single economic entity. And, I mean...

Leo: Well, we are, I mean, economically we're all linked. You know, if somebody brings our economy down, we know this, we just saw it, it hurts everybody. And so this is war. This is the same thing as a nuclear war. This is a scorched-earth kind of alternative scenario; right?

Steve: Well, exactly. And I think that's my point is that, I mean, we know that China is building its military. I've seen many reports that talk about China's really putting an escalating effort into cyberwar potential. And I think, okay, but wait a minute. Who are they going to aim that at? I mean, are they going to aim it at us? The American consumer is supporting a lot of China's economy from purchasing so much stuff. And so how are we going to be at war with China? I mean, to me that doesn't make any sense. Again, it's - once upon a time, when national economies were only national, you could imagine lobbing bombs at each other. But maybe I'm just being nave here.

Leo: Well, maybe it's a crazy idea. But remember they had that nutty idea of limited nuclear war. Maybe there's such a thing as a limited cyberwar, like a kick in the shins, where it wouldn't necessarily take everything out, but it might be like a little nudge with a threat, an implicit threat. And I think if - I think there was a very clear and implicit threat with the trojans that were found in our electrical grid. In a way maybe that was the point - not testing the technology, but to say we have the means.

Steve: There was also - I read a report that talked about a U.S. capability to infiltrate other countries' networks, which surprised me in its apparent effectiveness, and that our intelligence and ability to conduct cyberwarfare was so great that there was a concern that we would disrupt normal civil and civilian operations if it wasn't kept under control. That is, it was difficult to constrain it to military targets, and that it could leak out and affect - essentially we don't have the ability to target as well as we need to. We've got things that are a little too blunt. But the idea that we even have such things is like, whoa, okay. I mean, again, as a technology...

Leo: I'd be more "whoa" if we didn't. You know, I'd be more "uh-oh."

Steve: And, see, that's the other thing, too, is I wonder if some of this isn't the military saying to the politicians, well, what if? I mean, you can "what if" anything and scare the bejeezus out of people, politicians, and say we need hundreds of millions of dollars to develop this, if not billions, because we know the other side is doing it. It's like, okay, what? Okay, I guess. So they've got a bunch of hackers who are really good, and they're actively attempting to penetrate our networks. Okay. So we do the same?

Leo: Yeah, I mean, I don't know. Yeah, I guess we have to; right? To me it's very much like espionage. It's in the same kind of realm as espionage.

Steve: Sort of dark and murky, and no one's really sure.

Leo: Well, if they're spying on us, and we presume they are, then we need to spy on them. We have to have counterespionage. I think it's very analogous to espionage, with the difference that it's a weapon. So espionage can escalate to sabotage. And cyberwarfare could escalate to sabotage in the same way, I guess.

Steve: Well, yeah. And it seems to me, too, that the way this is being portrayed is as not a standalone attack. That is, we wouldn't - no country would launch only a cyberwar attack on another. But it would be part of a broader disruptive umbrella. So, for example, if, I mean, inconceivable as it is, the U.S. and China were ever to come to fundamental blows, then I guess there would be a massive, I mean, from everything we've read, a massive cyberwar, I mean, component...

Leo: Absolutely. Absolutely.

Steve: ...to what was going on in an attempt to disrupt each other's systems.

Leo: And it would be very effective. I interviewed a guy many years ago, this must have been 15 years ago, who wrote a book on cyberwarfare, who said you don't do it by itself. In fact, he used the grid as an example. What you do is you disrupt the grid with both cyberwarfare and sabotage. You blow up a few power plants. But you also make sure that you're in the computers that would then switch them over. You can create very easily with a few small incidents and computer hacking, you can take out the entire grid of the United States. And that would not by itself be a problem unless you were then also launching an invasion or bombing or sending nuclear missiles. So it's part of an overall strategy, not something that would exist by itself.

Steve: Right.

Leo: I mean, if somebody took down the grid, that'd be bad. But eventually you'd fix it. It's only as part of something much more serious that you would even contemplate this, I think. Now, if you're trying to undermine - now, then there's subtle things. If you're trying to undermine our economy by creating - years ago I remember there were always rumors that foreign governments were printing counterfeit dollars.

Steve: Right, hundreds.

Leo: The Soviets were doing that.

Steve: Yeah.

Leo: And the idea being that they would then circulate them and create huge deflation in the U.S. If there were an ideologue out there who said, well, we don't want to destroy the U.S., we just want to prove that capitalism doesn't work, nowadays they wouldn't print $100 bills. They would just create false trades and derivatives, and there'd be a lot of cyber ways to do this.

Steve: They would do the things we just finished doing to ourselves.

Leo: Unfortunately, yeah, they'd do what we did.

Steve: Yeah.

Leo: So that's what I'm saying is I think there's a lot of different ways to use this and look at this. This is a very interesting tool. And I know for a fact that the U.S. has been very aware of this for at least two decades and has worked very hard to both do counterwarfare and to have our own initiatives; right?

Steve: And I think what must be happening, then, is that - first of all, I think that what you're discussing is sort of - or were briefly there - I would call cyberterrorism.

Leo: Yes.

Steve: That is, more of a non-state actor that is using electronic information system...

Leo: Well, it could be a state actor. Remember the Soviet Union wanted to prove that capitalism was bad.

Steve: Yeah.

Leo: But it also could - so it could be state, or it could be...

Steve: Or independent.

Leo: ...independent.

Steve: Yeah.

Leo: I mean, the interesting thing about cyberwarfare is it doesn't require huge resources. You don't have to build a weapon of mass destruction. You don't have to...

Steve: No, and that's a very good point, too. Because, I mean, when we were talking before the show, or I guess at the top of the show, one of the things that strikes me as odd about this is that there isn't anything for either side to inspect about the other. The notion of us signing a cyberwar treaty, I mean, to me that just strikes me as ludicrous because how is anyone going to know that you're in compliance? And why would anyone be in compliance? I mean, it seems to be that everyone is taking this so seriously although, I mean, I'm trying to get my head around it because it's hard for me to take it as seriously as everyone else seems to be. But given that everyone is taking it as seriously as they are, then no one is going to abide by a treaty where what you're entreated against doing can't be found, can't be proven.

Leo: Yeah.

Steve: So everyone's going to just say, oh, yeah, we're all - we've stopped doing that. Meanwhile, as you say, a small group are able to develop strong cyberweapons, potentially. You don't need a huge industrial complex to do that. And so I guess it's just that over time, as the Internet is becoming more pervasive, and it's not a curiosity, it's becoming, well, as we've been discussing recently, now having access to it is being considered a human, a fundamental right of being alive, or being able to have access to it. Clearly countries are looking at it and saying, okay, well, we're not sure what it is, but it's something. And we'd better understand what it is because it seems that other countries are working to understand what it is. And it's going to be a component of national defense.

Leo: Some people in the chatroom are making a point that a treaty might also have importance in terms of protocols for communicating, to say hey, this isn't our attack. Or here's, let's, you know, it could be more than just we won't do it if you don't do it. It could be that there's more subtlety involved. It could be saying we agree not to do these kinds of things, or we should have some sort of early warning system that we jointly sponsor. I imagine there are things to talk about; right?

Steve: I think that's a very good point. John Markoff's article did only talk about sort of this mutual agreement not to develop. I mean, what was talked about in the article was an agreement not to develop cyberwarfare technology. Which struck me as like, okay.

Leo: That's impossible.

Steve: Good luck with that.

Leo: I don't think that's doable, yeah. No, my reaction to that is, no. Crazy.

Steve: Yeah.

Leo: But I think there might be more that we could talk about; right?

Steve: Yeah. Yeah. And I'm not a pacifist, but I'm not overly aggressive, either. And so I think talking is good. Talking is better than not talking.

Leo: Absolutely. Well, very interesting subject. I'm so glad you brought it up. The notes, Steve's copious notes are online at GRC.com. You can find those there along with 16KB versions of the show which Steve puts together - thank you, Steve - and transcripts, which Steve pays to have done by the great Elaine. Elaine Farris; right?

Steve: Elaine Farris, yup.

Leo: She does such a wonderful job. [Aw.]

Steve: Our transcriber.

Leo: So you can read along as you listen, or read instead of listen, or listen instead of read, or whatever you want. Whatever you want to do. While you're at GRC.com, look for those great free programs that Steve gives away. Wonderful stuff. We were talking on This Week in Google about your DNS program and how good that was.

Steve: Oh, cool.

Leo: Yeah. And also, of course, SpinRite, the world's best hard drive maintenance and recovery utility.

Steve: Yay.

Leo: Yay, SpinRite. Do it first so you don't have to freeze your drive.

Steve: There you go, exactly.

Leo: And congratulations once again. Best Technology Podcast.

Steve: Oh, that's so neat.

Leo: Isn't that a nice feeling? That's...

Steve: That is great.

Leo: We'll send you the trophy.

Steve: Thank you, Leo.

Leo: We will see y'all again next week. We do this show live on video, and you can watch every Wednesday at 11:00 a.m. Pacific, 2:00 p.m. Eastern time. I think, I've got to get my UTCs together, but I think if I'm correct that's either 1900 or 2000 UTC. You can also download video soon from TWiT.tv. And in a few weeks we'll be able to get podcasts of that and have it on the Roku box and all that stuff, too. We're moving ahead.

Steve: And next week is Christmas Eve, but Security Now! will be there.

Leo: Amazing. How do you do it? We'll see you then.