SECURITY NOW!

Transcript of Episode #861

Rogue Nation Cyber Consequences

Description: This week we examine many of the cyber-consequences of Russia's unilateral aggression against Ukraine. In a world as interconnected as today, can a rogue nation go it alone? Ukraine has formed a volunteer IT Army. Hacking groups are picking sides. Is Starlink a hope? Actors on both sides of Russia's borders are selectively blocking Internet content. Google has become proactive. The Namecheap registrar has withdrawn service. Use of the Telegram encrypted messenger service has exploded. Cryptocurrency exchanges block tens of thousands of wallets. Russia releases the IP addresses and domains attacking them, and likely some which are not. They also prepare to amend their laws to permit software piracy and appear to be preparing to entirely disconnect from the global Internet. All of the technologies we've been talking about for years are in play.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-861.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-861-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. Kind of a single topic show this week, everything Ukraine. What's going on in the war, cyberwarfare, the call for cyber hackers, Russia's response, and then the very real prospect of Russia disconnecting completely from the Internet. Steve talks about it all next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 861, recorded Tuesday, March 8th, 2022: Rogue Nation Cyber Sequences.

It's time for Security Now!, the show where we cover your safety, security, and privacy online with this guy right here. No, not this guy right here. That's the Linux penguin. This guy right here, Mr. GRC.com, Steve Gibson. Hi, Steve.

Steve Gibson: Yo, Leo. Great to be with you again, once again. Lorrie this morning asked me, she said, "What number is this?"

Leo: She's counting down, isn't she. I know, I know.

Steve: 861.

Leo: So she says, "Only 138 more?"

Steve: That's right. We're going to make it. We're going to make it. And Leo, at only 52, actually 51 - oh, no, but we do count that one, so 52 a year - yeah, we've got a few years left.

Leo: Yeah, couple and a half years, yeah, yeah. We're good.

Steve: We're okay. Okay. So there was some interesting news about a proposal from the EU that involves mucking around with TLS certificates, and it's got all of the browser vendors up in arms. And that's what I was going to talk about. But all of the news, well, okay, with a few exceptions, the vast majority of the news was about the cyber consequences of what's happening with Russia and Ukraine. So, and as I began to flesh that out and pull things together, I just thought, okay, I don't have room for anything else. So we'll probably talk about that next week when I dig into it and see whether it's podcast-worthy.

Today's Episode 861 for March 8th is titled "Rogue Nation Cyber Consequences." And I think a lot of really interesting cyber aspects to what's happening. We've got the Ukraine - I'm sorry, Ukraine. I'm trying to educate myself. We're not supposed to say "the" anymore. That's an old way to do it. Ukraine has formed an IT army with amazing strength. And sort of the theme of this is, with the world as interconnected as it is today, can a rogue nation go it alone? We're seeing lots of consequences of what's happening as a result of this. As I said, we've got the IT army. We've got hacking groups, many of them well known, forming up and picking sides in this. The question is whether Elon Musk's Starlink might be a hope where connectivity is being threatened.

Actors on both sides of Russia's borders and, well, yeah, both sides of Russia's borders are selectively blocking Internet content. Google has become proactive now. One domain registrar, Namecheap, has decided to withdraw its services in a way that I find a little questionable we'll talk about. We also have the surprising, well, maybe not that surprising, explosion of the Telegram encrypted messenger usage as a consequence of all this. Cryptocurrency exchanges are blocking tens of thousands of wallets. Russia's released the IP addresses and domains attacking them, and it looks like some that are probably not actually doing that.

They're also preparing, believe it or not, well, yeah, you can believe it, to amend their laws to permit software piracy. And they appear to be preparing to entirely disconnect from the global Internet, something that we talked about last summer when they did a DNS dry run. So this is all the stuff we've been talking about for years. Everything's in play. So lots of news to talk about relative to the cyber consequences of someone upsetting the rest of the world. Is it possible these days to be on your own? I don't think so.

Leo: Yeah, I think it's interesting. We talked - Cory Doctorow was on TWiT on Sunday, and we talked about why it would be a very bad idea for ICANN to disconnect, as at least one Ukraine minister requested, disconnect Russia from the Internet. That's not how it works. So, yeah, good topic coming up. Certainly very timely.

Steve: Okay. So our Picture of the Week is just one I've had, it's not apropos of today's topic, it was just around, and it's kind of fun. And I just thought it was interesting how the laptop is now the icon for the computer. You know, once upon a time it was staring into a big screen in front of you. But you never see that anymore; right? It's just people use laptops. That's just - anyway, just random observation.

But anyway, so our guy, he's got his wife behind him sort of like with her hand on his chair back and looking on at what he's doing. And he's saying to her as he's typing on the laptop: "Of course this website is safe. As an extra measure of security, they make you sign in with your Social Security number, mother's maiden name, your bank account, your home address, phone number, and date of birth."

Leo: It's got to be you.

Steve: Nobody else would know that.

Leo: Well, not until I do it, yeah.

Steve: Okay. So unsurprisingly, as I said at the top of the show, the world cyber news this past week was dominated by the cyber aspects of Russia's invasion of Ukraine. We've been living through, and this TWiT podcast network has documented and chronicled important and fascinating aspects of the evolution of the personal computer and the Internet. When I think back, Leo, to where we were with Honey Monkeys, you know, almost 18 years ago, it's like, okay, a lot has changed. HTTP was a thing, right, with no S. Now, good luck if you don't have an S there.

And I have to admit that when this podcast, Security Now!, began, I was personally skeptical of the idea of cyberwarfare. It just, like, really? Like packets? Well, obviously since then I've been well disabused of any such skepticism. And I've been interested to note that in the last few weeks all the experts, because cyberwarfare is a topic now, like any time there's a discussion of what's going on, it's like, oh, this threat of cyberwarfare. And the presumption is that it would not be constrained to Russia and Ukraine. It would be global to some degree.

But the point is that all the experts that I'm hearing talk about it feel much as I do, which is that it's something no one is really that excited to unleash, very much like the Cold War days of mutually assured destruction. As I said last week, the feeling is that no one has any real confidence in their own defenses being adequate. So nobody wants to be the first to initiate what - whoa. I forgot to turn that down, our little friend telling me I've got email, sorry.

No one's that confident about their own defenses being adequate, so no one wants to be the first to initiate what might be mutually assured cyber destruction. We don't even know what that looks like. And nobody wants to find out. Yet here we are today kind of picking around the edges of exactly that possibility, such that more than any other time in the past it's on everyone's lips.

Okay. So I'm not going to spend an inordinate amount of time on any one of these topics. But literally, as I was going through the last week's what is there to talk about, it was all about this. It was all about the consequences of this. So Saturday before last, on the 26th, Ukraine's Minister of Digital Transformation, whose name we'll hear of a few times today, Mykhailo Fedorov, announced the creation of an army of IT specialists to fight for Ukraine in cyberspace. Mykhailo said: "We have many talented Ukrainians in tech: developers, cyber-specialists, designers, copywriters, marketing specialists, targeting specialists." Wow, targeting specialists. And he said: "We are creating an IT Army. All operational tasks will be posted here. There's plenty to do for everyone. We continue our fight at the cyber-front."

So of course being that he's their digital transformation guy, his focus is that. Anyway, turns out that Mykhailo's call did not go unheeded. When I captured this particular report, the number of volunteers that had signed up, and we'll see that by the time we end this podcast that number has grown, at this point it was already 175,000 people had said yeah, I want to, you know, sign me up.

Leo: What?

Steve: 175,000.

Leo: Wow. I didn't know there were that many people with skills.

Steve: Well, and they said copywriters, marketing specialists.

Leo: Oh, all right. Okay.

Steve: So, you know, like you don't have to actually know how to sharpen the front edge of a packet in order to send it off.

Leo: Wow.

Steve: You just have to know what that packet should contain, I guess, if it was some propaganda or something.

Leo: They're going to need some IT specialists to manage the database of volunteers.

Steve: That's right.

Leo: Is what they're going to need.

Steve: That's right. So he said: "Many have been tasked with launching DDoS attacks against Russian websites including government websites, banks, and energy companies. On the 27th, the day after this, officials also told volunteers to target websites registered in Belarus." Mykhailo also publicly released the targeting list. Okay? So this is the IT Army of Ukraine. It says: "For all IT specialists from other countries, we translated tasks in English." So, he says: "Task #1. We encourage you to use any vectors of cyber and DDoS attacks on these resources."

So, I mean, this is a publicly posted list from Ukraine. So we've got three categories: business corporations, banks, and the state. So, for example, business corporations: Gazprom, I can't even pronounce these things. I won't try. But there's like [counting aloud] 19 specific business corporations where their URL, and I think without exception, oh, there is a .com. By far the most are .ru, of course. Though there are some - there's a .org. Predominantly .ru. Then we've got three banks: the Sberbank, VTB, and

Gazprombank. And then the third category is the state. There's public services; Moscow State Services; President of the Russian Federation; Government of the Russian Federation; Ministry of Defense; Tax, whatever that is; Customs; Pension Fund; and our favorite Roskomnadzor is also there.

So, I mean, obviously they're being put upon, that is, Ukraine is. And they're saying, hey, cyber is now a vector of counterattack. So let's go. And here's your initial targeting list. Yikes. An open call for anyone and everyone to participate. But let's be clear that the perceived justice, if that's how you feel, of this cause doesn't make it legal. Right? So people listening, you know, don't go off attacking Russia because some guy in Ukraine said, yeah, here's where you go. Don't do that.

According to Victor Zhora, an official at the Ukrainian cybersecurity agency charged with protecting government networks, he said: "Russian media outlets that are 'constantly lying to their citizens,' and financial and transportation organizations supporting the war effort, are among the potential targets for digital attacks from the so-called Ukrainian IT army." He said that the IT army is a loose band of Ukrainian citizens and foreigners that are not part of the Ukrainian government, but Kyiv is encouraging them. It's an example of how the Ukrainian government is pulling out all the stops to try to slow Russia's military assault, and illustrates how cyberattacks have played a supporting role in the war.

The goal of this IT Army of Ukraine is to "do everything possible to make the aggressor feel uncomfortable with their actions in cyberspace and in Ukrainian land." And so this was Victor Zhora in a videoconference with journalists on Friday. And I will say, because I've just gone through this myself, assembling the 17-page notes for this podcast, if you follow along, by the end of this podcast I would argue you will have a very mature, complete, almost comprehensive, I dare say, appreciation for everything that is going on, like everywhere on this. It's what we're here to talk about.

So one organization, the so-called Cyber Unit Technologies, the CUT, is paying for attacks on Russia. Given what we've been seeing in the news, it's unclear actually why you would need to give any Ukrainian hacker a bounty to encourage them to launch cyberattacks against Russia. Just making it legal is all I would need, I would imagine. But last Tuesday, a week ago, the Kyiv-based cybersecurity firm Cyber Unit Technologies initiated a campaign to reward hackers for taking down Russian websites, pledging an initial $100,000 for the program.

Although, as we'll see next, many traditional criminal gangs have publicly expressed their allegiances either way, this CUT emphasized that the company only seeks to work with locally known security experts, they said to prevent infiltration by Russian agents. And actually they referred to them as "white hat hackers." And that gave me pause because I'm thinking, okay, wait a minute. I'm not sure that your hat stays white when you attack anybody else. Again, no matter how you feel about it, that sort of seems like your hat's going to get at least a little gray in the process.

But if such hackers already had mature tools that they had been using for sanctioned, you know, we've talked about red, blue, and purple teaming; right? You know, all of the attack and counterattack, in order to build up through drills and exercises the skills that you need both to predominantly to defend against attacks, but you need to have somebody attacking you; right? So you use a team to do that. They might well be able to retarget those tools which have been sharpened as a consequence of doing local drills. And you kind of have to imagine that Ukraine, being as much in Russia's cyber crosshairs as they have been for the past 20 years, that they've had the occasion to develop and hone such tools over time.

So this is probably the reason why NATO's - NATO has an organization known as CCDCOE. Everybody likes their abbreviations. That's the Cooperative Cyber Defense Centre of Excellence which has, just as a result of its 30th committee meeting, invited Ukraine to become involved as a participant in this Cooperative Cyber Defense Centre of Excellence. It is a NATO organization. Ukraine of course is famously not a member of NATO. But yet they're going to be invited in because they have so much expertise that they're going to be able to share.

So, okay. Hackers taking sides. As a result of Russia's determination to unilaterally and by sheer force attempt to illegally annex Ukraine as they previously did Crimea, we have the world's well-known hacking groups now squaring off and taking publicly declared sides for and against. Last Friday, Recorded Future's publication The Record described the declarations on both sides as follows.

They said: "Russia's invasion of Ukraine has taken place both on and offline, blending physical devastation with escalating digital warfare. Ransomware gangs and other hacking groups have taken to social media to announce where their allegiances lie. The Record will be tracking who these groups align with, as well as any attacks they launch related to the conflict. Many of the pronouncements from these groups include threats against critical government infrastructure. Some collectives are state-sponsored, while others are decentralized; but all are able to take down computer systems and breach organizations."

Allan Liska, a ransomware expert at Recorded Future, said: "It is now an inevitable part of any military action that so-called 'Cyber Patriots' will engage the perceived enemy, either of their own free will or at the direction of their own government. Some of these activities, such as Anonymous launching DDoS attacks, will be nothing more than minor nuisances; but others could have real consequences. Ransomware groups, for example, have more targets than they can go after right now and may decide to focus on attacking the enemies of their country to create real disruption. And the more skilled groups can have an even greater impact." Liska warned that Sandworm and UNC1151 are among the most concerning in terms of their capabilities and activity, and should be closely monitored.

Okay. So what do we know at the moment about who's on which side of this mess? Well, the well-known collective "Anonymous" declared via Twitter on February 24th that its collective is "officially in a cyber war against the Russian government." The group later tweeted that they had targeted the Russian state-controlled international television network RT, and "has taken down the website of the Russian propaganda station RT News."

Now, we've talked about Anonymous. Everyone is probably familiar with that logo that they use. They describe themselves as a "decentralized hacktivist group that targets different government institutions and government agencies, corporations, and the Church of Scientology." Okay. There's also GNG, a hacking group affiliated with Anonymous. They've gained access to Sberbank's database and leaked hundreds of its data files. Sberbank, who is Russia's largest lender, is apparently now facing failure.

NB65 is another affiliate of Anonymous who tweeted their support for Ukraine: "Anonymous is not alone. NB65 has officially declared cyber war on Russia, as well. You want to invade Ukraine? Good. Face resistance from the entire world. #UkraineWar All of us are watching. All of us are fighting."

And also, as of February 28th, another group under the Anonymous umbrella named DeepNetAnon has joined in the operations against Russia by attacking and intercepting Russian radio receivers. The group tweeted: "The Russians have now taken offline the second web server hosting a Software-Defined Radio receiver, used to intercept with radio frequencies. Too bad there's many more sites we can use."

The collective also announced that they have successfully hacked the Ministry of Economic Development of Russia. The group 1LevelCrew also showed their support for Ukraine and tweeted, "TANGO DOWN," and then a URL, http://pfr.gov.ru. And that was actually one of the targets that the IT Army had been assigned. That's the Pension Fund of Russia, which they tweeted as a result of this TANGO DOWN is offline. Another collective known as HydraUG made a clear statement via Twitter, saying: "I'm not here to deface/destroy your website, I'm here to liberate Ukraine."

As of last Wednesday, another affiliate named N3UR0515, maybe that's neuro, probably neuro something or other, took to Twitter to declare support and call on YouTube to take down Russian propaganda. We'll be talking a little bit later about Google's moves along those lines. The group has administered DDoS attacks and taken down RIA.ru, the official Russian information website. Joining the Anonymous collective, VogelSec announced that they had hacked into the Russian Space Research Institute database and leaked files from Roscosmos, though the hack has not yet been confirmed.

Ghostsec announced their support for Ukraine, saying: "In support of the people in Ukraine, we stand by you." Also known as Ghost Security, the group considers itself a vigilante group and was initially formed to target ISIS websites that preach Islamic extremism. Ghostsec is also commonly referred to as an offshoot of Anonymous.

Then we have AgainstTheWest (ATW). They, while they're against the West, are standing with Ukraine. The group's Twitter account says: "We are back in action, standing against Russia, active until Russia stands down." The group's actively working to breach Russian infrastructure, including Russian railways and Russian government contractor promen48.ru. On March 1st the group issued a new statement for further clarification. Actually it's a little waffling.

They said: "We won't be collaborating with Anonymous. ATW - remember, that's Against The West - will be splitting into two groups, one for Russia-related breaches, one for Chinese-related," the group stated. ATW accused Anonymous of taking the credit for the work they had done, saying: "Anonymous has had a lot of media publicity over the years for hacking; and to see this, it didn't sit right," referring to some credit that Anonymous took. They said: "ATW appears to have been suspended from Twitter as of last Thursday, March 3rd." So again, like I said, this stuff is not all legal, folks.

SHDWSec joins the movement to support Ukraine. The group is working in collaboration with ATW and Anonymous in operations against Russia. And they tweeted: "SHDWSec joined forces with AgainstTheWest. First stage is now on the roll. Expecting us is too late. Brace for impact. More to come."

Leo: Oh, lord. These are 12 year olds. Come on.

Steve: I think a lot of that, yes, you're right. Some of these guys it's clear are that. I'll skip over some of these. We have the Belarusian Cyber Partisans supporting Ukraine. We have KelvinSecurity announcing they stand with Ukraine. Raidforums2 also stands with Ukraine. The group announced: "Raidforums2 is in support of Ukraine. Members are actively DDOSing Russian websites and attacking Russian infrastructure. We also have reason to believe the Chinese are hacking Ukrainian networks," though they didn't support that accusation. "Previously labeled as only Raidforum, the collective is now operating as Raidforums2 after having outage and access issues." Yeah. Maybe a counterattack. It's unclear what went wrong with the original Raidforum.

However, ContiLeaks is significant. Definitely not Conti. We'll get to them a little bit more in a minute. But they also back Ukraine. The group has exposed the infamous ransomware group Conti from the inside out. Following February 27th, Conti's statement of full Russian support, an account named ContiLeaks leaked hundreds of files containing internal Conti communications. The informant is believed to be Ukrainian and has continued to leak more and more files as days have gone by. More recent data shows communication depicting the chaos within Conti where, for example, one person says: "Hi, all VM farms are cleared and deleted, servers are disabled." And then somebody responds: "I deleted all the farms with the shredder and shut down the servers." So hacker speak.

Okay. So and of course we also have Conti, which is in full support of Russia. Emsisoft's ransomware expert Brett Callow shared a tweet from the Conti gang. They said: "If anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use all our possible resources to strike back at the critical infrastructures of an enemy." And of course, as we know, the Conti ransomware gang is certainly one to be reckoned with. They are very sophisticated and known for being the first group to weaponize the Log4Shell vulnerability and operate a fully deployed attack chain.

But it appears that not everyone within Conti shared the group's loyalty to Mother Russia. As I mentioned, this what was their name, ContiLeaks, ContiLeaks group leaked 400 files of internal communications between members of the group. The leaked messages go back more than a year to January of 2021. The data was shared with the malware research group VX-Underground, who have since posted an archive of all the leaked data on their site. I have a link to it in the show notes, after having taken a look at it last evening, and I tweeted the link because I thought it might be of interest to some of our listeners. It looks like a legitimate source of Conti-leaked information, though obviously treat it with skepticism.

There is, oh, and this is one that The Record had referred to, a Minsk-based group, UNC1151, in support of Russia. They're believed to be a state-sponsored by Belarus group, and they've already been working to compromise the email accounts of Ukraine military personnel. The group's members are officers of the Ministry of Defense of the Republic of Belarus. Facebook has taken down accounts used by UNC1151 which targeted Ukrainian officials through Facebook posts that displayed videos depicting Ukrainian soldiers as weak. Facebook also blocked various phishing domains that were being used to jeopardize Ukrainian accounts.

We also have Zatoichi is supporting Russia through the spread of disinformation via the group's Twitter account. Among many of their claims, the account stated: "Killnet has already taken down the Anonymous website, which announced the start of a cyber war with the Russian government, as well as the Right Sector website, and the website of the President of Ukraine." And again, that's not true. And speaking of Killnet, they also clearly stand with Russia. The group published a video addressing the people of Russia, encouraging them to never doubt their country. The video features a hooded figure with a distorted voice claiming to have taken down the website belonging to Anonymous. Again, it's not down. Little is known about the group, and it's unclear as to whether the group existed previously.

There's also, and I'll skip details of the rest of these since it goes on and on: XakNet backing Russia, the Stormous Ransomware collective standing with Russia, Digital Cobra Gang. FreeCivilian united with Russia. Sandworm, that is a serious group. The group known for its recent malware called Cyclops Blink is comprised of Russia state-sponsored hackers. They've been around for a while - we've spoken of Sandworm on the podcast before - and have malware which targets WatchGuard Firebox firewalls.

We've got the Red Bandits, a cute name, and the CoomingProject. An international hacker group announced in a statement: "Hello, everyone. This is a message we will help the Russian government if cyberattacks and conduct against Russia." So broken English. They're linked to the 2021 data breach and leak of the South African National Space Agency. So all this going on with the groups declaring for and against, and it does seem clear, if we are to believe the tweets of those who have said they are going to attack Russia and then providing details that there is a lot of activity aimed in that direction.

Starlink. We know what Starlink is. It's Elon Musk's low Earth orbit satellite technology. I've got one very good friend, Mark Thompson, who's in an area in Phoenix where, believe or not, he doesn't have any broadband Internet service. And he's hoping that this is all going to work out well.

This Ukraine Minister of Digital Transformation, I think he's 31 years old, he looks young, Mykhailo Fedorov. On the 26th he tweeted to @elonmusk. He said: "@elonmusk While you try to colonize Mars, Russia tries to occupy Ukraine. While your rockets successfully land from space, Russian rockets attack Ukrainian civil people. We ask you to provide Ukraine with Starlink stations and to address sane Russians to stand." To his credit, Elon replied: "Starlink service is now active in Ukraine." It hadn't been a day before. And, he said: "More terminals en route."

Okay. Although so far Ukraine's Internet access has been relatively stable, and it's actually been surprising people, concerns over the possibility of widespread outages, as Russia has been increasingly attacking communications infrastructure, have recently increased. So it was with some sense of relief that an equipment truck arrived from Starlink, like that day, which of course is the Internet subsidiary of Elon Musk's SpaceX.

So will it be helpful? Was it another PR stunt for which of course Elon is rather famous? It's too soon to say. But it would take more trucks, many more trucks, in order to make a significant difference. According to Ukraine's Ministry of Digital Transformation, only one truck of Starlink kits has arrived so far. The Ministry is raising funds to purchase additional Starlink equipment, according to Forbes Ukraine. Ukraine is also considering the purchase of used Starlink devices, if they can get them. According to Business Insider, a standard Starlink kit costs $500, with a subscription to the network costing $99, presumably that's per month.

Anyway, so the system appears to be helping some Ukrainians to stay connected. The general stability of the Ukrainian Internet service should, and in general has been, allowing Ukraine's president and other citizens to stay in contact with the outside world and keep everyone updated about what's going on. But Internet connectivity has been affected in the south and eastern regions of the country where the fighting has been the heaviest. Ukrainian officials stated that Russia would not be able to switch off Internet access easily for the entire country.

And it turns out that Ukraine's multiple land fiber connections which come in from the West makes it more difficult to take Ukraine off the 'Net as a whole. So they've been able to stay online so far. Still, many Ukrainians fear that they would be cut off from the world if Russian troops were to destroy the critical infrastructure responsible for television and the Internet. We had an Internet outage briefly yesterday, and it is amazing how much we've come to be dependent and to take for granted the connectivity that we have with the world.

Control of the Internet and telephone communications is obviously of immensely important strategic value. Ukraine has limited the Russian troops' access to networks by having its phone carriers Kyivstar, Vodafone, and Lifecell shut down network access to phones from Russia and Belarus. So troops from those countries will be unable to send messages and spread false information via phone calls. And obviously just thwarting your enemy's communications is good policy.

And interestingly, Elon had apparently been having trouble obtaining a license until now to activate Starlink in Ukraine. One can imagine the political pushback from the existing carriers who were in no hurry to increase their competition from above. But no one batted an eye when Elon said: "Give me permission to turn it on, and I will." They did; he did. And afterwards a Ukrainian engineer, Oleg Kutkov, said in an interview with The Verge that his Starlink dish got a signal from one of SpaceX's satellites in just 10 seconds. He told The Verge: "I honestly didn't believe it would work."

So it certainly is the case that satellites are going to be, unless you shoot them out of orbit, are going to be impossible to cut off. Well, I guess you could jam the signal, except they can also be targeted. So that is, you know, line of sight connections to the dish. So it might be the jamming is also much more difficult to do.

On their side, Russia has blocked access to Facebook, Twitter, and foreign news outlets. This would be the "two can play that game" line. They blocked access to Facebook after Meta deactivated or restricted access to accounts belonging to pro-Kremlin media outlets and news agencies, including that RIA - the main Russia media outlet - Novosti, also Sputnik and Russia Today. And our favorite Russian agency, Roskomnadzor, told Interfax that Russia has now also blocked access to Twitter following a demand made by the Prosecutor General's Office. I had read that that happened last Friday.

On Thursday, Roskomnadzor asked Meta to immediately lift all restrictions on Russian media outlets, that is, the members of the RT Media Group. Roskomnadzor said Friday that the decision was motivated, that is, their decision to disconnect, by Facebook discriminating against Russian media and information resources starting in October of 2020, so quite some time ago. Roskomnadzor stated: "On March 4, a decision was made to block access to the Facebook network within the Russian Federation." Although notably some other properties, Instagram and WhatsApp, have as far as I know still not yet been blocked, only Facebook.

And also last Friday, Roskomnadzor blocked access to multiple foreign news outlets, some of them designated as foreign agents, including Voice of America, the BBC, DW, and Radio Free Europe and Radio Liberty. Not that they had to, but Russia justified the media outlets' ban saying that they spread fake news regarding the ongoing invasion of Ukraine, the methods used by its military against Ukrainian citizens and infrastructure, and the number of casualties suffered by the Russian army. We in the West have seen a great deal of coverage, and I'm unsurprised that Russia would not want all Russians to see what we see here going on.

Google was also asked on Thursday to stop advertising campaigns spreading what Roskomnadzor called "misinformation" on YouTube videos about the Russian invasion of Ukraine. Roskomnadzor said that online ads with no age labels and inaccurate content are being used to instill "protest moods" and spread false info on the Russian "special operation," as they're calling it, in Ukraine.

And YouTube has become quite important. As I was putting this together, I hadn't get gotten to a chart that I saw indicating that it is the number one social media outlet used in Russia. It's, like, way above everything else. So Roskomnadzor sent a letter to Google LLC demanding that Google immediately stop disseminating false information of a political nature about the special operation of the Russian Armed Forces in Ukraine on the territory of Russia. Well, of course, that's rich.

Roskomnadzor's demand continued, saying: "Such advertising messages are shown to the Russian users of the video hosting site YouTube and contain misinformation aimed at forming a distorted perception of the events taking place and creating protest sentiments among the Russian Internet audience. The agency considers it unacceptable to use YouTube in the information war against Russia, including using the advertising capabilities of the platform." And I'll just give everybody a hint. This is all building towards a conclusion that we'll be getting to here at the end of the podcast. Which is, you know, ultimately what Russia's probably going to have to do.

Roskomnadzor also notified all independent Russia media outlets not to spread false information, that is, the media outlets inside Russia that are independent, not to spread false information about the shelling of Ukrainian cities, as well calling the "ongoing operation" an attack, invasion, or a declaration of war. And I'm sure everyone has probably heard by now, Russia is also planning to introduce a new law that would punish the spreading of what they consider to be fake news about the Russian armed forces' military operations in Ukraine with up to 15 years in prison.

For their part, Google has already taken action to stop actual misinformation, taking down disinformation campaigns regarding Russia's invasion, and blocked YouTube channels belonging to Russia Today and Sputnik across Europe at the request of European Union authorities. Roskomnadzor protested YouTube's decision, as we said, demanding the immediate removal of all access restrictions to the official accounts of Russian media, including RT and Sputnik, in Europe.

Previously, Google demonized Russian state-funded media across all its platforms - I don't mean demonized, I'm sorry, demonetized. Google demonetized Russian state-funded media across all its platforms to block Russian state-funded media from running ad campaigns. And YouTube has removed hundreds of channels with thousands of videos which violate its Community Guidelines, including channels engaging in "coordinated deceptive practices," as Google labeled them.

Google said: "When people around the world search for topics related to the war in Ukraine on Search or YouTube, our systems prominently surface information, videos, and other key context from authoritative news sources." So for the time being, Google said that most of its services, including Search, YouTube, and Maps, remain available in Russia to provide Russians with access to global information and perspective.

So overall the situation appears to be developing as we would have expected it to. The providers of the content hold the cards. They, and they alone, are able to decide which content their platforms serve up and which they block and delete. The only power a local authoritarian government has is to choose to block everything from a provider.

Also, Google has been even more proactive on the security front. They announced last Tuesday that they were focusing upon increasing security measures to help protect Ukrainian civilians and websites, which other U.S. technology providers, like Meta, you know, Facebook, had also been doing. Meta has been actively working to disrupt the flow of disinformation in the region and take down accounts that targeted Ukrainian officials with phishing attempts.

But as for Google, in a statement by Kent Walker, their President of Global Affairs, Google said the measures include SOS alerts on its Search function, automated detection and blocking of suspicious activity, Gmail notifications of government-backed attack warnings, increased authentication challenges, and the expansion of its Advanced Protection and Project Shield programs. In other words, rapid and strengthening of Google's authentication.

As for Search and Maps functions, the company has disabled various live Google Maps features within Ukraine, such as traffic information, to prevent public access to population densities within different areas. The company also issued SOS alerts that will guide users to United Nations resources for refugees and asylum seekers when they search for refugee and evacuation instructions. So they've been more carefully curating their search engine results during all of this. And they've reportedly expanded security protections after its Threat Analysis Group - remember the TAG team, T-A-G - reported an increased focus from threat actors on Ukrainian targets. They've blocked attempted attacks "without any compromise," they said, "of Google accounts as a result of the campaign."

They increased the frequency of authentication challenges for Ukrainian civilians and are relying on their Advanced Protection Program to safeguard hundreds of high-risk accounts in the region. A campaign known as Project Shield is also being used to help protect over 100 websites belonging to news publications, human rights groups, political organizations, and other groups that are targeted by distributed denial-of-service attacks. So they're also stepping up and strengthening the sites that they're responsible for against DDoS.

And following the statement issued by Google last Tuesday, Apple announced, as we've probably heard, that they had ceased all sales of their technology in Russian online stores after Ukraine's Prime Minister pleaded with them to shut down the app store and halt all Russian sales, which they've done. Microsoft also recently, I think it was on Friday, said that they are suspending all of the sales and support inside Russia's borders.

A domain registrar, Namecheap, that I've heard of in passing, eight days ago they - they're Phoenix-based, you know, Phoenix, Arizona-based, founded 22 years ago, so they've been around for a while, in the year 2000, now operating in 18 countries with 1,700 employees and managing 14 million domains. They sent an email that I guess I feel of mixed mind about. This went out eight days ago to all of their registrants, their customers, their domain name customers, located in Russia.

They said: "Unfortunately, due to the Russian regime's war crimes and human rights violations in Ukraine, we will no longer be providing services to users registered in Russia. While we sympathize that this war may not affect your" - may not affect, that's what they said - "affect your own views or opinion on the matter, the fact is your authoritarian government is committing human rights abuses and engaging in war crimes. So this is a policy decision we have made and will stand by. If you hold any top-level domains with us, we ask that you transfer them to another provider by March 6" - two days ago - "2022." Okay, so that was a seven-day, a one-week notice of unilateral service cancellation.

Their note continues briefly: "Additionally, and with immediate effect, you will no longer be able to use Namecheap Hosting, EasyWP, and Private Email with a domain provided by another registrar in Russian top-level domains. All websites will resolve to 403 Forbidden. However, you can contact us to assist you with your transfer to another provider."

And predictably, this email generated some angry pushback from Russians, to which Namecheap's CEO replied over on Ycombinator. He said: "We haven't blocked the domains. We are asking people to move. There are plenty of other choices out there when it comes to infrastructure services, so this isn't deplatforming. I sympathize with people who are not pro-regime, but ultimately even those tax dollars they may generate go to the regime. We have people on the ground in Ukraine being bombarded now nonstop." He says: "I cannot with good conscience continue to support the Russian regime in any way, shape or form. People that are getting angry need to point that at the cause, their own government. If more grace time is necessary for some to move, we will provide it. Free speech is one thing, but this decision is more about a government that is committing war crimes against innocent people that we want nothing to do with."

Now, I'll just note that expecting anyone in Russia to successfully move their domain at this moment with banks closed, Visa, MasterCard, and PayPal all having suspended service, and the value of the Russian ruble having collapsed, is totally infeasible. So in practice this really doesn't represent, I mean, it does represent effective abandonment.

And as I said, I feel a little queasy about that. It seems to me that individual Russian citizens, small businesses, charitable organizations, et cetera, ought to have the West standing with them to help them survive this period, rather than abandoning them in their time of what could be great need. All indications are that Russian citizenry is quite divided in their feelings about the actions of their own regime, to the degree that they know what's going on. You know, being politically aware in the U.S., we certainly understand the nature of division. There are many topics of discussion which are now off limits between my own much beloved family members. So we, too, are a divided nation.

But when Namecheap took their Russian customers' money, they didn't ask about their political sentiments. They took their money in return for a promise to provide service for some period of time. Commitments are not subject to reconsideration. That's what makes them a commitment. I would have no problem if Namecheap were to announce that they would be suspending the renewal of domains at their expiration, so giving their Russian customers fair notice of the need to find another service at that time. I don't see Namecheap offering to refund their customers' money in U.S. dollars, which are now quite valuable at the current dollars-to-rubles exchange rate. But even doing that would still have left those customers stranded. So I don't know. To me, that seems like a hard-to-defend breach of commitment.

Two days after that, they posted: "Effective immediately, we will begin offering free anonymous hosting and domain name registration to any anti-Putin, anti-regime, and protest websites for anyone located within Russia and Belarus. Please contact our support for details." And since this announcement followed two days after their Russia abandonment email, doing a little reading between the lines, I wouldn't be surprised if this was their way of selectively backpedaling and arranging to continue offering some services and hosting, but only to those entities whose politics they're aligned with. So anyway, even DNS providers are getting in on all of this.

Leo: And now Steve will talk about Telegram.

Steve: So we've talked about Telegram, you and I, Leo, for the past nine years, ever since it first appeared in 2013. And as our listeners know, despite its popularity, I've always looked askance at it since for reasons I will never understand, its authors unnecessarily violated the cardinal rule of cryptography. They rolled their own, unlike the many other properly designed alternatives such as Signal and Threema, just to name two. And offering a bounty for someone who cracks their crypto is not the same as designing it properly. For all we know, it has been cracked by someone like the NSA. And the knowledge they have and the access this provides is worth far more to them than Telegram's bounty. They would want things to remain just the way they are, with Telegram being unexamined, apparently unbroken, but certainly not fixed.

So in any event, I mean, it is - I remember when I first rolled up my sleeves and looked at it, it was just the screwiest random pile of crypto primitives anyone had ever seen. And it's been described the same way, not just by me, but by other crypto experts who are like, what? But anyway. As far as this goes, no one could care less what I think. Telegram is super popular, and its popularity has recently exploded during this horrific Russia-Ukraine mess.

As we've followed Roskomnadzor's and the Russian Federal Security Service's (the FSB's) ultimately futile efforts through the years to shut down and block Telegram, we saw them finally give up a couple years ago. They just, you know, Telegram just kept dodging and weaving and refused to be taken offline, and they've survived. The risk intelligence company, Flashpoint, noted in a recent report that six out of 10 Russians use Telegram precisely because their country's authorities are unable to impose any oversight on the platform.

So it should also be no surprise that Telegram's messaging has taken a pivotal role in the ongoing conflict between Russia and Ukraine and is being widely used by both hacktivists and cybercriminals. According to a report from Checkpoint, the number of Telegram groups has increased six-fold since February 24th. And some of them, dedicated to certain topics, have exploded in size, in some cases counting more than a quarter million members.

Three categories which have rapidly gained in popularity as a direct result of the Russian invasion of Ukraine are, first, volunteer hackers engaging in DDoS and other kinds of cyberattacks against Russian entities. Second, fundraising groups - whoops - that accept cryptocurrency donations, allegedly for Ukrainian support. And, third, various "news feeds," and you've got to put that in air quotes, too, because just citizens aiming their smartphone somewhere that promise to offer reliable reports from the frontline.

We've already talked about the group that stands out among those that lead the anti-Russia cyberwarfare operations, the so-called IT Army of Ukraine, whose membership is now at, okay, and remember at the beginning of the podcast I said 175,000? I got an updated number. We're now at 269,972.

Leo: Wow. Wow.

Steve: So just shy of 270,000 subscribers are like members of this IT Army of Ukraine. I would not want to have all those people, like, you know, empowered to do what dastardly thing they can. That would be daunting. In addition to targeting, orchestrating, and launching DDoS attacks against key Russian sites, the group exposes the personal details of opinion-makers in Russia and other people who play a significant role in the conflict. So, yeah, again, I wouldn't want that aimed at me. As for the "fund-raising groups," that's in air quotes because, naturally and unfortunately, the majority of the self-declared "donation support" groups in Telegram are scams, as they're going to be, that take advantage of sentiments to relieve people of their money.

And then there's the "news," also in air quotes. Checkpoint's coverage of Telegram notes, they said: "In the era of social media, traditional news channels are merely a sideshow for numerous newsfeed Telegram groups. These groups on Telegram report unedited, non-censored feeds from war zones 24 hours a day, including footage that traditional mainstream media often refrained from airing live." I can imagine. "In fact," they said, "about 71% of the groups we see are dedicated to news around the current conflict." So just shy of three quarters of Telegram groups are about providing news.

"Checkpoint researchers," they said, "observed such groups appearing rapidly from the beginning of the conflict and have continued to grow since then. In such groups, the quality of newsfeeds is not a factor, and users often leverage this to spread 'news' and 'facts' that are not verified or checked. This is a form of psychological weapon, used to demoralize and influence morale.

"So the bottom line is to be skeptical, use your own judgment, and guard against becoming seduced by anyone's narrative that seems too good to be true. It may indeed be too good to be true." Or, you know, too horrific to be true. And in fact Michael Horowitz, a geopolitical and security analyst who's the head of intelligence for the firm Le Beck International, recently tweeted. He said: "I have deleted footage of a plane being shot down above Kharkiv as it seems to be from a video game." He said: "That's a very realistic one. Sorry for the mistake." So, yeah, be careful what you think of as real.

As I mentioned before, Microsoft has also shut down in Russia. There were some interesting tidbits in what their Chairman and President Brad Smith posted under the title "Microsoft suspends new sales in Russia." He said: "Like the rest of the world, we are horrified, angered, and saddened by the images and news coming from the war in Ukraine and condemn this unjustified, unprovoked, and unlawful invasion by Russia. I want to use this blog" - I'm just going to share the top of it - "to provide an update on Microsoft's actions, building on the blog we shared earlier this week."

He said: "We are announcing today that we will suspend all new sales of Microsoft products and services in Russia. In addition, we are coordinating closely and working in lockstep with the governments of the United States, the European Union, and the United Kingdom. And we're stopping many aspects of our business in Russia in compliance with governmental sanctions decisions. We believe we are most effective in aiding Ukraine when we take concrete steps in coordination with the decisions being made by these governments, and we will take additional steps as this situation continues to evolve.

"Our single most impactful area of work almost certainly is the protection of Ukraine's cybersecurity. We continue to work proactively to help cybersecurity officials in Ukraine defend against Russian attacks, including most recently a cyberattack against a major Ukrainian broadcaster. Since the war began, we have acted against Russian positioning, destructive or disruptive measures against more than 20 Ukrainian government, IT, and financial sector organizations. We've also acted against cyberattacks targeting several additional civilian sites. We have publicly raised our concerns that these attacks against civilians violate the Geneva Convention." So Microsoft, too, in addition to a growing list. And actually I have a brief list in a minute.

Coinbase. Last Sunday the 6th, Paul Grewal, the Chief Legal Officer for Coinbase, announced the employment of crypto tech to promote sanctions compliance. They announced that they are actively blocking access to more than 25,000 blockchain addresses in other words, wallets linked to Russian individuals and entities. And Coinbase shared all of the blocked addresses with the U.S. government in order to further support sanctions enforcement. So they used their blockchain analytics in order to say here's the people; here's the wallets that we've seen them link to.

Coinbase will also be blocking sanctioned entities from opening new accounts and actively detecting attempts to evade the ban. The ban addresses sanction lists maintained by countries worldwide, including the United States, United Kingdom, European Union, United Nations, Singapore, Canada, and Japan.

Citing an example, Paul wrote: "For example, when the United States sanctioned a Russian national in 2020, it specifically listed three associated blockchain addresses. Through advanced blockchain analysis, we proactively identified over 1,200 additional addresses potentially associated with the sanctioned individual." Okay, now, I'll just stop and say, wait a minute. What do you want to bet that's a ransomware entity? Because they're saying it sounds like the U.S. had three blockchain addresses. These guys dug in and found everything that those three were connected to.

The fact that it exploded into 1,200 additional addresses, that sure feels to me like somebody who was doing a lot of monetary movement through various chains. Anyway, "1,200 additional addresses potentially associated with a sanctioned individual, which we added to our internal block list. Today, Coinbase blocks over 25,000 addresses related to

Russian individuals or entities we believe to be engaged in illicit activity, many of which," he said, "we have identified through our own proactive investigations."

Now, two weeks ago, on the 27th of February, our friend in Ukraine, Mykhailo Fedorov, asked for more than the crypto exchanges were willing to do. He tweeted: "I'm asking all major crypto exchanges to block addresses of Russian users. It's crucial," he tweeted, "to freeze not only the addresses linked to Russian and Belarusian politicians, but also to sabotage ordinary users."

But Coinbase and the other crypto exchanges, including Binance, refused to freeze all Russian users' accounts. Their various spokespeople added that, while they will not block all Russian accounts on their platforms, the crypto exchanges will take steps to identify all sanctioned entities and individuals and block those accounts and transactions. Coinbase cited the "economic freedom in the world." And Binance said it was about the "greater financial freedom for people across the globe." And banning users' access to their cryptocurrency, Binance said, "would fly in the face of the reason why crypto exists in the first place." So cryptocurrencies are also involved.

Now, naturally, Russia has not been doing nothing. Last Thursday, amid the continually escalating Russian attack on Ukraine, Russia's NCCCI, their National Coordination Center for Computer Incidents, published a list, presumably intended to be used by those sympathetic to President Putin's expansionist agenda for retaliation against these claimed attacks on Russian cyber infrastructure. And I say "claimed attacks" because, in addition to the massive list containing 17,576 individual IP addresses were 166 domains that the NCCCI said were behind a series of DDoS attacks aimed at its domestic infrastructure.

So in other words, Russia is saying we want anybody who is pro-Russia to go on the cyber offensive and attack all these. Among the domains were the U.S. Federal Bureau of Investigation, the Central Intelligence Agency, and websites of several media publications including USA Today and Ukraine's Korrespondent magazine. So it appears that not liking someone is enough to get them on the list. I doubt that USA Today was DDoSing Russia.

But anyway, not surprisingly, the NCCCI is reacting to the gradual and incremental, but also probably inevitable withdrawal of Western and non-Russian cyber services from Russia. As part of its recommendations to counter the DDoS attacks, the agency is urging organizations to "ringfence" network devices, whatever that is; enable logging and changing passwords; enforce data backups; and be extra alert for phishing attacks. In other words, the standard things you would do to better raise and defend yourself against cyberattack. But the coolest advice from NCCCI caught me a bit by surprise at first. But then I thought it was really interesting and obvious in retrospect. The NCCCI advised its citizenry and Russian enterprises to turn off automatic software updates and disable third-party plugins on websites.

Now, at this point Microsoft has pulled the plug on Russian revenue, but the U.S. is not at war with Russia. And of course we're being very careful not to be at war with Russia. However, wow. Consider the implications of Microsoft's - and I'm not suggesting this has ever happened or ever would - but the implications of Microsoft's deliberate sabotage of Windows security in aid of a war effort against Russia. I would not want to be on their side, on the other side of that.

And I have to say this puts a spin I had never considered on my rooting for having all of our devices phoning home and auto-updating all the time. You know, we don't want to go to war with China, either. We could easily be on the receiving end with all of the IoT gadgets that most of us are now using. This is all quite sobering. It's one thing to have an inadvertent security mistake be patched. It's another thing to have a deliberate attack launched as a consequence of auto update, which has just loaded a bunch of stuff there, who knows, into one's computer. And I know I was slow to buy into this whole cyberwar idea. So I suspect I'm still probably being a little naive.

The NCCCI also advised its citizenry to "Use Russian DNS servers. Use the corporate DNS servers and/or the DNS servers of your telecom operator," they said, "in order to prevent the organization's users from being redirected to malicious resources or other malicious activity." In other words, they're battening down the hatches. They said: "If your organization's DNS zone is serviced by a foreign telecom operator, transfer it to the information space of the Russian Federation."

And there again, Russian devices are necessarily trusting the certificates issued by Western certificate authorities, since the websites and services that Russians depend upon are serving Western certificates. Just think for a minute how much implicit cross-border trust there is in today's globally interconnected world. This has been the background thought I've had all throughout this mounting aggression. It's really no longer in any way practical for any single country to completely isolate itself from the rest of the world. There's just too much true interdependence, and there is implicit trust that comes with that interdependence.

And speaking of interdependence, according to the global Internet access watchdog NetBlocks, Russia has placed extensive restrictions on Facebook access within the country. We talked about that before. And late last week there were reports that Twitter had also become unavailable. Again, Twitter wasn't doing what Roskomnadzor had asked, so no Twitter for you, Russians. Ukraine has also updated its list of targets for its volunteer IT Army of civilian hackers. Now on the list are the Belarusian railway network, Russia's homegrown satellite-based global navigation system GLONASS, and telecom operators MTS and Beeline.

And in another shoe dropping, Russia authorities are drafting a set of measures to support the country's economy against the pressure of foreign sanctions, which they're certainly feeling. And as part of this, the proposal, which is in the process of being finalized, would eliminate intellectual property right limitations in order to explicitly permit piracy within Russia.

The plan is to establish a unilateral software licensing mechanism that would renew expired licenses - and this is all euphemisms - without requiring the consent of the copyright or patent owner. This new process will be available in cases where the copyright holder is from a country that has supported sanctions against Russia for products without Russian alternatives, which of course are many, if not most. The move is Russia's response to numerous software vendors exiting the Russian market and suspending new license sales, including Microsoft, Cisco, Oracle, NVIDIA, IBM, Intel, and AMD. In other words, okay, you don't have to honor those licenses any longer, says Russia.

The original Article 1360 of the Civil Code of the Russian Federation says that, in the original one: "In the interests of national security, the government of the Russian Federation shall have the right to permit the use of an invention, utility model, or industrial design without the consent of the patent holder provided that he is notified as soon as possible and payment to him a reasonable remuneration." Now, however, in multiple proposed amendments to this Russian Civil Code, the Russian Ministry of Digital Transformation wants to bypass compensation to license holders who are under sanction restrictions so that they can continue using the software.

Translated proposed amendments read: "Amending Article 1360 of the Civil Code of the Russian Federation regarding the use of a license and other types of rights and the abolition of compensation to foreign companies originating from states that have acceded to the sanctions Federal Law." Now, of course, software products that rely on cloud services or online verification, as so many do now, will stop working since no unilateral change in Russia's international intellectual property treaties will keep online services from being shut down. But this does feel as though Russia will be entering a bit of a dark age, depending upon how long this goes on. Who would want to sell to a rogue nation, even if sanctions were not in place?

And so this brings us to the big question. Will Russia disconnect? Are we about to see Russia flip the switch? It feels like we are. Although Roskomnadzor has been working overtime to censor information by blocking its citizens' access to Western media, services such as Telegram have withstood all previous blocking attempts. And YouTube, as I said, remains the number one most popular service in all of Russia. Google is refusing to comply with Roskomnadzor's censorship attempts and demands, while simultaneously blocking Russia's own state-sponsored propaganda from being carried by YouTube. So it may be that nothing short of disconnecting all of Russia from the rest of the Internet will be the only solution that they believe is workable. And given the things we've seen, these comments about using your local Russian-based DNS, and if your DNS is coming from outside of Russia switch to inside, this all feels like a preamble.

We've previously talked about the RuNet, Russia's sovereign Internet, which has been in development, we've been talking about it as it's come up from time to time for years, and remember was successfully tested for actual deployment with the collaboration of their largest Internet providers in Russia last summer. It worked. Remember when we discussed the need for and their establishment of an entirely autonomous DNS system. In other words, they needed to replace the global root servers in order for their system to continue working as DNS caches expired.

Well, this past Sunday afternoon, two days ago, a letter allegedly leaked from the Deputy Minister of Digital Marketing and Mass Communications of the Russian Federation was posted by Anonymous on Twitter. Since it's written in Russian, of course, I cannot read what it says. But Anonymous claims that it provides instructions to all organizations about how to prepare for connection to the RuNet and disconnection from the Internet. Anonymous's tweet says: "Russia is preparing to disconnect from the global Internet, limiting access to information for the Russian people. That means censorship, and we [Anonymous] are totally against censorship of any kind. So let's turn up the pressure!" And then in the show notes I have a link to their tweet which does show a picture of this two-page document written in Russian.

It would seem to me that I don't know what "turning up the pressure" means, but it would only hasten the pulling of the plug. Russia doesn't have, and must import, Western technology. They cannot duplicate our semiconductors. But unfortunately they may have reason to count on China as a strategic partner. China really is the wildcard in much of this. But China is not the West and cannot replace much of what only Europe, the U.S., the U.K., and others provide. So we are living in interesting times, and we might be on the precipice of having Russia disconnect itself from the Internet in order to once and for all isolate its citizens from what's going on. Wow.

Leo: And there you have it, Security Now! for another exciting week, thrilling, gripping edition. Steve is available at GRC.com. That's where you'll find his SpinRite, world's best mass storage maintenance and recovery utility. Currently 6.0; 6.1 is coming. You can buy 6.0 now, get 6.1 for free when it's available and participate in its development. That's at GRC.com.

While you're there you can pick up a copy of the show. He has two unique formats, the 16Kb audio for the bandwidth impaired. I always, for some reason I imagine somebody in the Australian Outback who's on some sort of weird satellite connection.

Steve: Well, of course it started with Elaine; right?

Leo: She didn't want a big audio file, yeah.

Steve: She was satellite because she's out in the boonies somewhere.

Leo: Right, right.

Steve: And she said, this is a big file, Steve. I said, oh, I'll fix that.

Leo: So she takes it, she transcribes it, and that's the other unique format, the human-written transcriptions from Elaine Farris, which makes it a great, you know, read along while you listen or search for a part of the show. Or just, you know, have a text version of Security Now!, including all the ums and uhs and pauses. GRC.com. We have everything at our website, too, TWiT.tv/sn. There's audio there. There's video there. You could subscribe in your favorite podcast client. There's an audio stream, a dedicated video channel, I should say, at YouTube. Lots of ways to consume it.

In fact, you can even watch us do it live, which we do every Tuesday at about 1:30 Pacific, 4:30 Eastern, 21:30 UTC at live.twit.tv. There's audio and video streams there. You can chat with us at irc.twit.tv. Club TWiT members can chat inside the Discord. There's always something going on in that Discord, including some really cool, unique shows like our untitled Linux show. I guess that's it. That's all the business. Thank you, Steve. Great job. See you next week.

Steve: Well, that's the news from there. Hopefully nothing catastrophic will happen in cyber world. If it does, we'll talk about it next week. But there were other things to talk about which we'll get to next week for sure.

Leo: Yes. Thank you, Steve. We'll see you all next time on Security Now!.

Steve: Bye-bye.