THE BROOKINGS INSTITUTION

THE CURRENT: How is Russia conducting cyber and information warfare in Ukraine?

Thursday, March 3, 2022

PITA: You’re listening to The Current, part of the Brookings Podcast Network. I’m your host, Adrianna Pita.

As Russian ground forces advance in Ukraine, Ukrainians are sheltering from artillery shells and cruise missiles and subways and bomb shelters. But in addition to the conventional military forces that Russia brings to bear, their security and intelligence services are also well-known for their cyber capabilities – the ability to hack into computer systems to steal or destroy information or shut systems down, among other effects.

So here to talk to us about what we’ve seen so far in the way of cyberattacks and information warfare in the war in Ukraine is Jessica Brandt, a fellow and policy director in the Artificial Intelligence and Emerging Technologies initiative here at Brookings. Jessica, thanks so much for talking to us today.

BRANDT: Thanks for having me.

PITA: So we've been hearing for years about how vulnerable some of the most basic systems to our daily lives are, how vulnerable these systems are to cyberattacks, both in this country and elsewhere around the world: everything from the electrical grids, to water sanitation and filtration systems, and, of course, the internet and telecommunications systems. However, just this Tuesday we saw one of the main TV towers in Kyiv be hit in a military strike, but so far there's been no major infrastructure or communications cyberattacks that we've seen in Ukraine. What kind of cyber activity have we seen Russia use against Ukraine so far in this war?

BRANDT: Very little and that's been a surprise. I'd say many of the cyberattacks that have been directed at Ukraine in the past month have been relatively basic DDOS or distributed denial of service attacks. What we've seen hackers bombard Ukrainian government websites with so much traffic that servers are forced offline for a period of time. And these kinds of attacks, they're effective for short term disruption, but they're not really like new or impressive cyber capabilities.

Maybe a little more worrying is that in recent days, you know Russia deployed wiper malware to delete data that's been held by the Ukrainian government agencies and by at least one financial institution. This is a more sophisticated form of attack, but one that was largely thwarted because Microsoft detected the code, it quickly picked it apart, and it notified Ukrainians and it updated its virus detection systems to block it. And then at the request of the White House it worked with other governments in Europe, the Baltic States, and Poland to make sure that they were aware of the code. And I think this is an important example of effective cooperation between businesses, government, and among allies.

PITA: That's great, I'm definitely going to have some another question for you further on about that cooperation element.

So we know that Russia has the capability, or at least has had the capability to conduct these larger scale infrastructure cyberattacks. In 2015 there was a major attack against the Ukrainian power grid. What sort of theories are there as to why we haven't seen this sort of attack so far?

BRANDT: That's right. Ukraine's long been a testing ground for Russian cyber capabilities. Beyond the power grid attack that you just mentioned, I'm thinking in particular of the notorious NotPetya malware that was deployed using Ukrainian accounting software that very quickly spread around the world and cost billions of dollars in damages to businesses. And many other Russian cyberattacks that targeted Ukrainian targets, including the Kyiv metro, the Odesa airport, so there's a real history there.

And I guess maybe there's three theories, for what we're seeing today:

One is that maybe Putin wanted the rest of the world to see him achieve a decisive victory in Ukraine and thought that such an attack could maybe prevent the outpouring of images and videos demonstrating his prowess that he might have wanted to see.

I think that seems somewhat implausible now, because it seems clear that a quick victory at least is not forthcoming, and then, as you pointed out, Russia used a missile instead of a cyberweapon to take down a TV tower in Kyiv the other day.

Another theory is that he didn't want to destroy infrastructure on territory that he later planned to occupy because disabled systems can be expensive to repair, and they can also take time.

And maybe a third is that he hasn't wanted to shut down, for example, Ukrainian government computer systems which can be used to gather intelligence in wartime. So it could be any or all of these, and there are other possible explanations as well.

PITA: Great. So, cyber warfare, of course, isn't the only non-conventional military means of attack. Another avenue that Russia is quite famous for is information warfare. And the last day or two we've heard from Facebook, their parent company Meta, and Google, Twitter, that they've been taking some steps recently to block both official Russian propaganda channels, like the Russia Today TV news channel, but also against some other disinformation campaigns, particularly on social media.

Sort of a two-part here: One is, what is it that they've been reporting that they're taking steps against? And then the second question is, getting back to your cooperative element, is this the best way to counter disinformation online? Letting the technology companies and the platform's themselves handle it? Or are there other avenues for coordination?

BRANDT: Yeah, it's a great question. So, to your first point, what is it that we've been seeing? Russia has been running a long-running campaign to cast Ukrainians as Nazis and the perpetrators of genocide against Russian-speakers in eastern Ukraine in order to justify an invasion. By the same token, also to cast United States and NATO as the true aggressors in this conflict. And all of this is happening right out in the open on Russian state media, and Kremlin-backed accounts online.

We know also that Moscow planned to fabricate a justification for an intervention, including by filming a gruesome video of purported war crime, hiring Russian-speaking actors to play the part of mourners, and also by sending saboteurs into eastern Ukraine to carry out a false flag operation.

To your point about what's the best way to respond, I guess I would step back and say, I think perhaps some of the most effective measures that we've seen undertaken in this information contest is the effort that Washington and other allied governments, including London, have taken to repeatedly expose Kremlin hybrid activities, to get ahead of those measures. Because I think doing so really prepared the information space. It made it a lot harder for the Kremlin to justify its invasion with lies. I think it really shaped the public mind and created, I think, a stronger coalition for a sharper response.

So I think all of that pre-bunking work that really set the stage for this conflict has been responsible for, if not putting Putin on the back foot, certainly keeping him on his toes.

And then your question about what the platforms have done, yes, there have been takedowns and then also this wide variety of steps to push back on official Kremlin propaganda. Twitter said that it would you know downrank or not promote Sputnik and RT content. Microsoft has said that its Bing search engine is not going to send users to Russian state media content unless it's clear that that's where the user intended to go. Who else? Google news has said that they will no longer feature that Kremlin propaganda content in news searches. And Facebook has outright blocked Russian state media content reportedly at the request of governments.

Now that move, I question. I just am somewhat concerned about the precedent that that sets, and I’m not sure platforms should be in the business of outright banning content at the request of governments and doing so on the fly without a ton of transparency, especially when approaches like downranking, demonetizing and labeling I think can be quite effective. But anyway, that's how I see it.

PITA: Gotcha. I'm wondering what we're seeing in that sort of similar angle about disinformation or control of information within Russia? Around the world, we saw coverage of the really remarkable protests in St. Petersburg and Moscow of Russians protesting Putin's war and facing mass arrest. We've also seen President Zelensky and other Ukrainian soldiers recording their own messages intended for Russian mothers of Russian soldiers who are there, and the Russian public in general. Are Russians inside of Russia, seeing much of that?

BRANDT: Yeah, that's a good question. I mean Russia obviously does not have an open media environment. It’s consistently ranked near the bottom of ranking lists in terms of press freedom, but it's also not as closed as, say, China. I think maybe an interesting strategy here for Washington and for the White House is to expose Russian losses and the cost of Putin's adventurism as a way of speaking to the Russian people about the costs of Putin's exploits.

PITA: Before we wrap up, I want to come back to the angle of cyberattacks. As you mentioned, and you'd written a really great piece explaining about, how the U.S. and the other allied intelligence services were pre-bunking, getting ahead of Putin by saying look, this is what, we see you doing this and we were going to tell everyone that we see you doing this.

Obviously, when it comes to tracking hey there was a bunch of tanks that were in Siberia a month ago, and now all of a sudden, they’re a lot closer to the Black Sea, that's a lot different than maybe trying to track cyberactivity. What sort of advanced warning is there for cyberattacks? Is there much of that sort of advanced motion? Would the U.S. and allied intelligence services be able to take some of the same steps when it comes to cyber warfare?

BRANDT: I think what I can tell you is that an important step the intel community can take is to publicly attribute attacks and to do so quickly in their aftermath as a as a means of calling out Russia for its behavior. That's what the White House has done with some of those DDOS attacks and I'd like to see it continue that strategy in the days to come.

PITA: All right, Jessica, thanks so much for talking to us and explaining this today.

BRANDT: Thanks so much for having me.