The Balance of Control and Vulnerability: Cyber and Nuclear Risks

[00:00:00] Welcome and Introductions

Ryan Vest: Welcome to *Horns of a Dilemma,* the podcast of the *Texas National Security Review.* I'm Ryan Vest, executive editor of *TNSR*, and I'm here with our editor-in-chief, Dr. Sheena Chestnut Greitens. We're pleased to have joining us today Dr. Jackie Schneider, author of the article "Cyber Operations and Nuclear Stability: Networked Instability." Dr. Schneider is the Hargrove Hoover fellow, and director of the Wargaming and Crisis Simulation Initiative at the Hoover Institution at Stanford University. Her research operates at the nexus of technology, national security, and political psychology with an emphasis on cybersecurity, and autonomous systems. A prominent voice in defense policy, Dr. Schneider is the co-author of *The Hand Behind Unmanned: Origins of the US Autonomous Military Arsenal.*

Dr. Schneider is an affiliate at Stanford Center for International Security and Cooperation, and previously served as senior advisor to the Cyberspace Solarium Commission. Her work has appeared in a series of academic and policy outlets, including *International Organization*, *Security Studies*, *Foreign Affairs*, *Financial Times*, and *The New York Times*. She holds a PhD from George Washington University. Jackie, welcome to *Horns of a Dilemma*. It's great to have you on the show.

Jacquelyn Schneider: Thanks for having me.

[00:01:10] WarGames and Pop Culture Fears

Sheena Chestnut Greitens: So, Jackie, I wanted to jump into the introduction of your article, and maybe start with where people have seen some of the topics that you cover in the popular imagination, and even in pop culture today. So your introduction references the movie *WarGames,* and the very real impact that that had on the Department of Defense's thinking.

How do you think the fictional fears raised in that, and other movies that the listeners might have seen–how do those echo in today's debates about cyber threats and nuclear stability? And, you know, where do those fears maybe diverge from the reality that you explore in the article?

Jacquelyn Schneider: So first off, if you're going to talk about cyber, and nuclear, it's almost like a requirement to mention *WarGames*. So like, if you have your bingo card, like–check, check, done, right? But, you know, the reason why I lead with that is, because it ended up being so influential to how the United States started thinking about this relationship between digital and nuclear.

And I want to say that the cyber thing is really hard for us to visualize, and get our head around. You know, if anybody's ever tried to publish cyber work in, like, kind of a popular media outlet, they really struggle to find pictures. It's always like, you know: a computer screen with, like, green ones, and zeros. And so *WarGames* is so useful, because it makes something real, that otherwise lives in this very, kind of, virtual world.

And the other, you know, kind of–this is good news–is that we haven't actually seen cyberattacks that create nuclear effects or, cyber threats that lead states to use nuclear weapons, right? You have two kinds of, as we, as social scientists would think about, you have two variables that are actually really hard to operationalize.

Like, how do you operationalize cyber operations that are both virtual and, you know, clandestine, and people aren't attributing themselves? And then you have nuclear use, which thank God is something that we haven't seen for a very long time. And so these kinds of visual references become really important to helping us understand, like, "Oh, this is a threat." But they kind of Hollywoodize the threat. And so because we have two variables that are really hard to measure, we either *A*) ignore, or *B*) turn it into something that Matthew Broderick can star in.

And so the goal with this piece was to say, "No, actually, there are some kind of real fundamental characteristics of both cyber and nuclear, that may help us understand where there is a true threat, and what that threat could look like."

[00:03:58] Why Cyber Nuclear Analogies Mislead

Ryan Vest: I'm glad you brought that up, because right at the beginning of the article, you start off with this assertion, that general understandings of when, and why, cyber operations create this instability are intuitive at best, and misguided at worst. What do you think has driven the disconnect between the perception and the reality; and what do we tend to get most wrong about the relationship between cyber operations and nuclear use?

Jacquelyn Schneider: Well, cyber operations, because they're virtual–at least for a very long time–scholars would kind of hypothesize about their impact. And this is something we've done in the nuclear realm, for a really long time. Almost all of our understanding, or beliefs, about nuclear policy are based on theories, because we have very little empirical use–also good news.

But cyber is a little bit different, a lot of bit different, because actually cyber operations are happening all the time. And so it's a little irresponsible for us to say [that] cyber operations will lead to nuclear war, or cyber operations should lead to nuclear war in the following situations, because we actually do know a little bit about how cyber works, and the way it works in these kinds of non-nuclear realms.

And so the goal with this piece was to say, "Hey, look, actually, while we don't have a lot of, like, data about cyber and nuclear, we have a lot of data about cyber on its own." And there's something we know about how cyber operates in these kinds of more conventional domains, and how it affects the things that we actually interact with on a day-to-day basis–that maybe we could take that, and we could apply it to this nuclear variable, that we have very little data on.

And in the past, I think, we've relied more on analogies, like cyber is Pearl Harbor, cyber is Armageddon, it's 9/11. And that's actually kind of irresponsible when it comes to cyber, because it may be [that] our kind of poor, or bad analogies, that lead us to focus on either worst case scenarios, or scenarios that are not likely to happen at all.

[00:06:01] Three Pathways to Escalation

Sheena Chestnut Greitens: So, one of the things I really appreciate is that you focus on three specific pathways, where things could happen in the world, that lead to cyber-driven nuclear instability. And those three pathways are: deliberate escalation, inadvertent escalation, and accidental use. So just to get us started, in terms of going a little bit deeper into what you explore in the article, can you walk us through each of those pathways, and talk about how cyber operations interact with, or play a different role, in each of those pathways?

Jacquelyn Schneider: Yeah. And I'll start with maybe the easiest for us to get our head around, which is this idea of accidental nuclear use. So this pathway is a pathway, in which nobody wanted to use nuclear weapons, nobody intended on nuclear weapons, but something goes wrong. Either there's a technical malfunction, or a human malfunction.

And actually this type of escalation, while incidents can occur, we have many incidents of accidents. For example, you know, shooting civilian airliners down. This is an accident, right? Like, they don't mean to go to war, but this accidentally occurs because they misidentify an incoming threat, which is actually a civilian airliner. So this is kind of the accidental way that nuclear war could occur.

The other two are really about human intentions: deliberate and inadvertent. Deliberate means that the use of nuclear weapons is a part of my strategy. I think that the use of nuclear weapons actually allows me to achieve my objective.

So a few ways in which this occurs: one is that, you know, you are overwhelmingly not as dominant in other domains. Think North Korea–really good example. North Korea does not have as good an army, air force, navy, as South Korea and the United States, but they do have a burgeoning nuclear power. And so it could behoove the North Koreans, who would be worried that a first strike would take out the vast majority of their conventional military, to instead go nuclear early. Or if they're worried about the vulnerability of their nuclear arsenal to survive a first strike, then there is, you know, a chance–so these are, like, deliberate strategies, and reasons, to use nuclear weapons.

And then there's this thing called inadvertent escalation. And I think actually, we, as scholars, love inadvertent escalation, but it's actually really hard to prove.

So inadvertent escalation is this idea that, like, we are using nuclear weapons instrumentally. It's not an accident, but it is an inadvertent escalation. It wasn't something that either one of the states intended on doing. It's not core to our strategy. We just kind of felt like we had to. So this is all about misperception and uncertainty.

A really good example here is the idea of the security dilemma. So states that wouldn't otherwise go to war with each other, we call these status quo states, are confused about each other's intentions. And they may be confused because it's difficult to differentiate between offensive and defensive weapons, or because there's kind of a technological advantage towards the offense. And so states are

investing in weapons that they don't mean to use as an attack, but it looks like they're going to attack.

And so there is this chance for inadvertent escalation because you have these, like, arms races, and people end up targeting the wrong things, and then it convinces states that–I'm not actually going up against a state that doesn't want to go to war. I'm going up against a state that absolutely wants to take my territory, or wants to coerce me into doing something–and so this is an example of inadvertent escalation.

The other kind of good example of misperception here is entanglement. When you take resources, and instead of saying these are all satellites we're using for nuclear weapons, or these are all communications nodes that we use for nuclear command and control, you say, "actually, we also use these for kind of conventional command and control, or conventional early warning."

And so there becomes this entanglement between missions. And therefore, a state could think they are fighting a conventional war without escalating to nuclear war, and accidentally target something that makes a state feel like, "oh, shoot, now I need to go nuclear."

Ryan Vest: I'm glad you talked through all those different escalation pathways, because I think it's really important to kind of set aside, and look at the different ways this can happen.

[00:10:25] Percolation Theory Explained

Ryan Vest: But in your article, you actually use a different framework–this analytical framework of the percolation theory, to explain escalation risks. So moving on from looking at the pathways that can happen with nuclear escalation, I was wondering if you could talk a little bit about what percolation theory is, and how it applies to nuclear networks.

Jacquelyn Schneider: Right. So percolation theory is about networks, and how networks either gracefully degrade, or catastrophically are destroyed. And it's a theory that posits a relationship between the amount of nodes within a network, and the amount of linkages, and pathways, and the direction of those pathways.

And so, for example, the internet, which is this kind of extremely loose type of network, that has tons, and tons, and tons, and tons, and tons, of little nodes, and lots of little pathways, and multidirectional pathways. This is one in which the

destruction, or removal, of one of the nodes, or one of the pathways, has little overall influence on the ability of the network to continue to function.

But as you decrease the amount of nodes and centralize nodes, so think about, really good example here is a very kind of formulate form of cloud computing, where all the data is in the data center, and there are just a few linkages between the data center and the user–then you have much fewer nodes that can become much more vulnerable, and lead to kind of the overall destruction of the total network, with just a few node removals.

I don't think people think of platforms as nodes, or parts of a network. But what becomes clear from this theory is that, if you are a state that has chosen to go all in, for example, on just a few legs of the triad, right, like maybe just submarines, for example, you are actually fundamentally changing your nuclear network, and maybe inadvertently creating less resiliency, in terms of the diversity of pathways.

And so, I think that we may have relied sometimes on having one leg of the triad, in order to create deterrence and stability. But increasingly in this cyber world, even submarines are not going to be unfindable. They're not going to be invulnerable. And so thinking about, not only, kind of, how you're building out your sensor network, and your command control network, but also thinking about your platforms, and your weapon systems as networks as well.

Sheena Chestnut Greitens: When you're exploring this idea of the network structure, you really emphasize the potential trade-off between centralization, efficiency, and vulnerability in these different systems. So as nuclear networks have become more centralized, more sophisticated, how does that make them both more attractive, and therefore maybe more dangerous, or vulnerable targets, for cyber operations?

Talk to us about how that then plays into this idea of cyber risk, and cyber-generated instability.

[00:13:28] Centralization Control and Vulnerability

Jacquelyn Schneider: Yeah, centralization is a really interesting set of trade-offs. So look, if I'm just like a normal user of the internet, it makes sense to have this really huge network, and to be able to use lots of different ways in

which to access that network, because I'm not as concerned about whether somebody else is kind of mimicking me, right?

But nuclear weapons is this really difficult trade-off between, you need to make sure it is the right people who are making the decisions, right? We don't want someone to manipulate it, we don't want someone to intercept it, and we need to make sure that there is control over nuclear weapons. And that can lead to a network that is really focused on centralization, and making sure that you're privileging control, potentially over resilience.

And so here's kind of the big trade-offs. So a centralized network is going to be something that is the most efficient, and potentially the most secure. So think about control, for example. But a more diffuse network, a network with a lot more nodes, and a lot more pathways, is going to be a lot more resilient, but it also means you're giving up some element of control. It also is more expensive, and the most resilient networks are also the networks that have these complex kinds of elements, within the network.

So I mentioned the cloud earlier, and I talked about a really centralized kind of network. That's actually not how modern cloud works anymore. The modern cloud means that, most places like Amazon, you've got, you know, your data is not in one data center. There are backup data centers, and those can come on and come off, and there are backup relays, right? And this means that I can rely on getting my images out of the cloud. I mean, thank God, right? Like, I'm not going to lose all my pictures of my dog. But it also means that a lot of people can hack into pictures of my dog–and that's the trade-off that you have when you're thinking about how to build a network for nuclear control.

Ryan Vest: This is really interesting, Jackie, because you've talked about some of the trade-offs that we have between control and vulnerability with the net.

[00:15:47] ISR AI and Sensor Entanglement

Ryan Vest: I was wondering if we could move, or pivot just a little bit, to talk about ISR networks, and how digitization simultaneously increases resilience and entanglement, in kind of a similar way. How does the growing use of AI and machine learning in ISR change the balance between better warning, and greater escalation risk?

Jacquelyn Schneider: Yeah. So, when nuclear weapons first came into the scene, there were actually very few ways for states to get any indications and warnings that these were going to be launched. And some of the primary means that we were able to know that a missile was launched was through really sophisticated satellites, and that was their whole mission, right? They were trying to detect the infrared, the heat, that comes off these launches.

And everyone knew, like, that's what these satellites are for. They are vulnerable. Even, actually during the Cold War, the Russians, or the Soviets at the time, actually had anti-satellite weapons, and we were concerned about these vulnerabilities. But we're like, "That's okay," because everyone knows these are nuclear, and so if they targeted them, that would be really escalatory.

Now the good news is–because we know that those satellites are vulnerable–we now have a lot of ways of getting indications and warnings that there is some sort of activity that might lead, or is actually evidence of, a nuclear test. This is the proliferation of sensors–sensors in space, sensors underwater, sensors on the surface–and all of those pieces of information which really look at different things, right? Like they're pictures, they're environmental intelligence, they are intelligence that has to do with waveforms and electronic warfare, right?

So it's a lot of different types of data coming, a lot of different types of places. That's actually, like, really hard to parse together, because there's different uncertainty terms for all of this different type of information. And what AI and machine learning does is, it not only takes all that information and puts it together. So I'm not just like, you know, back in the '60s, I'd have to get a canister that had like the pictures of where we thought Soviet nuclear weapons were, or I'd have to fly a U2 over Cuba, for example.

Like now all that stuff's coming together real time. And that means that we have a better understanding of where nuclear arsenals are, how they're being used, if and when a launch would occur, so we're not completely reliant on, like, you know, a few satellites up in space, in order for us to understand the nuclear threat. That's great. It leads to situational awareness. But these are not assets that are necessarily even considered nuclear intelligence. These are assets that are used to understand a wide variety of different things going on in the world. In fact, some things that are like civilian things, that are going on in the world, like weather.

So there's this entanglement now, between sensors and resources, that mean that we have more uncertainty about whether a technology is being used to

anticipate very specifically a nuclear launch, or more granularly like, you know, the movement of maritime traffic, all over the world. We don't know, right?

And so that means that we have a network that has lots, and lots, and lots, and lots of nodes, but we have entanglement issues, and so there's a lot of confusion about whether those nodes lead to uncertainty. It also means that a lot of that information needs to be kind of put together in centralized places–so data centers.

And so, even while all that data is virtual, it creates a geography of modern-day intelligence that can actually be very centralized. And so you have nodes and hubs where the data is located, or where the data comes together to be looked at and disseminated. And then, you know, those relays themselves can be very vulnerable, especially if they're passing classified information.

So we have a network that is both more resilient, in terms of this sensor diffusion, but also has created a geography of centralization, when it comes to data amalgamation, and processing. So, goods and bads, right? It's a give and a take.

Sheena Chestnut Greitens: So this discussion around uncertainty and early warning always makes me think of the story, at the beginning of Scott Sagan's book, about the limits of safety. Where there's an alarm that goes off, and it turns, you know, lots of, sort of, near disastrous consequences, that luckily get stopped in time. But it turns out that the whole thing was triggered by, I think it was a bear climbing the fence at that particular site.

And I'm thinking–gosh, it would be nice if we had, you know, some AI tools that could enable us to say, "Probability of saboteur," or, "Probability of incoming nuclear missile, *X*. Probability of bear climbing fence, *Y*." Right? That might be sort of a helpful diagnostic panel for some of our decision-makers.

[00:20:57] Uncertainty vs Confidence in Crises

Sheena Chestnut Greitens: But I wanted to go back to this point about uncertainty, because I think this is so important when we talk about issues that, as you mentioned at the very beginning of this conversation, are hard to picture, right? And so you talk about, in the article, that cyber operations, and you've been talking about it for the last few minutes, that cyber operations often create uncertainty.

We've largely focused on the network so far. But as you also mentioned, nuclear command and control, and nuclear decision-making, ultimately is made by humans, and a very small number of humans. So how do you think that the uncertainty that you've been talking about affects human decision-makers, or could affect them during potential crises? And how do you weigh that element of human perception of the uncertainty around cyber operations, versus the sort of actual technical effects of cyberattacks themselves?

Jacquelyn Schneider: Oh, this has been the–so for anyone listening who's not an international relations scholar–we love uncertainty as international relations scholars. It is complex, it is difficult to measure, so, like, we're slightly obsessed with uncertainty. And I was raised by a defensive realist, Charlie Glaser, and so uncertainty's a huge part of realism.

So realism is a theory of international relations, and what matters for this conversation is that realists think that uncertainty leads to war. So quite often they're trying to recommend policies that decrease uncertainty, so that states are less likely to lead to kind of security dilemmas, and spiral dynamics that lead to war.

So when cyber came on the scene, everyone looked at it and said, "Oh my God, it is so uncertain." Like, "I can't see it. I don't know what it's going to do. I don't know who is doing it." Like, "Oh my God, this is going to cause nuclear war." And I actually did a bunch of empirical work in war games, and experiments, trying to understand how people responded to cyber, and was kind of baffled at first, because all that uncertainty around cyber did not, in my games, lead to escalations, or concerns about nuclear war.

Instead, it led to, like, restraint. It caused people confusion, anxiety. It slowed them down. So it's this really kind of interesting phenomenon. But I found something else in the games, which was that, quite often, when I gave people cyber capabilities, it gave them more certainty and confidence.

And here's where I gave three pathways to war in the paper. In the paper–I'm not–I don't say which pathway to war I think is most likely to lead to war, but I'll say empirically it's deliberate escalation. We actually have very few examples of inadvertent and accidental escalation to war, and I think Kori Schake's done some really good work on this.

And so then it's like, okay, well–let's see if these ways in which cyber creates uncertainty are less likely to escalate to nuclear war, then how does cyber create certainty? And this, I think, there are kind of network implications, because

when cyber networks tend towards that centralization, and when states are more confident that they understand where those vulnerabilities are, and what the effects of those vulnerabilities might be, they're also more likely to take that first strike against that target.

So data centers are a great example here. If your data's all over the place, right? I'm, as a state, not confident that I can blind you–we often talk about blinding attacks–I'm not so confident I can like blind you. But if you are putting the data in just a few nodes, then I might be more confident that a first strike is going to either protect me, or allow me to take that offensive action, that otherwise I would be unsure if it was effective.

And so, I think what we see here, is that when cyber attacks can imbue that level of confidence in the cyber attacker, then we both see kind of more likely to take those cyber attacks, so kind of more likely to take cyber attacks against NC3, if they're really confident that there's only a few nodes that they have to attack in order to cut off control.

And so I think this is an interesting thing because actually, when I started working on this, I was convinced that uncertainty was going to be my dominant pathway to war. But I'm more and more convinced that it's actually when we build networks, and make choices that create certainty about vulnerabilities, that we're more likely to see that kind of deliberate pathways to escalation.

Ryan Vest: This discussion on confidence certainty and uncertainty is really fascinating, because I've never really looked at nuclear escalation in those terms before.

[00:26:04] Data Trust and Manipulation Risks

Ryan Vest: And as you get to the culmination of your article, you argue that the most dangerous cyber operations are not necessarily those that cause dramatic failures, but those that attack our relationships with data, and undermine this trust in decision-making systems, and really get after the confidence and the uncertainty.

What do these kinds of operations look like in practice, and what are they especially likely to induce, or I guess really, why are they especially likely to induce an accidental nuclear use?

Jacquelyn Schneider: Yeah. So I like to tell people this story of when I was a baby lieutenant, which at this point is actually a very long time ago. Think about the world before the iPhone. That was when I was a baby lieutenant. And my first job was in South Korea–it was my job as the watch officer to stare at this common operating picture, and if I thought the North Koreans are coming south, I'm the one who has to call the general and let them know.

As you can imagine, it is both extremely boring, and extremely scary. This is the early 2000s, the first time you're sitting watch and you see a little thing coming down south like, "Oh my god, this is it." Like, "I'm gonna call the general. We're going to war."

And then the person, more experienced, sitting next to you is like, "No, no, no, no, no. Like it's, this time of the day, and at this time of the day, we only have a few sensors, and they have a tendency to malfunction in the following ways," right? And so I could believe everything else in that common operating picture, and not believe that one part. So there's this graceful degradation of trust, right? This is, kind of like, if you only have a few early warning sensors, type of thing?

But, if I went back there today, I don't think I would have any idea [of] the multitude of sensors. I would not be able to gracefully degrade my trust. I would either believe everything or I would believe nothing, and that can be extremely dangerous.

First, it's very dangerous to manipulation–and I think in the world of AI, where the developer's role in developing the algorithm, and the data, and the way in which a bad actor could influence, both the data that it's trained, on and the algorithm, that has really big implications for nuclear war.

And if you're building young officers, lieutenants much younger than me at this point, who are having to make that decision, like, "how do I respond to that little track coming south?" Then the characteristics of the network really matter, because today's diffuse networks means that manipulations are going to be far more important, and they will have a very large effect.

And how that lieutenant responds, whether they respond with, "I don't believe everything," or they respond with, "Oh my God, we have to go nuclear,"–that's a human, right? That's a human decision about technology–very hard to model what that will be.

But I will say, and this is not in the paper either, but I think there's a relationship between cyber and AI. And I think that the way AI is being developed right now is one that imbues confidence, right? Like when I go on Gemini, it tells me how amazing I am, right? It is designed to make me feel confident in its outputs.

The other side of that, for cyber, means that those deception, manipulation, and the cyber attacks that actually are generally kind of more likely to work, are also potentially, could have devastating effects, because they create misplaced certainty. And I think we need to talk more about that, when it comes to nuclear war, and this relationship between AI and cyber vulnerability, which, you know, is not in the paper. So that's like the next paper.

Sheena Chestnut Greitens: There's definitely a ton to unpack here, and I just want to flag that especially in this case, I really recommend people go read through the article, because there's a lot here that we just won't have time to touch on in the discussion today, but that really bears, I think, mulling over, and thinking about. Because what the possibility these are and how they combine, your article really challenges some of, at least my thinking, and I think the thinking of many other people, about what could go wrong, how, and why.

And so I just wanted to put in that plug. Please go read the article. It's great.

[00:30:37] Policy Lessons and Network Design

Sheena Chestnut Greitens: So I wanted to ask a question to you about the implications for policy. If you could have policymakers take one lesson from this article, what should they, or should we be rethinking about how to design, defend, or operate nuclear systems in this current cyber era? And what trade-offs are just going to be unavoidable, even with improved, or near perfect cyber defense? How should policymakers think about their priorities in this world?

Jacquelyn Schneider: So in general–kind of more nodes, more platforms, more sensors, more data processing centers, is going to lead to more resilience. I think resilience is good, right? I think resilience increases deterrence. I think it decreases accidents, but it's really expensive. It requires a lot more training and knowledge.

And I think you give up some level of control, right? So maybe there's some nuclear missions, like command and control, that you can't actually go all in on

resilience for. In which case, you need to focus on where those vulnerabilities are, and really harden them. So if you have a very centralized network that has only a few nodes, those nodes have got to be prepared to survive a physical attack, prepared to survive a cyberattack–if they only have a few pathways, data relays.

And I think that one of the things we don't think about enough, is the trade-off between limited nodes and multiple pathways. So maybe one of the solutions to–I don't have a lot of nodes because I don't trust a lot of people–is a lot more different types of pathways. So think about it like, "Oh, I have a way to communicate over the horizon via space, but I also have a way to communicate with wireless, kind of, line of sight relays, right?" Like thinking about different ways in which you can kind of solve the problem that your network creates for itself.

And I think in general, we talk a lot about cyber, in terms of the ability of the exploit to create an effect. And what this article is about, is not like the exploit to the effect, but instead how the probability of the scope of the effect is based on the network structure, not the particular vulnerability.

And I don't think we think enough about that, partly because–what are the cyber processes, the practitioner processes that have to do with the network? The way we build the networks is generally kind of siloed in a very different place than how we build weapons. And so there's kind of a disconnect.

So each weapon system, there are requirements to make sure it's kind of cyber hardened, but then how that weapon system then connects to the overall network, so that it can be used, and so that it can receive intelligence inputs–who looks at that? Whose job is that? So I think it's kind of this more holistic look.

And then always, this is what I say all the time–training, training, training. It's all about teaching the operators, not that there will be no vulnerabilities, but where their vulnerabilities exist, so that you can avoid inadvertent and accidental escalation. I think that there are ways in which we can train out inadvertent and accidental escalation, in which case then all we have to deal with is deliberate escalation.

And that I think is an easier, almost an easier trade-off, than if we're trying to focus on one versus the other.

[00:34:21] Closing Thanks and Where to Read

Ryan Vest: Jackie, we want to thank you very much for joining us today. This has been a really interesting discussion.

Jacquelyn Schneider: Well, thanks so much for having me.

Ryan Vest: Thanks for joining us on *Horns of a Dilemma* from the *Texas National Security Review*. Our guest today has been Dr. Jackie Schneider, author of the article, "Cyber Operations and Nuclear Stability: Networked Instability," which as always can be accessed for free on our website. If you enjoyed this episode, be sure to subscribe and leave a review wherever you listen, and you can always find more of our work at *TNSR*.org.

Today's episode was produced by *TNSR* Digital and Technical Manager Jordan Morning, and made possible by The University of Texas System. This is Ryan Vest and Sheena Chestnut Greitens. Thanks for listening.