PRESENTER: Thank you, Elizabeth, for that very kind introduction, and thank you to all of you for having me. When I agreed in early February to do this talk, Russia hadn't yet invaded Ukraine. So I thought, well, I'm going to have to think hard about what to talk about. Not so much now. That's the obvious topic and pretty clearly the biggest challenge for US foreign relations right now.

But I want to use my time to say a bit about where things stand with respect to the Russia Ukraine conflict but also to use that conflict as a way to highlight some broader challenges for US national security and foreign relations, ones that predate the Ukraine invasion but are being brought into sharper relief by that conflict. So I'll talk a little bit about US sanctions policy and then inevitably about cybersecurity, which is one of my main focus areas.

So the invasion and the conflict, which started February 24, are of course first and foremost a tragedy for the people of Ukraine. The best estimates to date suggest that there have been thousands of civilian casualties and many more are expected to be discovered in the coming weeks and months. In the first few weeks of the conflict, the International Organization for Migration estimated that more than 4 million Ukrainians have become refugees and over 7 million are currently internally displaced. And the United Nations has warned that the number of refugees could rise to 8.3 million by the end of the year. This is a displacement. The rapidity of this displacement is unprecedented in modern history.

Also for those left in Ukraine, the situation is dire. Estimates suggest that a further 12 million people there now are in need of humanitarian aid. And the conflict is having ripple effects around the world. I'm sure we're all familiar with the rising energy prices. But it's also causing an exacerbation of food insecurity around the world. The World Food Program buys half of its grain from Ukraine and UN officials have warned that the conflict will exacerbate food insecurity in places like Afghanistan, Yemen, and the Horn of Africa that are already struggling.

But Russia's aggression against Ukraine is not just a humanitarian catastrophe. It's also a fundamental challenge to the international order and to international law. So Putin announced the invasion, the so-called special military operation, during a UN Security Council meeting. And this is, to be clear, a flagrantly unlawful action. As many countries have noted, this is a war of aggression. It runs completely contrary to the UN charter's prohibition on the use of force and to the respect for territorial integrity. And the revelations of Russian war crimes since the invasion have been just horrific.

But for all of its illegality, the main entity that's theoretically supposed to be addressing the crisis, the UN Security Council, has been paralyzed. Russia has used its veto to block Security Council action. In addressing the Security Council on April 5th, Ukrainian President Volodymyr Zelenskyy raised some very pointed questions about the future of the Security Council and about the United Nations. He accused Russia of turning the veto into a license to kill and argued that the Security Council must be reformed. Unfortunately, those reforms can be blocked by a Russian veto.

So in this predictable absence of the Security Council, what we've seen is that the United States, European countries, and other allies have turned to coordinated actions outside the United Nations to both support Ukraine and to punish Russia. Some of this has been in the form of military and intelligence support, which you may have seen playing out in the pages of *The New York Times* recently. But I want to pivot now to two issues that I think have broader implications beyond just the Ukraine conflict. So the first is the use of economic sanctions by the United States and the second is cybersecurity.

So in economic sanctions, the US, EU, and their allies have imposed just a massive raft of sanctions and other economic measures. To give you just a sense of what all has been done, here is a partial, and I emphasize partial, list. They've targeted Russian banks. They've imposed full blocking sanctions on them and prohibited them from accessing SWIFT. They've sanctioned Russian companies involved in defense and critical industries. They've sanctioned Russian government officials, oligarchs, people close to Putin, and the adult children of all of these categories of people. They prohibited debt payments in dollars held by US financial institutions, pushing Russia toward a default.

They prohibited imports of luxury goods into the United States and exports to Russia of tech components that are needed for military and other industries. They've banned Russian planes from their airspace, Russian boats from their ports, and the United States and other countries have banned some energy imports, though Europe is not fully on board with that yet. All of these actions are designed to do significant damage to Russia's economy, and they're being exacerbated by private companies that have also exited the Russian market.

But the big question with these sanctions is will they be effective and effective at what? So the threat of sanctions obviously did not deter the invasion ex-ante and it's also very far from clear that the pain of sanctions can force an end to the conflict. Nonetheless, sanctions have become the US move in foreign relations. During the Obama administration's first term, the United States issued about 500 sanctions a year. By the end of the Trump administration, that figure had risen to 1,000 a year. And I suspect this year in the Biden administration, we are surely on track to surpass that number as well.

The Obama administration Sanctions Coordinator Dan Fried wrote in 2020 that economic sanctions have become a default setting for US foreign policy and for the US government and Congress to respond to policy problems that seem to require more than a demarche but less than military action. And the United States is using sanctions as expressive policy. Sanctions express condemnation of the behavior of the sanctioned party. So the US sanctions human rights abusers, proliferators of nuclear weapons, states that engage in destabilizing cyber attacks, and this condemnation, both moral and legal, is certainly part of the point with Russia sanctions.

But there are still serious policy concerns with whether sanctions will have the intended effect on their targets. So there's a risk of evasion. There's the ability of sanctioned countries to turn to other countries to evade sanctions to get around the prohibitions that have been put in place. And there's a serious concern with respect to Russia that China will play that role. There's also real concern that sanctions just don't work that well when you're going after big economies like China and Russia. They have more capacity to cope, more resources to adapt.

And from a policy perspective, there's also concerns about sanctions being a one way ratchet. So what do I mean by that? The US frequently imposes sanctions and only very infrequently does it lift them. It's easy legally and politically to impose sanctions. It's much harder politically to walk them back. Who in the executive branch or Congress wants to be seen as going soft or going easy on parties that have been sanctioned?

But this raises a problem for the United States and for its policy. So if the targets of sanctions don't believe that the sanctions will be lifted even if their behavior changes, why change their behavior? The goals of sanctions and the conditions for lifting them need to be made clearer if, in fact, the goal is compelling a change in behavior.

It may, however, be the case that that's not the goal and that the goal is instead containment. So if the goal is containment, then there would be no conditions for lifting the sanctions and we may very well be in a containment situation with Russia. Secretary of Defense Lloyd Austin said after a visit to Kiev a few weeks ago that the United States, I'm quoting here, wants to see Russia weakened to the degree that it can't do the kinds of things that it has done in invading Ukraine. That sounds to me like containment.

Sanctions are more effective when they're done multilaterally, as the Russia sanctions are. But one additional challenge that comes with multilateral sanctions is keeping all of your co-sanctioners on the same page, especially when the sanctions have important costs for those who are imposing them. And we're seeing that challenge now with getting the EU on board with energy sanctions against Russia. Treasury Secretary Janet Yellen has said that the Biden administration's goal has been to impose maximum pain on Russia while to the best of our ability shielding the United States and our partners from undue economic harm. But that's really hard to sustain, especially for Europe, which is heavily dependent on Russian energy.

So to wrap up on sanctions, there are a lot of open questions about how efficacious sanctions can be. And there are also open questions about what is the plan? What is the point? What is the strategy? These aren't issues that are specific to Russia, but certainly the Russian sanctions are going to be an enormous test case for sanctions policy more generally.

So let me switch to the second topic, which is cybersecurity. And this is actually a little bit of a happier story with respect to Ukraine, because I'm not here to tell you that there have been massive destructive cyber attacks, which is great, because back in February I thought that might be the speech. But cybersecurity is a persistent challenge for the United States. We're just past the one year anniversary of the Colonial Pipeline hack. You might remember last year sort of panic buying, gas shortages after Colonial Pipeline shut down, a major US East Coast US pipeline, in response to a ransomware attack.

That incident came only months after the discovery of another hack, a supply chain hack on a company called SolarWinds, that the United States has attributed to the Russian government. It was basically Russian government espionage against a bunch of US government agencies and private companies. And also it came just two months after the Microsoft Exchange hack, which compromised thousands of small businesses across the United States. The United States blamed China for that one.

This is not an impressive track record for the United States in cybersecurity. The United States is not so good at defending its own systems and networks, or at least it doesn't appear that way. And so there were a lot of concerns in advance of the Russian invasion of Ukraine that this would be a very bad story. Russia has used Ukraine in the past few years as a bit of a testing range for some really nasty cyber operations.

So in 2015 and 2016, Russia launched operations that turned off the power in parts of Ukraine. And in 2017, Russia used compromised Ukrainian accounting software to launch an attack called NotPetya that's become the most expensive cyber attack in history. It eventually spread around the world and caused about $10 billion in damage. So given this history, there was a lot of concern about what the cyber component of the Russian invasion would look like, about attacks on Ukraine itself and about the possibility for spillover.

But the role of cyber operations, successful cyber operations, has actually been pretty muted. And that's a good thing. But the problem, for those who study cyber, is that it's not clear exactly why. So the *Washington Post* recently cataloged no fewer than 11 possible explanations for why this has been the case. But I think they can be grouped in two very broad categories. And I say this because either of these categories, if it proves to be the explanation, has interesting implications for US policy going forward.

So what are these two broad categories? First possibility is that Russia attempted cyber attacks but they failed. And the second possibility is that Russia chose not to launch widespread destructive cyber attacks. So taking the first one, that they attempted attacks but they failed, that might suggest that the cyber defenses in Ukraine and assisted by other parties succeeded. This is surprising given the frequent mantra in cybersecurity that offense dominates defense.

It would fit with the broader picture of the invasion where Russia failed to achieve its objectives due to poor planning, due to underestimating Ukrainian defenses. And it also fits with what's been said or leaked publicly about cyber operations. So the head of US Cyber Command, General Nakasone, testified to Congress a few weeks ago that the United States has worked, quote, "very, very hard" with Ukraine over the past two years, including putting US hunt forward teams in Kiev.

There have also been a couple of interesting announcements in the last month about attacks that were disrupted before they succeeded. So US Department of Justice announced in April that they had disrupted a Russian government controlled botnet before it had been used. We're used to seeing these announcements after this destruction has happened, sometimes years after the destruction has happened. This one was in advance. And Ukrainian authorities also announced that they had successfully stopped an in progress cyber attack by Russia's military intelligence that would have caused a blackout.

Another version of defenses succeeding is resilience. I mean, we're seeing a lot of ways in which the Ukrainian people are resilient, but this is another. So the most significant example of a successful cyber attack accompanying the invasion was a hack directed at a company called Viasat that provides satellite intelligence-- sorry, satellite internet service in Ukraine. And just a couple of days ago on Tuesday, the United States and the EU and other allies formally blamed Russia for the hack, which occurred an hour after the invasion started. But at the same time, disruptive as that incident was, and it knocked out some communications as the invasion unfolded, Ukrainian networks, Ukrainian communications networks have proven resilient, as we've all seen.

So what do we learn from this? Despite the fact that defenses often fail, the ultimate lesson may be here that experienced defenders engaging in focused defense of discrete targets against known enemies, the situation in Ukraine, can actually succeed. And having a clear example of successful cyber defenses in such circumstances might spur the United States and its allies to supercharge assistance internationally to vulnerable countries and perhaps even, fingers crossed, domestically. We'll see.

But what about the other possibility, that Russia chose not to deploy significant cyber attacks? It's possible Russia was deterred by fears of spillover, although they don't seem to have been deterred by much else. I think it's probably more likely that the choice, if this turns out to be correct, that they didn't deploy massive cyber attacks accompanying the invasion tells us something interesting about the optimal role for cyber attacks in an armed conflict. It's a lot easier to bomb something than it is to cyber attack it.

And so one thing we learn from the Ukrainian conflict ultimately may be that even when a major cyber power launches a major war, major cyber related disruptions may not follow or at least not necessarily. Different countries in different circumstances may make different choices, but one does not automatically follow the other. So I think there's a lot more to learn factually, strategically, legally from the Ukraine conflict.

But I want to end on perhaps a more optimistic note about international law and the international order. So I think the international order is a little bit battered at the moment, but it's also rallying. That's the optimistic part. So there's a tremendous amount of unity and resolve in pushing back against Russia's aggression. Not perfect unity, to be sure. There have been some very significant countries that have not joined in the condemnations. But a lot of unity from US, the EU, and allies around the world, and Ukraine itself to end this conflict on terms that are favorable to Ukraine.

And that unity itself is worth a lot. We've seen major violations of the international legal order met with major responses from sanctions to military aid to prosecutions that are still to come. And the first one started today in Ukraine. So I'll end there, and I look forward to your questions.

[APPLAUSE]