AI on the Frontline: Lessons from the Iran Conflict

May 6, 2026
Featuring Max Lesser and Max Meizlish
Moderated by Behnam Ben Taleblu

TALEBLU: Hey, guys. Good morning. Woah, that's loud.

(LAUGHTER)

TALEBLU: I definitely know you all can hear me well enough. Thank you so much for coming. I think we'll have a few more folks trickling in as the conversation starts but thank you for choosing this panel and for spending your morning with us. It's a pleasure to be at AI Expo, with two friends and colleagues from the Foundation for Defense of Democracies. You guys signed up for, in case you forgot, the AI on the Frontline conference, or I should say, panel, with three guests from the Foundation for Defense of Democracies, just by way of background with our organization. FDD has been basically operating for a quarter of a century in Washington, D.C. It's a fiercely independent nonprofit, nonpartisan think tank focusing on foreign policy and national security. I've been there a little bit – about 13 and a half, 14 years now. I'm the senior director of the Iran program. We got Max Lesser, who's the senior analyst on emerging threats at the CCTI, the Center on Cyber and Technology Innovation at FDD. That's one of our three centers of American power. One of our other centers of American power is being represented today by Max Meizlish. That's the Center on Economic and Financial Power. And they're going to splice and dice an AI issue for you that is in the news. And that is the Iran war. So, while folks still trickle in and you've got the obligatory bio out of the way, let's get cooking.

AI in the Iran war. There's an information space. There's a kinetic battlefield. There's a financial battlefield. AI kind of is the connective tissue between all of them. We've been seeing and hearing a lot about it. I'm going to ask you guys about some specifics in your lane, things you're sort of looking at on a day-to-day basis at FDD. But maybe if you could just both tackle this question first. AI in the Iran war: overhyped, under-hyped, or has the kind of mainstream media and social media and AI commentary gotten this right? Max and then Max.

LESSER: Hey, can everyone hear me? Yeah? So, I want to get a sense of – of how hyped AI actually is in the Iran war. Who here has seen the Lego videos?

TALEBLU: Two hands up.

(LAUGHTER)

LESSER: Two hands up? And who here has had the hip hop tracks stuck in their head as they're brushing their teeth and going about their day? OK, I'll raise my hand for that. But I also – my job is to binge-watch Iran Lego videos, so. But clearly, it's penetrating the U.S. information environment. I can say anecdotally and based off of the engagement that I see on various platforms that it's resonating with American audiences. I would say likely also with international audiences. So, when it comes to information warfare, I would say AI is not overhyped. And I'm looking forward to unpacking that with – with you guys today.

TALEBLU: Max?

MEIZLISH: Yeah. I think that within the space that I've covered, which is on economic statecraft and illicit finance, to ask whether it's overhyped, I think, is actually the wrong question. It's – it's actually more…

TALEBLU: Starting off dangerous.

(LAUGHTER)

MEIZLISH: Yeah. Well, it's probably more appropriate to think about whether we're thinking about it at all. And so, this issue isn't really Iran-specific per se, but in the context of sanctions evasion and illicit finance, bad actors who try to use whatever financial flows that they can to generate revenue and attack U.S. interests, allied interests as well. AI has a – a really interesting use case there. So financial institutions are adopting AI to combat anti-money laundering, to combat terror financing. But it goes the other way as well, right? And so, what we will likely see over the years is more adoption by bad actors to utilize AI to rapidly generate accounts at financial institutions. And I think that where there's really a vector of attack that these – these bad actors will look to is in the realm of crypto. So, we'll touch more in this conversation about how AI and crypto can kind of be linked together by bad actors. But that's where I think the attention needs to be and we're not really focusing on it as much as we should.

TALEBLU: I want to get in, a little bit later, into this thing that you mentioned, account creation, given that so much of the majority of the Iran war, which is now kinetic and being run by the Department of War, formerly known as the Department of Defense, has for 20 years in D.C. been dealt with by the Treasury Department. So, we're going to get into that in a little bit, but Max – the not Lesser, if I shall. Let me start with you about AI in the information space. How can – how do you situate the use of AI into Iran's larger disinformation strategy? Usually, people think about disinformation and tech and foreign policy, and they think Russia. They don't think Iran. Is there a connective tissue here? And how does AI really help or magnify Iran's larger disinformation operations?

LESSER: Yeah, that – that is a great question. And yes, in the American public mind, when we think about information warfare, which is the term I prefer because it is warfare, right? It is a form of conflict. It's not just a form of competition. We tend to think Russia. Those of us who've been paying close attention, like myself and my colleagues at FDD, know that Iran has actually been very active in this space for years. For years. And also, China, right? Talking about the AI Lego videos, China actually in 2020 released a Lego video about COVID and sort of having a dialogue between a statue of liberty represented as a Lego figure and a Lego figure representing China and sort of going back and forth comparing both responses to the pandemic, right? And I think that also illustrates the big difference now is – back in 2020, right, that's pre-ChatGPT, right? Or at least before it was widely used or widely available.

When you look at the quality of the propaganda coming out of Iran now, the AI-generated propaganda, the quality has improved dramatically. And then one other point that I want to bring up that I think is very important. You said a very important word, Behnam. You said disinformation. And unfortunately, that word has become a very politically charged or polarized word. And the other thing is, that is just one tactic within information warfare. Disinformation, deliberately false information, is one tactic. And why the Lego videos are so powerful – which, if you guys aren't aware, millions of views. Millions of views. It's hard to even totally count it because the accounts get taken down and they get put back up – is it's a story. It's not fact. Stories are arguably unfalsifiable often, right? Because facts are just one component that can support or not support the narrative. And disinformation – the thing about disinformation is, when we think about AI and information warfare, for the longest time, I remember two, three, four years ago when – when AI started becoming more mainstream and people started using chatbots more and generative AI became more accessible.

There were all of these news articles sort of warning of an imminent deepfake disinformation apocalypse. Has that happened? No. Right? Actually, a lot of public awareness was raised. There are things like community notes on X. There are a lot of fact-checking organizations. If somebody creates something that's false, it's actually easier to debunk that than it is to combat a narrative, right? And I think to say the last point here, using AI to illustrate narratives and tell stories in more engaging ways and in the language of the community that you're trying to affect. That is, I think, the most potent and powerful application of AI within information warfare, even more so than deepfakes.

TALEBLU: And again, just as – leading the Iran Program at the office, a lot of this stuff in terms of the platforms and the software that Max just mentioned, way above my pay grade, but looking at the specificity of the details of these AI videos – you know, you may remember the downed American pilots in Iran recently. It was in a particular area of Iran where even the Lego video got the appropriate Balochi tribal wear on the Lego person. So that was the level of specificity. Or looking at Iran's ballistic missiles, usually you look at all these kind of AI, very quickly generated videos. You know, it doesn't look like the projectiles of a certain country's arsenal. So much time was spent on the color, the scheme, the warhead shape, the finlets. So, there's an eerie level of accuracy coming, and the speed at which this accuracy is coming is really shocking.

And I want to get to speed because you mentioned, you know, creating and taking down these accounts. You know, you've, hand in glove, let's be honest, looked at what Treasury has been doing for a very long time on Iran. And, you know, one of the big things that the Treasury Department calls sanction success – or people who come in and out of the Treasury Department called sanctioned success on Iran is ratcheting up the hassle factor. You know, none of America's adversaries are going to stop the bad things they're doing tomorrow because of a single sanction or a single penalty or a single call out, but it increases the cost. You – you just alluded to the rapid way in which Iran could get around that cost. So, could you just unpack that for the audience a little bit? And then you also mentioned – you know – I want to talk about the stablecoin, but you also mentioned cryptocurrency. What is Iran doing in the financial warfare space as it relates to AI specifically, and was that helped or hurt by, I think what we're calling now, the 40-Day War?

MEIZLISH: So, you know, it's interesting because Max was sharing that in the context of the information warfare domain, that the battle over the narrative is where AI can prove to be most effective. And I imagine that's the case for our adversaries, but also for the US and its allies and partners in combatting those narratives. And you – you relay that in contrast to – to deepfakes. And so, AI, what we are seeing, is just across the illicit finance landscape, is that AI tools are increasingly being used for deepfake purposes to create fraudulent forms of identification, to create fraudulent forms of proof of life, right? Verifying someone's status as a living individual. And so, all of these tools are actually being utilized at scale to open up accounts at a rapid clip.

TALEBLU: So, like address, health record, name, birth certificate?

MEIZLISH: Exactly.

TALEBLU: Wow.

MEIZLISH: Right. So, all these fraudulent forms of documentation that are needed to validate someone's personal identifying information. Beyond Iran, right, we actually see this happening a lot with North Korea, which is a huge sanctions evader where they have individuals going in, applying for jobs at firms, and they're using AI tools to mask their identity, appear as they're – they're based somewhere else, or they actually appear to be someone else. So, they can enter a workforce and then hack into those domestic systems for corporate espionage purposes. But with respect to AI and also finance, beyond the data verification or – or creating fraudulent documents, there is this ability to just rapidly create accounts, right?

So, we have agentic payments, which have a legitimate commercial purpose. We want agents to go out there and actually execute functions on behalf of individuals and entities in the corporate environment. We want agents to go out and be able to purchase and restock for a commercial enterprise when stocks run low, right? That's something that an AI agent can do, and it needs to be able to transact financially. The same principles there can actually be used by bad actors to obfuscate their identities, to create new levels of shell corporations and opaque trust structures, all without a human actually being involved in a loop. And so that's going to raise new questions for regulators as they think about the extent to which these know-your-customer rules and regulations need to be applied to agents themselves or can we do know-your-agent regulations.

So, I think that's at the forefront of some regulators here in D.C., but I'm waiting to see where the test case is from the enforcement posture there. And then, you know, the crypto elements…

TALEBLU: Stablecoins.

MEIZLISH: …It's – it's related when we think about how money can move, how these agents can actually take hold of – of payments, right, and be the forcing function for payments being made, for money moving from account to account. And so, there's a natural symbiotic relationship with AI systems that can engage with blockchain and move funds. And so, the preferred vector for – for moving crypto by the Iranian regime and a lot of other bad actors is through stablecoins, right? So looking at cryptocurrency that's pegged one to one with the U.S. dollar, for instance, the most important of which is USDT, it's Tether, oftentimes on the Tron blockchain.

So, the regime has moved billions of dollars this way and has cryptocurrency exchanges that have been sanctioned by the United States over the years. You know, what we're seeing is a proliferation of this illicit finance at a scale that I think is just going to be a new challenge, unlike anything we've really seen over the years, because these exchanges will be able to pop up, right? The core infrastructure exists, that financial plumbing is there. And where AI is going to be advantageous for our adversaries is in quickly moving some of those accounts in the underlying infrastructure so the funds can ultimately stay and keep flowing though bad actors.

TALEBLU: I think we also together, last week or a week before, got to – it's been well known already, but we got to expose further this Iranian, I think the largest crypto exchange, which is still yet to be sanctioned and there's more open source material coming to light about who some of these partners are in doing exactly what Max just said. But pivoting back to the other Max now. You know, Max – the not Lesser – discussed the pipeline, the infrastructure. What about the pipeline on the information warfare side? What has Iran set up that makes it effective, if at all? And you mentioned in your last response, audiences. Who do you think is Iran's target audience? I have my view looking at Iran, especially given that now there's – I think some of you still know this – a 68-day national internet blackout. A lot of times we talk about these videos and for so many authoritarian regimes, when they put out stuff that they tout their ideology or their worldview or their narrative, we tend to talk about this in D.C. in policy circles as cheap talk or really for a certain domestic constituency.

But if their domestic constituency can't access this stuff, what does this say about them under war targeting what I think is a foreign audience? But am I correct to think the primary audience is foreign, not domestic?

LESSER: Yeah. So, I guess I'll start with the second question first. So, it's interesting. One of the – the major content creators behind these Lego videos, there's several, and one is called Explosive Media. And I was – you know, I love my job. I'm a professional doomscroller, right? So, I just get to spend hours and hours watching this propaganda content. And I haven't been brainwashed yet, I'm happy to say so. But so today I was looking and I was looking at Explosive Media's videos, and they actually have videos that are clearly oriented towards a domestic audience. And it's a fascinating point, Behnam, because they use a totally different language – literally a different language, right? They're using Persian. But they use a different set of cultural motifs and things like that. They're using a lot of religious language, a lot of the motifs that come from Shia Islam, right, things like that. And also, I don't think they would want those videos necessarily to be seen by the West because they're a lot more violent.

They're a lot more aggressive, right? One of the most recent Lego videos I saw was clearly geared towards an American domestic audience. They had somebody – they had this one image that was depicting an Iranian chatting over like Zoom or something with somebody in Portland, with somebody in San Francisco, right? Things like that. There is a lot of targeting of anti-war sentiment in America, which also, by the way, is nothing new when it comes to information warfare and influence operations. Famously, the Soviets heavily targeted and tried to co-opt the anti-war movement in the US during the Cold War. Famously, there's a wonderful book out there for anybody who's interested in this topic by Thomas Rid called *Active Measures*. And I guess you'll know if you're interested in this topic if you read it, because for me it was the most riveting thing I've ever read, and for some people it will probably be extremely boring. But they talk about how they were trying to – the anti-nuke movement in the US, they were trying to co-opt that.

Why? Because they didn't – they didn't – they – wanted the US to not have nukes, right? Because they wanted to keep building nukes, but they want there to be more domestic resistance against the US having nukes. So, there is this sort of two-faced approach where they use very different language and a very different narrative to – to talk to their own domestic audience than to foreign audiences. And we could extend that at length. Iran has gotten very targeted in their influence operations targeting the United States in the past. And this is something I've paid very close attention to for the past few years before it was in headlines. They were – in the lead up to the 2024 U.S. elections, they created specific websites, fake news websites in America, targeting veterans, targeting people on the far right, targeting people on the left, targeting African Americans, even targeting Muslims in Michigan, right? Very specific demographic targeting that we see here.

But what I would say, the difference between the fake websites in 2024 and the AI Lego videos that have gone viral: none of those websites went viral. Why? They were using AI. They were using AI. Sometimes you would even see the prompt. They accidentally kept that in the article. So, it would say, "write an article about blah, blah, blah." And it would be funny too, because you would see something that acted like it was – there was one called *Savannah Times* that kind of acted like it was in Savannah, Georgia. And then there would be this random obituary for like, you know, the president who'd passed away or something.

Something doesn't fit here. But I – I don't know if – partially, I would say yes, because of the quality of the models. The models become more powerful and that enables them to create content more quickly and create content, crucially, that's more compelling, right?

TALEBLU: To the target audience.

LESSER: More compelling. And they don't have to know it. They actually say that they're getting tips from Americans about what they should include in their next video too, which is fascinating, right? But also, it's – it's just – it's not just about the AI. It's also they – some people have said that the reason their international propaganda, right, their foreign-facing propaganda has become more effective is because Explosive Media is Gen Z, right? They're having younger people – they're giving trust to younger people and commissioning younger people to create these videos for them. These younger people, Gen Z, they're fluent in the language and the culture of the internet. And that's why this stuff is more effective.

And I know we're not getting to solutions yet, but just because I have to, like, this is something that I think the US should learn from. Our – we try to communicate with international audiences for many years, right? Radio Free – Free Liberty, Radio Free Europe, Voice of America. I think placing trust in the younger generation to be those content creators and to be able to communicate in the language of the internet and in a sort of web-native fashion, I think that is – is a lesson that we can take away as well.

TALEBLU: Absolutely.

MEIZLISH: I have – have something to add here on. You know, it's interesting. My work is really focused on economic statecraft and matters of illicit finance and tracking the money, thinking about the coercive tools that we can use against financial institutions. So, you know, I don't want to sound a little bit too out of my depth, but, you know, we do have another colleague at FDD, Leah Siskind, who's done a bunch of work related to AI, but forgive me if we're going into this, but there's this concern also that adversary regimes are proliferating the information space and that their state-backed propaganda is actually being incorporated into the output for Western audiences as well, right? So beyond just the narrative space of, you know, the Lego videos that are being produced in these compelling stories, just from a fact-based perspective of people increasingly looking to AI as a source to assist them in their research and relying often…

TALEBLU: On crawls and scrapes and…

MEIZLISH: Exactly. And so, they're proliferating by creating dozens and dozens, hundreds, thousands of webpages that the AI models are scraping from and then incorporating that into news reporting or whatever it might be that's utilizing AI. I think that's concerning. And so, the link to my – my space and the economic element to it – a friend, he and I wrote this piece a little while ago in the *Wall Street Journal*. He just published another piece yesterday in the *Journal* about this. Thinking about how, with the rise of event-contract prediction markets, how there's a new balancing space there as well, and thinking about how adversaries in the information space can actually manipulate our understanding of truth, right? And so, with these prediction markets, which their promise is to help proliferate a crowdsourced understanding of information, how bad actors can actually utilize tools like AI to create different levels of exposure that we wouldn't have been able to see before from the manual information operation space. And that's – it can be really damaging because these event-contract markets, prediction markets, are increasingly being utilized by trusted news media. Like Dow Jones, for instance, I believe has a partnership with Kalshi or Polymarket. There are a few other mainstream news entities that have these relationships.

And so, we need to be thinking about how…

TALEBLU: And how many of them, just to your point about AI, cite these sorts of stories in their press?

MEIZLISH: Right. And so, I think this is because there's obviously a need for greater – maybe we call this literacy and education by the reporters who might be relying on – on AI outputs as trusted information. But I have real concerns where some of this AI-generated reporting that's pulling from state-backed sources might be then used to manipulate the environment in these event contracts, especially if we have automated bots that are placing rapidly bets that are impacting these event-contract markets. And then downstream from that, we have impacts in broader markets with more liquidity. And then we can actually see around financial institutions or commodity pricing soaring. Something that's downstream in the material world outside of these event contracts, and it all stemming from the information space that's being generated by AI.

TALEBLU: What about, just as a piggyback on that, to go back to that architecture you mentioned on the plus stablecoin, what is Iran able to do in terms of terror finance with this stuff? I mean, yes, you know, terrorism is not one of the major justifications of the president or the Israelis for this conflict, but no doubt. I think if you're looking at the Iran threat matrix as an architecture or a wedding cake of threats, support for terror has been a big one. It's been one of the hardest for U.S. governments in every era, now in the digital and cyber era, to be able to crack down on. How is Iran using AI for terror finance?

MEIZLISH: So, I think this is another instance where we can – we have to imagine what's possible, right? So right now, we're – we're living through this new moment where AI tools are coming online. So, I haven't seen anything in – in Western governments where there's enforcement actions that indicate AI is being used by the Iranians. Really, this is for the North Koreans who are using AI to manipulate their appearance in job interviews so they can get into different systems for corporate espionage purposes. But with respect to Iran and terror finance, I think we need to be looking out for a rise of crowd – crowdfunding, sham charities being set up, rapidly created accounts that are creating donation pathways for terror finance. When you look at blockchain analysis firms like Chainalysis, TRM Labs, Elliptic, they all produce great reports that look at crypto in the illicit finance space. And we just see that there's billions of dollars every year that's moving to Iranian proxies, right?

Like a billion dollars here to Hamas and Houthis, certain accounts being shut down. So, it's – it's happening and it's going to happen more because there's an ease by which these systems can be set up. And so, this is going to require a lot of partnership across jurisdictions between governments. And I think that there's a necessary marriage between these two topics of AI and crypto where they're two distinct things, but they also share a lot in the sense that the regulators who are responsible for actually implementing regulations and going and enforcing against them don't have the education that they need from a technical perspective, and that's going to get in the way of shutting down a lot of these accounts and holding bad actors accountable.

TALEBLU: So harder to do – do due diligence then. They don't have that kind of training.

MEIZLISH: Yeah. I mean, for blockchain analysis in part – and I know this is the AI Expo, but for blockchain analysis in particular, there's a high level of sophisticated training that's needed so that you can ensure when you go and seize funds and you freeze them, that you're going after the right wallets and accounts that are being blocked rather than someone else's, who, you know, on their long string of digits for their – their crypto wallet, you're getting incorrect and not blocking somebody else's funds. So, the same thing, I think, in the AI space where we are dealing with some novel challenges with respect to freedom of expression, right? Free speech. There's constraints here also with respect to U.S. sanctions, right? So, think about bad actors who might be proliferating models – AI models that are meant to actually be open source in nature, pushing a narrative. With respect to U.S. sanctions, right, we have limitations.

There's express prohibition on regulation of information materials, right? So that's codified in statute. So, where the United States may want to take action and say sanction a lab or sanction a model, something that could proliferate in the open source, we have prohibitions that might get in the way of us doing that. And so, I wouldn't be surprised if Iran, when the dust settles and there's – there's more resources available to them to build something like this, that they'll do it. I'm sure that the Chinese will be doing it or already are. Russians as well. So, there's that marriage there that I think we need to understand from a legal perspective. What authorities need to be updated and what training do we need to provide to law enforcement regulators so that they're actually prepared to handle these challenges, more than just talking about the thematic threat?

TALEBLU: You know, you touched on three other countries that at FDD, we happen to call, when you marry them with the Islamic Republic, the Axis of Aggressors. Other people have different names for them, the Axis of Authoritarians or the Axis of Revisionists. Now these are predatory anti-American authoritarian regimes: Russia, China, North Korea, Iran. Iran actually right now being the one that's weakest, economically, socially the most divided, and also militarily the only one thus far without nuclear weapons. And Max, I want to get to you talking about that in terms of the domestic war in a moment, but our other friend Max just had to mention something about crowdsourcing. I think you a few months back wrote prior to the conflict about Iran creating websites for crowdsourcing to actually see who would put a hit on the president of the United States. Can you just talk about that crowdsourcing effort for one sec, and then we'll go talk about Iran's integration with the other powers?

LESSER: Yeah. So, I the honor in attributing actually a website – a – a terrible website that was essentially giving the impression that it was crowdsourcing funds for the assassination of – of President Trump. And it was unclear who made it. And what we did at FDD, we used open-source intelligence and cyber threat intelligence to actually identify the specific man who created that website. And we then found that he had ties to the Iranian government. Specifically, he was an employee of the IRIB [Islamic Republic of Iran Broadcasting], their state broadcaster. And what I would say is it's unclear. He said he had crowdsourced or crowdfunded $40 million, and it was actually kind of sad. You would see people who would like – he shared – people would share like the deed to their farm and stuff like this. Like he was triggering people to give up used cars and things like that. But the $40 million number, was it real?

Was it not? We don't know. But the great thing about, or the terrifying thing about that, when we think about information warfare, is it doesn't matter if it was real or not, right? Some wacko in the United States who sees that, well, first of all, if they're thinking of doing that in the first place, they probably don't need the financial motivation, right? But it could potentially mobilize and motivate people. And all he had to do was spin up a poorly made WordPress website. He made a video game where you could shoot Netanyahu and like whatever, and it was made on a children's programming language called Scratch. I don't know if anyone here – when I was younger, I used to make video games on Scratch. I mean, it was childish, but it was potent, right? And one of my interns at the time flagged it to me because it was penetrating the information environment. She saw when she was doomscrolling, right?

So, and another thing about crowdsourcing and crowdfunding, that's one application of it in information warfare, right? The illusion of crowdfunding to try to create a bounty to motivate people to do something violent, right? But then there's also – Iran is very good at this – where they will actually crowdsource participants in their information operations, right? So, they will put out a call domestically for people who are motivated or ideologically aligned to create fake accounts. And actually, we found a network impersonating Israelis during the 10-Day War sharing messages like, 'I'm losing all hope,' like demoralizing messages, messages meant to spread fear, uncertainty, and doubt. And we found their Telegram channel. It was public, which just goes to show they had terrible operational security, which makes me also think that this might have been a non-state actor who was facilitating this, right? And literally to speak of AI, and tie it back to AI, we saw and we captured the archived videos of them instructing their participants on the Telegram channel how to use ChatGPT to translate their messages from Persian to English, right?

This is not hypothetical. And what I would say is it's like also – it's also, I would say, somewhat unremarkable because these tools are so accessible, right? And they're so easy to use for anyone who's used them, which I would imagine is everybody in the room at this point. We know how easy it is to prompt them and things like that, right? So, they are the masters, and this is not the first time that they've crowdsourced participants. They do this domestically too with their Basij paramilitary force. They do a lot of coordinated influence operations and psychological operations against their own people as a tool of domestic control. And you best believe it, they're using Telegram and other channels on their sort of domestic Telegram called *Eitaa* to crowdsource people. And we even found a YouTube channel that was associated with this – with the Basij force, which was teaching participants how to use AI to create content, right?

This was before the Lego videos. So, they've been using crowdsourcing and AI, and those two things go together because ultimately when you're crowdsourcing participants, they might not be graphic designers. They're certainly probably not going to be psychological warfare officers or – or marketers or digital marketers or people who actually know how to make that, but the AI, it just makes the barrier to entry to actually make something somewhat convincing or compelling, or at least something that doesn't have typos and grammar errors, it makes that barrier to entry a lot lower.

TALEBLU: And what about now the information war at home? Russia and China have for years now reportedly been assisting Iran with facial recognition software, now this thing that is called –sometimes jokingly called the halal internet. It's basically the national intranet versus the actual internet, which they've shut off now again for, I think, 67, 68 days inside of that country. What about America's authoritarian adversaries bolstering this weakest link of the axis of aggressors? We saw just again, the first shutdown of 2026, 20 days under a three-and-a-half-week protest in January 2026, where reportedly 30 to 40,000 were killed. What's the – what's the incentive there for America's great-power competitors to be helping the Islamic Republic, and how is Iran really wielding any kind of assistance that it gets, more in the digital surveillance space and also cyberspace, against an increasingly dissatisfied and dissenting population?

LESSER: That's a fantastic question. And I want to say this first: Iran has been trying to control a Persian-language information environment for many years. If you look, they were jamming Radio Farda broadcasts, which is sort of the Persian-language Radio Free Europe or Radio Free Liberty. They were jamming those broadcasts going back years to try and control the Persian-language information space. That's not just…

TALEBLU: Threaten the families and journalists?

LESSER: Yes.

TALEBLU: Abroad and at home?

LESSER: Not just the internet, radio waves too, right? I think they even did something – I forget what – to block Persian-language broadcasts coming out of Los Angeles, right? Like so, all of these things. But you brought up a really great point, which we're talking about their offense, which is honestly increasingly skillful and, in some ways, very skillful.

TALEBLU: If you had to give it a grade?

LESSER: I would say the Lego videos, I would give an A+. I mean, honestly, again, who here has seen them? A lot of us have seen them and things like that. And I know anecdotally they're resonating with people, right? So, I would give that an A+. But let's talk about defense because that's an important thing too. And guess what? They don't have the same free speech protections and civil liberties that we have in the United States. And the most effective defense, which is something that we rightfully in America would never tolerate, is censorship, right? That is their defense. Their greatest defense that they have is censorship. And that is what distinguishes us, but it also makes us more susceptible to attacks, right? And we have to, right, like we have to figure out the way to combat them and play defense while protecting civil liberties and free speech.

That's absolutely essential, right? And there are ways we can do that, which we can get into later, but Iran doesn't have to care. So that's of course why they shut down their internet. Because not just they don't want us to penetrate their information environment, they don't want their people to be able to mobilize themselves, right? They don't want their people to be able to organize themselves. And you brought up a great point. It's not just Iran doing that. Russia famously is doing that. They have this app called Max. They're making it compulsory. They're cracking down on VPNs. They're cracking down on WhatsApp. They're trying to tighten their grip on their domestic internet and the domestic information environment. China famously has done this for a very long time, right? You know, the famous stuff with them in Google, with the great firewall, things like that. And as you said, they're assisting Iran.

Well, guess what? They're not just assisting Iran. They're also exporting their surveillance tech and their AI facial-recognition tech, right, that is an AI-enabled technology, to other aspiring authoritarian countries like a small south Caucasian republic called Georgia, where they're exporting their facial-recognition technology so that that want-to-be authoritarian regime – they're just wannabes, they're actually not very good at it, but they're trying – can tighten their grip on domestic protests and quash those as well. So, it's not just them assisting Iran. Any aspiring authoritarian country throughout the world will get ready and welcome assistance from these ideologically aligned authoritarian regimes like China and Russia.

TALEBLU: So when we talk about an arsenal of democracy, America being able to militarily support its partners, politically support the systems that are free, that are open, there is literally this capability, or the advocacy of the axis, the ability to shut down the internet, the ability to control populations, to repress them off the street and repress them in cyberspace. This is literally one to one, that's amazing. Max, I want to give you an opportunity to weigh in on just this entire cocktail, as you and the one we first mentioned: North Korea, China, and Iran. Anything else to weigh in here on this architecture or on this space before we pivot?

MEIZLISH: Yeah. I think it's fascinating to – to listen to this picture that Max is outlining. There's real alignment, right? And that's, I think, the point of FDD's work on the Axis of Aggressors: to show alignment amongst these adversary countries, showing how their capabilities are aligned, how they're transferring technology in a very strategic way. The interesting thing, and this definitely relates when we think about our context with Iran, the effectiveness of U.S. sanctions. A lot of people will argue, "Well, sanctions, they're an old tool. They're not effective." Oftentimes I will ask if we're really using them well, right? Are we resourcing parts of the government that are responsible for executing those mission sets? And so, the answer to that, in my opinion, is no. And the reason why I'm raising it here in the context of the axis is because we need to see this growing alignment for what it is, and we need to see how in the financial space there's growing alignment as well.

Right, so, there's alternative financial infrastructure and architecture for payments and messaging systems that are being developed by our adversaries. China has developed a system called CIPS [Cross-border Interbank Payment System]. Russia has SPFS [System for Transfer of Financial Messages]. Iran has SEPAM [System for Electronic Payments Messaging], right? There's all of these different systems that connect adversarial countries financially. And so when we think about sanctions as a tool of economic statecraft, something that in the ideal world will be used to great effect so that we don't have to find ourselves in the midst of a war that's going on for some amount of time – we all know when it'll end – we need to think about that greater integration, how U.S. sanctions will become increasingly ineffective if we're unwilling to use them now to shut down these growing elements of collaboration where our adversaries are actually tightening those bonds now, developing infrastructure among them.

TALEBLU: I want to say something provocative now. Get you guys to respond, offer one brief moment for a policy recommendation about what we can do better, and then open it up to the audience where I think we'll have a traveling mic at some – yes – because we do have, I think, a hard out at 30 or 45, if I'm not mistaken, and there's a lot more of you, and we want to make sure that there's time for productive Q&A. Now here's the provocative charge, if you will. Sometimes in foreign policy, we have to distinguish between the signal and the noise.

And the Iran war, absolutely it's costly, it's challenging financially, politically, militarily, morally, every which way you slice it, it can be a challenge. It's a kaleidoscope. But actually, given all the challenges you guys just raised today and how much bigger and broader this domain of warfare is, this tool is, and the other much larger, more powerful state actors that we face as the West, but also as the United States of America, I think the Iran war is the noise. The signal is the capabilities that have brought it to the fore and that will far outlive, you know, even if there's a resumption of conflict. As an Iran watcher, am I putting myself out of business or is this – is this the right diagnosis?

MEIZLISH: Well, I think that…

TALEBLU: We'll be in business for some time?

(LAUGHTER)

MEIZLISH: I think we'll be in business for some time. The threat's not going anywhere, right, especially from Iran. If we don't think that there's going to be a change in the regime, then all these problems that we're describing are actually the same as they ever were. There's the greater capacity to inflict harm militarily, but this kind of gets to, you know, where I think we need to go as a country and see China as the – the central actor in this developing axis, this developing cooperative organization between bad actors who are acting against the US and our allies. In my view, I would want the war against Iran to be a proving ground for all of the capabilities that the United States actually has and can deploy. And unfortunately, I think that we're seeing that's not actually the case right now, right?

So, there's been significant efforts to attack the enemy militarily, right, directly targeting Iran's military assets and some elements of critical infrastructure and heavy industry. But from a sanctions perspective, most of what we've seen is actually very similar to what we've done in the past. There's some escalation there, but not really an extension to the third-party enablers. So that's aimed at China. And I think there's a very similar thing here in the information space, where it should be a proving ground for all of the capabilities that we can bring to bear because the world is watching and China is watching how the United States responds. And I think that we have a lot to be concerned by if we're not able to utilize those tools for whatever reason in this conflict and think for some reason that we'll be able to do it against a larger, more powerful and impactful adversary.

LESSER: So, I want to end with a question again. Who here has seen the official U.S. response to the Iranian Lego videos? Because it hasn't existed, pretty much. I think somebody might have mentioned it at a press briefing. So, correct me if I'm wrong, Behnam. Khamenei. Khamenei, right?

TALEBLU: Khamenei, the son?

LESSER: No, the original.

TALEBLU: Khomeini, the OG.

LESSER: Khomeini.

TALEBLU: The founding father.

LESSER: Do we know – do people here – are people here familiar with how he spread his ideas throughout Iran from outside the country? Tape recordings. Tape recordings, right? Propaganda, information warfare, audio, extremely powerful, extremely potent. It was one of the catalysts for the revolution in Iran. America needs to wake up. We need to start putting up a fight in the information war. That's the most broad thing I can say. We could talk about how to implement that on a policy level. Yes, the DOD is doing things to try and get its game together. They're doing a lot, but we need to move faster. We need to – we have to – to learn from our adversaries, right? And the things that they're doing, right? OK. Not the domestic censorship stuff, right? That's a big no-no. But the Iran Lego videos, why are we not taking our talent, right? I went to a high school for the arts. I know that being a creative person, that's talent, right?

Unfortunately, you can't always train people to do that. We have to get a reserve of our talented people in America, and we need to get them to join the fight. We have to motivate them to join the fight, right? Which I think people might say, "Well, oh, culturally you think about people in entertainment and maybe politically they're not aligned"' But it's an interesting analog and it's very true. So, a lot of what I do touches on cybersecurity as well, right? I do cyber threat investigations and cyber threat intelligence. When you look at the cyber community, a lot of those people you wouldn't obviously think would be interested in national security, right? Maybe a little bit more on the fringe, they're playing a lot of video games, right? This is sort of painting with a broad brush strokes, but it's true. When you go to any cyber conference, it's this weird mix of sort of more fringe sort of cultural and political stuff and national security.

We can do the same thing in the entertainment space. I know that there are many Americans deep down inside, no matter how much they backtalk the government or whatever, they would. If you told them, "This is an important mission. You know, we need to do this. This is essential for our national security," I'm sure you would be able to. And the time is now, because this administration has a lot of people who have a lot of experience in entertainment, right? So, they should understand the value and the importance of information, of media, of information warfare, and it's time to wake up and actually start putting on a fight in this domain.

TALEBLU: Amen. I do think we should clap for that. But – but that aside, to both of you, and then we'll open up to Q&A. Ideally short if possible. Besides that fight in cyberspace, information warfare, AI, what's one specific policy gap perhaps brought to you by the Iran war that should be setting off a red light that you would like the USG to address by the end of the year, and thus far they haven't? I agree wholeheartedly. I would love to see an American counter to the Lego video. And we have a great monograph, I think out last year or two years ago, I think called
"Cognitive Combat," run by one of FDD's other centers, just about the information warfare domain being treated as a domain of warfare. So, I highly recommend that to folks as well, but Max and then Max, and we'll go to the audience. Again, one specific policy gap to close.

MEIZLISH: Yeah. So, since I only have one, I'll go big, right? So, we need to think about actual resourcing for the agencies that are responsible for fighting these fights. So, as I've said, my background is in sanction, right? I used to work at Treasury doing sanctions investigations and enforcement. And just the other day, the comptroller from the Pentagon testified before Congress and said that in just two months of fighting this war against Iran, we spent $25 billion. That's probably on the low end, right? A conservative investment: $25 billion in two months of fighting war. I did some back-of-the-napkin math to look at Treasury, the agencies responsible for sanctions, financial intelligence, illicit financing, these things. Over the last 10 years, the last 10 years, they've been funded $3.4 billion total, compared to $25 billion that we've used to fight the war in two months. So that means that in one week of fighting the war against Iran militarily, it's the equivalent of spending 10 years' worth of funding for these agencies in the illicit finance space.

So, I think that probably extends the agencies that are responsible for information warfare, for actually combating aligned AI technology, for putting out better alternatives and ensuring that there's a proliferation of good, reliable information from the West and combating the malign influence. So that's the number one thing that I would push for, and it requires a big change, and it requires ground-up support for legislators to understand that we actually do want our government funding this work because it's more valuable and it can prevent us from hopefully fighting wars down in the future.

TALEBLU: Here, here. You know, pick your favorite munition. If it's the MOAB, if it's the delivery vehicle like the F-35, compare that to the cost of any of the things that you guys have mentioned today, even on the older school stuff like Voice of America, Radio Free Europe, all these
"antiques," and just see how much one of these munitions are, how much more of these platforms are, and how much one of these agencies or organizations. It's really mind boggling. Max?

LESSER: Yeah. So, there's a lot of things that I can say and obviously it's kind of murky. It's hard to tell. I thought Radio Free Europe was cut, but then one of the journalists reached out to me and I was like, oh, maybe it's not. Like it's always hard to figure out what's going on in that space. This is why I said the biggest – from a policy perspective, America needs to have a coordinating body or a coordinating individual. We need to coordinate. We have some stuff going on, or a lot of stuff going on in DOW or DOD, right? We have some stuff going on in the IC. We have stuff going on in State with public diplomacy. We need a coordinating body, and there is currently a director of Cognitive Advantage in the NSC. If that's where it's going to sit, and if him and his staff, if they will be the coordinating body, that's it.

But we need to have a vision. We need to have a vision for what is our grand strategy in the information warfare space. That first, if that's going to be the congressional committee or whatever. And then we need to have somebody be in charge of it and somebody who can make sure that all of the different branches of the U.S. government who are involved in this are executing that mission and are executing that vision.

TALEBLU: It's a big picture, big ask. I hope it gets implemented. We can turn it over to Q&A and we'll start here on the front with this gentleman, if you wouldn't mind saying your name and identifying yourself and then ask your question, hopefully an inflection point at the end.

COMBS: Probably more directed toward Mr. Lesser. I'm Cody Combs, technologist and editor for *The National*. We've got several stories on the Lego AI videos. We spent a disproportionate amount of time trying to get comment from Lego and other media outlets as well. The closest we've gotten was from the Middle East division of LEGO, which is Denmark-based and they've said no comment. Their name, image, and likeness is being used, to say there could be a legal case to be made or not. But why do you think LEGO is so reticent to weigh in on this?

LESSER: You know, it's hard for me to say because I'm not obviously involved in corporate strategy at LEGO, though maybe – maybe that'll be a future employment idea. But I mean, look, I mean, honestly, it's hard. It's like, well, what can they do? Let's say they sue Mr. Explosive, I think he likes to call himself, the head of Explosive Media. I mean, as you know, it's hard to enforce that, whatever. But look, I mean, I remember – it's funny you actually mentioned that because in 2020 when the PRC put out this Lego video about sort of dueling, a statue of Liberty Lego versus the China Lego, which was very low quality, they did respond. So, it's unclear. Like I'm not sure why. Maybe because it's such a polarizing topic and they don't want to weigh in on it, obviously because there's been a lot of, I think, personally, very misinformed and misaligned domestic pushback against U.S. efforts to combat information warfare.

It is – it is a hot topic politically, and maybe I'm just guessing that's a reason why. But I think when it comes to information warfare, like what I always say is like – and I always try and discuss it in the most apolitical way possible, because it shouldn't be politicized. It's not a right-wing issue or left-wing issue. It's a national security issue, clearly. And so, I'm not entirely sure, but it's a shame that they don't feel like they can discuss that because obviously you would hope that they would come out and at least say, you know, "This is bad. You know, this is not good."

TALEBLU: Max, do you want to weigh in on that?

MEIZLISH: I imagine they also are concerned that if they comment strongly, they could be susceptible to hacks and some sort of malign attacks, but that's just conjecture.

TALEBLU: Just the cherry on that sundae, I don't know if any of you guys live here or traveled here for the conference, but if you go to any of D.C.'s two airports now – and I've been a lot traveling since the war – Dulles Airport and Reagan Airport, there are two big Lego displays at each airport. And every time I swear I walk by it now, I can't help but think of these videos.

(LAUGHTER)

TALEBLU: That doesn't strike me as a corporate strategy, to think of Explosive Media. Any other questions? Yes, right here, sir.

EISENBERG: Thank you. Seth Eisenberg from DOD. I'm curious, sort of a two-part related question. In terms of like the sheer amount of bots in the social media space and fake engagement and fake amplification, like how much of the sort of amplification of some of these things do you, you know, see or feel are genuine versus fake? And then also in terms of credibility, right? When FDD does something, makes a move, its research is backed, but it's obviously true and you can go back and see where it's coming from. And then you have influencers on the other side that just spout B.S. all the time, get called on it, it doesn't seem to affect the credibility for the most part. So, is that a way to – I mean, it's a little nihilistic, but like does the truth even matter in that space, or is it just the amount of volume of stuff coming out from each side?

TALEBLU: To put a final point on it, does naming and shaming have any utility? Both you guys?

MEIZLISH: Well, I do have some thoughts on maybe how we can address some elements of the credibility, you know, with respect to digital ID, right? Ways in which we might be able to use zero-knowledge proofs, things like this that can preserve personally identifiable information in such a manner where you demonstrate to a platform that there is a real individual behind these accounts and maybe someone who can be held liable if anything were to occur. You can peel back the layers of that onion through legal process for doing so. That might be a way in which we could actually create more of a not so transparent–information space. I mean, I think there is a lot of value in people being able to speak openly and maybe anonymously in open society, but there probably are ways in which technologists, and maybe there's some in the room here, can think about these digital forms of identification and attaching some of those identities to social media profiles.

So that, to your point, when someone is just clearly spouting nonsense, the platform itself is able to deduce: is there actually an indication that there's a real person here? Can we go and have outreach with this individual? Can we refer this individual to some authority if they're causing some sort of material harm? So, from the policy space, I think that's probably a promising path forward, but (inaudible) you think Max?

LESSER: Yeah. So, you bring up a couple of great points. The first that I'll say is that, yes, inauthentic amplification and inorganic engagement is a tactic that is used in foreign malign influence all the time. And what I would say, you asking a question that's very difficult for me to answer because unfortunately a lot of the major social media platforms have made it much more difficult for somebody like me to investigate them. Especially we work at a nonprofit, right? We can't spend – how expensive is the X API now, right? It's extremely expensive. And Meta used to have a tool that was for researchers called CrowdTangle and they took that down, right? Again, a lot of that is I think because of the really ill-informed and kind of misdirected pushback domestically against – against countering foreign malign influence, but that is a tactic. It's hard to say with this.

Some of the – some of the YouTube channels and things like that have been taken down. It's very fractured, things like that, but that is a tactic if people use. I wouldn't be surprised if they are using that here, and different indicators that you can look for. If you see a video or a channel that's created recently, there's not a lot of maturity – account maturity but you're seeing it's getting a very high level of engagement, that's an indicator of possible inauthenticity. But then you would have to do sort of large-scale data analysis, which we could do if we had access to that data, which is very hard for us to get access to that data. We could do it and we could look at different indicators of inauthenticity and map that out. Now the second question, which is more important: there's a famous saying – I forget who said this, some people probably know – like 'facts don't care about your feelings.'

Well, feelings also don't always care about your facts, right? That is an important point that people don't bring up. And I'm not just saying that because it sounds good. There's a whole book called *Narrative Warfare*, by – I believe her name is pronounced Ajit Maan – and she's a PhD, she got a PhD in literature, and she talks about narrative warfare. And I believe this book, it's taken very seriously in the community of people who research and study information warfare. It's called *Narrative Warfare*. And her first piece of naming she talks about is narratives are more powerful because that is actually what shapes people's beliefs and behaviors. And those narratives – facts play a supporting role in the narrative, right? You can think about even like people's political beliefs or whatever people's beliefs are. If something is proven to be true or proven to be false, one might still carry on to that narrative because that's a crucial part of somebody's personal identity, right?

It's deeper in the part of the brain – and I'm not a neuroscientist – but the part of the brain that is lighting up is not the fact part of the brain, right? So, I would say it doesn't matter, really. And that's like, for example, I think in one of the Iran Lego videos, I think a couple times they showed like down U.S. jets, or they showed the capturing – one Lego video somewhere showed them capturing the U.S. person who – the U.S. pilot who – who was stranded and then rescued. And I think they were – they were pressed on that, but it doesn't matter, right? Because the general narrative that we, Iran, are being oppressed, or we're victims, and like, it doesn't matter. And that's why I think it's important that America, we just tell – we have to tell a story that's compelling. And we can tell that story. They just murdered tens of thousands of their own people.

They've been chanting death to America for decades, right? We have a story to tell. Why aren't we telling that story, not just to our own people, but to the world? I don't know.

TALEBLU: This is great. This is a vote recommendation on top of these other great recommendations the panel's mentioned today. I think it's called *Descartes' Error*, you know the – the Cartesian line: "I think, therefore I am." The book is about I feel, therefore I am. And imagine if you lose the feeling part of your brain – and actually, again, not a neuroscientist, but it actually can impact the rational decision-making part. And we have to know how to value something. There's no doubt that the U.S. government can detect, defeat, and destroy, but how does it know which one to do first, in what order, against what target, and then how to magnify that. We're not just automatons. We live our life based on a whole series of values. These narratives in the media, in social media, on newer media, they're the ones that are now trying to change our ideas through changing our feelings.

So, it's a great book. Any other questions before we slowly adjourn today? I think we have – yes.

SOTHAN: I'll try to keep it brief because I think you guys are wrapping up. First of all, thank you for what you just said, Mr. Lesser. Because I've been thinking that for a long time and I'm wondering why there's not more activity on that front with creative information warfare. But this question's more for you, Mr. Meizlish. Am I saying that right? So, I was recently reading – oh, sorry. Michael Sothan and I work on a congressional campaign. You guys should all vote for Adam Dunigan for Congress. I was recently reading a book by William Polk, who's kind of considered – he's deceased, but a famous diplomat, kind of a Middle Eastern, Iran expert. In the opening section of that book, he was essentially talking about what he sees as the futility or ineffectiveness of sanctions in that conflict. He was basically arguing that it negatively affects the general population much more than it does kind of the power structure or the elites, because they always find a way to circumvent it through their networks.

I'm just curious what you think about that. Do you think it's because we're using it in an ineffective way, or do you think it's just generally ineffective at certain levels of the government?

MEIZLISH: Sure. So, I literally talk all day about this, but to keep it brief, the idea, at least from my perspective, is that for the most part, the United States is not employing economic sanctions in a smart way, and it never really has. This is a – a extremely coercive tool that can be used to great effect to compel some change from adversaries, but so often what we do is we use a trickle approach where we have a limited designation here, a couple months later another designation, or we – what we'll do is, like in the case of Russia, we sanction a section – sector of Russia's economy, and then six months later, another sector of Russia's economy, when we know how critically important all of these various sectors are. And so, we have a slow approach to imposing these sanctions, and then that's how you get new things coming years down the road.

So, if we really want to use these tools to greater effect, what we should be doing is maximizing their impact at the outset. We should be using them in a much more aggressive way initially, especially before a conflict emerges, so we can actually shape adversary behavior and limit the extent to which they're able to benefit from enablers who are supporting them. There's also other tools outside of sanctions. So, I've been pushing, especially during the course of this war, Section 311 of the USA PATRIOT Act is a tool that allows the United States to cut off a bank or an entire jurisdiction or even limit activity with respect to a class of transaction. And so, there's all these different special measures and you can prevent other adversaries from access to the dollar, or you can require that correspondent banks do enhanced due diligence for various things.

So, there's all these other tools that can be used to greater effect. And I think that for the most part, when people are talking about sanctions and saying that they're not effective or they don't work, I would think about it more like, would you ever say that a bullet just doesn't work? Right? You wouldn't, because it's a tool, and it's a tool of warfare and it can have a coercive effect, but if you're not using it strategically, if you're not actually firing multiple shots and you're firing just one here and then another shot six months later, how can you really expect your adversary to go down? Right, so, the better thing to think about is are we utilizing sanctions well from a strategic perspective? And then from the resourcing perspective, I cannot emphasize this enough, the agencies that are responsible for administering those sanctions are small potatoes in terms of the U.S. government.

There's just no replacement for actual resources.

TALEBLU: Yeah. Just to close on this, unless there's any other questions? We have a few thoughts I want to respond to, just because FDD has been part and parcel of the Iran sanctions debate for a very long time in Washington. You may remember there's always – first of all, there's always legally and politically there is no sanctioning of humanitarian goods, but unfortunately the Islamic Republic abuses humanitarian exemptions. In the “gas for gold” scheme, which is the biggest sanctions-busting scheme in history, tied to the Obama administration, with the Islamic Republic abusing a loophole that existed in the Iran sanctions architecture in about 2012, for example, you saw the Islamic Republic literally abusing this with its humanitarian trade with Turkey, for example. Also, given, you know, the regime being able to get goods on the black market, when it is still able to be connected partially to the international financial system, in what became the legal architecture under mid to late Obama that later on was resurrected by Trump – that was later on called max pressure – that legal architecture and its first iteration, you saw the Islamic Republic choosing its imports because of what it could gain on the black market.

So not food, not medicine, actually choosing to bring in lipstick, luxury goods, cars, for example, stuff that they can increase the price on the back end for significantly. Same of course with all these countries that used to purchase Iranian oil: China back in the day, Japan, South Korea, India. These monies are there, locked up in national currencies, not supposed to be developing interest, and Iran could be using it for humanitarian goods and medicine in those countries. Iran chooses to let the money sit there and have the population atrophy in the hopes of playing high-risk, high reward against the West to get that money as part of a larger deal. And it does so by being willing to sustain conflict for 40 days against a regional superpower and a conventional superpower in the hopes that they get tired first, and then they get the cash and they can go put the cash back into things that the conflict was started for in the first place.

So, see us after about the Iran sanctions lecture, but I want to thank everybody for coming today. It's a real pleasure and enjoy the rest of the conference, and a pleasure to share the stage with two really bright analysts on a really key emerging topic. So, thank you.

END