The following is taken from a panel discussion at the recent Mauldin Strategic Investment Conference. It was called.

Conflict Driven Capex: The Investment Implications of Dual-use Technology

Panelists were Marvin Barth, Karim Hijazi & Erik Bethel. Moderator: Renè Anino

I have included only the parts relevant to the idea that we are already at war. Yellow highlights are my emphasis.

Renè. ... the adversaries in this conflict environment know one thing that the most important and powerful weapon that the United States has is our capital markets and the resiliency of our economy. And so if they wanted to take down the US-led Western Alliance that they have to attack us in market space rather than kinetic space. And I think that is clearly what is going on with Putin, with the Houthis, with potentially what's going on in China and in Asia.

... Erik, we always talk about that we are in this conflict environment and you always say, "Hold on, hold on, hold on. Step back. You say we're in a conflict environment, but does anyone else know that we are in a conflict environment?" And I think we need to establish that first. So Erik, give me a few thoughts on where we are in terms of the landscape.

Erik. We live in, let's call it the matrix. Most people are living in the matrix and they're oblivious to what's going on. They're buying the latest Kylie Jenner product and they're following tennis and they're following basketball and they're living their lives. Maybe gasoline prices have gone up a little bit. Food prices are going up, but they haven't popped out of their pods, so to speak. Every so often somebody pops out of their pod and they see the world for what it truly is, and it's very frightening. It's my God, oh, I'm so skinny. Oh, I've got a battery. I'm a battery. So people need to wake up and understand the world around them. And here's what the world looks like. We've been fighting a war that's unseen at the very least for the last five years, but it's gone on longer.

And the war is primarily, the war is now war between the Axis powers and ourselves. The Axis is China, Iran, Russia, Venezuela, Cuba, North Korea, et cetera. The greatest of these is China. And China has been very surreptitiously eroding the power of the United States. The headline of course is intellectual property theft, but what about the wholesale elite capture of our institutions of Wall Street, of corporate America? Find a company in America that neither sells something to China, takes money from China or produces in China. And because China has now a stranglehold and leverage over corporate America, they have a lot of sway. China is also importing fentanyl by way of the APIs, the precursors to fentanyl through Mexico. And so we've hollowed out our industrial base, which is the topic of today's conversation, and they've given us back fentanyl. Thanks guys. Meanwhile, I talked about this earlier, half a trillion dollars a year of intellectual property theft for at least the last 15 years.

People are probably unfamiliar with this term, but United Front activities, which is China's global spy ring, which has infiltrated our universities, it's infiltrated our national defense labs, et cetera. China is weaponizing space and creating satellite killers. China is creating saboteurs in the United States. We recently found an illegal bio-weapons lab in California about six months ago that had all sorts of biotoxins. And by the way, it was located 45 miles away from a major Navy installation where we train our fighter pilots. I could go on and on, but I don't think people realize the magnitude of the situation that we're in.

And so we are in a version of 1937, 1938 Europe. The storm clouds are getting thicker and they're getting bigger, and the storm is coming. You just don't know when unfortunately, we're acting like we live in Atlas Shrugged or something, hurtling into World War III, but acting as if, well, there's no war, things are fine, and it's a very frightening place to be. ... if we are indeed heading toward some sort of conflict with China or the Axis powers, it's only logical that the United States is going

to retool and repurpose and reshore everything back here or to Mexico or to friendly allies.

Renè. Karim was very instrumental in discovering something called APT-one, which was the first nation state sponsored hacking cyber unit from China and Karim, look, you're deep involved in the weeds of stuff that quite frankly I don't think any of us want to know. But maybe you could just start by giving us some examples of what you see the adversaries doing to, Erik had a great word, degrade and erode the capabilities of the US and the West over time. What are some examples that maybe you're seeing that from not only the offensive side, but also what can we do in the United States from a defensive and offensive perspective? I've got this view that the Baltimore Bridge incident, for example, was not an accident. So give us a little bit of color in terms of what you're seeing tip of the spear where you are right now.

Karim. ...the most salient part of the conversation today when it comes to the nation state threat broadly speaking, is the use of cyber to facilitate a kinetic outcome. That's scaring everyone to death. And that is the asymmetry and the dual use of technology in certain ways to say, let me take something that fundamentally was bits and bytes and effect change at a water treatment facility, effect change at a power grid effect change on a supertanker going under a bridge. I don't know that, but let's call it that. Now, the problem with this is that fighting that is very, very hard because you're basically trying to battle what would be the equivalent of a missile that's incoming.

From a cyber perspective is that usually they'll use proxies, they'll use your computer, they'll use my computer, they'll use a naval computer, they'll use everything else that is the infrastructure of the very internet that we work with to facilitate that attack. They don't build their own networks for this. They use everything that's already there. So in destroying their initiatives, you're effectively destroying part of yourself. It's a little bit like a chemotherapy approach to a problem from a cyber perspective. It's extremely difficult. In my world, living on the private sector side, and I'm about as close as you're going to get to a Corsair or a privateer, which means that I'm given a certain latitude that is normally the mandate of the government to go and counter some of those activities in, as Renè said, a effectively offensive way.

And part of that is to identify infrastructure that they're setting up, pre-weaponized, or actively weaponized and dismantle it, or at least illuminate it in such a way that it nullifies it or it removes it as a threat altogether. Very hard to do because again, you're talking about a variety of other things, and I know I'm going to dovetail into other aspects of this conversation that are not just purely cyber, things like AI that have forced multiplied one individual to be many. And as FBI director Ray has said very clearly in several of his speeches recently, we're 50 to one outnumbered in China alone, much less the rest of the countrys out there.

So when you take 50 to one and then you take every one of those 50, and then you force multiply them with AI and possibly some level of quantum capability, we're in a fight of our lives frankly, to echo Erik's sentiment around this. I couldn't agree more. And it's something that's such a shadowy, mystical battle to most, it gets ignored because it's too complicated. So I know it's a doom and gloom story so far. It might stay that way for the majority of this conversation, but it isn't very, very, very deep and very wide problem as well.

Renè. ... Karim, you made a great point about being in our local networks. So Marvin, what do you think the implications are from all this in terms of what companies and governments are actually doing as a response? I mean, I think Erik's totally correct that guy on the street is more obsessed with Taylor Swift and what's going on on Instagram, but the guardians of the society do very well closely understand, and they have been advising both governments and firms on how to defend forward. So what do you think in practice is the solution and what's going on?

Marvin. Well, so there's good news and bad news to all of this. I mean, I think it's clear I'm 100% in alignment with both Karim and Erik on all this. I mean, I might switch the analogy to 1913, 1914,

because if we trade with people, we won't go to war with them. And we all live in a globalized, peaceful world now. All sound like familiar themes? Those were exactly the themes in the late Victorian area going into 1914. It was exactly the same as now. People were in this state of disbelief, as Erik described it, far more so than I think that they were in 1937, 1938. But the key point is both of them, the West was actually unprepared, especially America was unprepared for war. And I think the scariest thing about all of this is that a lot of the technologies that both Erik and Karim have highlighted, a lot of the methods of warfare that have already taken place are things that they can hit us with immediately.

So being unprepared is a real problem, far more so than it was in 1914 or 1939. The good news, however, is that whether it's coincidental, not the fundamental forces of economics have actually changed. One of the things I've written a lot about is that there is a very clear break in global production and distribution, investment patterns, everything. And you can see it in asset prices too, in roughly 2010 to 2012, but if you really want to pick one year it is 2012. ....

It is a large group of them in coordinated effort with China being the key one. The key driver here has just been technology. When it all of a sudden becomes cheaper to use a AI-enabled robot to produce whatever good you're doing, why not locate that right where your rich customers are in the advanced economies rather than a dispersed supply chain that is subject to all sorts of different disturbances. And oh, by the way, your robot never gets sick, it never unionizes or does any of these things. So that has been going on for 10 years. And Trump, Covid, all of these things have only accelerated. Now, I'm worried that to this earlier point, it's too late.

We are addressing this problem too late. But the good news is it's already fundamentally underway. A lot of these technologies are expanding rapidly. We are on-shoring more and more production. That's one of the reasons why people have been so shocked by how strong the economy is under higher rates. Well, this is a basic productivity boom. It isn't showing up clearly in the data yet, but I'm telling you it's there. That's why asset prices, the economy, everything is behaving this way. And so hopefully in five years, we will be in a better position for a lot of the problems that both Erik and Karim have suggested. The awareness of the problem plus the ability to diversify away from China and increasingly prepare for all the different threats, whether they be cyberkinetic or missile threats or otherwise, are actually moving in the right direction. My fear is we don't have five years. That's my big fear here.

Renè. I think the biggest casualty of the October 7th conflict in Gaza, setting aside all of the humanitarian disasters that have occurred on both sides, is the biggest casualty has actually been the credibility of the United States Navy. Because if you would have told me even nine months ago that we're going to put two aircraft carriers on each side of the Red Sea, and some guys in caves in Yemen are going to impair and completely shut down the Suez Canal and the Red Sea to commercial shipping, I think probably all of us in US arrogance would've said, "That's impossible. They will not do that."

So we've obviously failed with deterrence. There's clearly no maritime kinetic solution to this, and our adversaries, to your point, are only stretching the US Navy even further. I'll make one last point that arguably the most important factor in the disinflation post 1989 was not Central Bank and was not even really the global labor force shock, but it was the United States Navy ensuring freedom of navigation. So that has been, I think I've got to tell you, quite frankly, totally eroded and only getting worse. Is there a commercial solution to that problem there 'cause I think that's one of the most important that we can start.

Erik. ...don't misinterpret what I say as partisan because it isn't, but policymakers today in the United States are to some degree embarrassed to hold power, and there are certain policymakers that would just assume the United States be a one of many country, like a Belgium. There's nothing bad about Belgium. They make great beer. It's a nice country. The problem is, if you are one of many

country and you have $34 trillion in debt and you're adding a trillion dollars every a hundred days, it's not sustainable. So you need to first of all understand the situation that you're in, and then you need to wield power.

For the last, I would say several years starting in Afghanistan and then Russia and then Hamas and the list goes on, the South China Sea where Second Thomas Shoal is getting besieged every day by the Chinese Coast Guard. And for those of you that aren't tracking that, Google Second Thomas Shoal and the Philippines, and you're going to see Chinese ships water canoning little Filipino fishing vessels that are clearly inside of the Philippine exclusive economic zone, shooting green lasers at them to blind them. I mean, who does that, right? And so we're watching all of this unfold, and I fear that because we are in an election cycle, the policymakers are trying to tamp down any kind of global unrest. Now, this is again, my opinion and I don't want it to be partisan. When you signal weakness as an imperial power, as a hegemonic power, whatever, pick your analogy, your adversaries are only going to get emboldened. And what that does is it creates a very, very, very dangerous world.

So now let's take it to the Navy. I don't know where to begin. The Navy has a very difficult time building ships. You can't even throw... Even though you can throw more money at all the ship builders, Newport News, Huntington Ingalls, et cetera, we just can't build them because we don't have the skilled workforce, we don't have the supply chains, et cetera. Not to mention the fact that we're shooting down basically $300 drones with Tomahawk missiles, which cost $2 million, so the USS Kearny is exhibit A. And it's not that we don't have the capability of reducing the Houthis to basically rubble. I think it's that we lack the will, and that comes from the top. Now to your point about where we should think about making investments that are asymmetrical, where we're looking to find alpha, I think A, the military is having a very, very difficult time recruiting, B, Adding a trillion dollars every a hundred days is going to squeeze the defense budget over time.

If you take those two factors and combine them, you can only conclude, at least I do, maybe there are other people that are smarter, but you can only conclude that the future of war is going to be technological, not just cyber, which is Karim's specialty, but underwater drones, loitering underwater munitions, redundant communications, navigation in GPS-contested environments, logistics, and all of this is going to be, there's going to be this new influx of technology meeting the maritime domain that's going to be extremely important. ...

Renè. I was at one of these conferences and I finally understood the scale and magnitude of the proliferation of devices when it comes to the internet of things. And if, for example, if you go to an auto manufacturing facility and the robotic arm that you see that is required to be programmed by an engineer, that probably costs $250,000. Now with a large language model, that robotic arm is going to program itself, that going to $50,000 a cost is going to go straight to the bottom line of, for example, Ford, but it's also going to disintermediate labor.

However, with this proliferation of devices, you need a different scale of cybersecurity because if every device, every item that you see is linked, Karim, I think we think of cybersecurity now as antivirus still.

Like McAfee, and it's clearly not that. So maybe you could talk to us a little bit about what we can see in the physical and digital security space because without that, all the other stuff that we're talking about, robotics, autonomy, bioengineering actually becomes moot because if you don't have the proper security, actually we enlarge the threat surface rather than reduce it. But talk to us a little bit about that.

Karim. Yeah, you said the exact word I was about to use in this answer, which is threefold. It's pretty interesting. The first part of this is that people get wrapped around the axle when it comes to cybersecurity, to your point, because A, like I left off with, it's somewhat murky and nebulous and

esoteric and all that. It's really not. It's just speed. It's just a faster way of medieval warfare. What was once a feather and a knock at a fortress gate and a certain verbal password is now your two-factor authentication tools. It's exactly the same thing. It's just been digitized and recapitulated out in a faster, more efficient method. So history is our best feature for this kind of situation, for especially the investment side of this. We're now in a full-blown to mirror or echo Erik's comment in a new Cold War. We're back to Bond, but now it's technical Bond, it's new spies, it's new counter spies, it's new intelligence apparatus, it's new counter intelligence apparatus.

No, it's no longer AV. That is an arms race, indeed, Renè, that is now dead. This idea of being able to, I used to do this in my training sessions that antivirus is like a bouncer at a club. If you look like your ID, okay, come on in. I don't care that you're 12, you look like the idea. Come on in. And it's ignorant and it's unfortunately one of these technologies that needs to die. This castle moat approach to the problem is gone. The interconnectivity, to your point with IOT and OT, which is operational technology, which is tied to factories and refineries and water treatment facilities and everything else, the operational technology layer, which is unfortunately quite outdated, ... that is ripe for disruption, that is ripe for investment in a big, big, big, big way.

As is everything associated with the way intelligence is collected, refined and disseminated ultimately because it's happening at machine speed due to AI. Because now we're having to counter a psyop problem from technology that never existed. Even three years ago we never had this level of problem. We're now having to figure out whether an AI system is going to be convincing you of something as a human. The technology is now hacking humans versus machines, and this is where the world's going. We're moving into a place where the malware that is being deployed is smart enough to figure out how to manipulate you as an individual to do something to facilitate its end versus the classic hack the machine and do what you needed to get done. Those days are effectively over.

.... Maritime is a phenomenal spoke in the hub of many of these, but they all feed together back to your point about supply chain, which again, I'll shut up there because that's going to go into a tirade around supply chain. That's our biggest and most prolific attack surface to end on where we started Renè.

.... There was then a discussion about robotics and the implications for the workforce, about energy and the transition to green and a lot more that doesn't fit with the theme here ....

Renè. ... "Erik says the average American is not aware of the dynamics." What do you see likely happening going forward? And to put in another question, "What is your percentage estimate of the number of sleeper disruptors crossing the southern border ahead of the election?" Erik, Karim, any ideas? Because we've got all these protests, for example, on college campuses of, for example, people at NYU wearing NYU hats who are actually not NYU students.

Karim. I think we have lost Erik. I'm not sure. No, it's an interesting question. There's zero question back to the disruptors coming over the border. I mean, look, it's absolutely an impossibility that there's not a huge influx of people moving in with the intentions to destroy, disrupt and a variety of other things that are going on. I think as it relates to the quantity and exactly how they're going to be affected, that is a very good question. I think we've seen some of it already. We've got a big problem when it comes to the access to everything. We've been talking about it through the entire conversation so far. But Renè, if you can go back to the first part of the question, could you repeat that because I think we lost track of it

Renè. What was your percentage idea of what types of adversarial actions inside the United States would potentially happen?

Karim. Yeah, I mean look, there's this old notion from an attack standpoint that it's a staged effort. Part of what I had been alluding to, which is they're going to go after a certain aspect of our

infrastructure, which I guess in the last two, three weeks we've been hearing about it continuously from the FBI, the fearmongering a little bit. I'm not trying to say it's wrong, but a little bit of it, they're going to come after us, there's going to be this attack, that we're going to feel it. That's just part of it. And I'm the cyber guy saying that actually that's just a very small part of the equation. It's going to be a ramificated effort across a variety of different groups. If there are indeed sleeper cells, if you want call it that, eventually going to take kinetic action when something affects us in a distractive way cyberwise, that's a very high likelihood. When is the question. I think anyone could guess on that. That's a tough one. I'd be simply guessing if I were to give anyone indications there.

Marvin. I think there's a related point here to exactly what Karim was just saying that I think is important for investors to think about is there was this very popular book a few years ago by my friend, Marco Papic, called Geopolitical Alpha, and it puts forward a very classic international relations constraint-based framework for thinking about investing through geopolitical risk, which is frankly what we're talking about here. As Karim just alluded, there's a lot of different things that you may not have been thinking about that the adversaries are doing. And the same thing I think really applies to thinking about a constraint-based framework. Over and over and over again I hear from clients and people in the investment community, "Oh no, China wouldn't do this because this would hurt their economy." I think you have to throw that out and understand that it's never been about their economy. And so yes, the constraint-based framework still works. You just have to understand what the constraints are and it ain't their economy.

....see two very large non-quantifiable risks. One is significant political violence in the United States this year. Both sides, I don't care what side you're on, both sides absolutely think that they're on God's side and that the other side is evil, and that's going to breed some serious problems, and I'm very concerned about that. I'm not caring about which candidate wins. Frankly, I actually don't think there's a huge difference between them other than non-social policy. It's really about what each side is going to react.

So that's one big unforecastable risk that I think we have to deal with. The second is exactly what we've been talking about when I said that I'm worried that we don't have five years. What I see developing right now is a grand strategy to completely overwhelm the US system across multiple fronts and then all of a sudden launch the attack for Taiwan. It'll probably be a blockade 'cause they can enforce it. And I'm not saying that's my base case, but I think that chance is way higher than people understand. I don't know what the probability is, but I could see it as high as 20, 25% this year.

Karim. My starting point is actually that Taiwan will be the catalyst, but it'll be in a way that I don't know that we're necessarily going to feel as overt as a military incursion right on the front end. It may actually already be in play because what's really happening here is there's a subversion of technology with the semiconductor space. The implications of, and seeing this in my data, I've shared it with you, Renè, I've seen it. I've actually put it out on LinkedIn very, very quietly as to not ruffle feathers, but to sort of say, look, it's there, it's visual. You can see it in the spark lines. The level of exfiltration of very critical information around being able to hobble and utilize and then essentially deploy that is probably going to be done at the same time, there's a massive impact on the supply chain.

I know I said this five times in this conversation, but I have to double down on it or triple down on it at this point because that is essentially Achilles' heel. They're going to use that against us in a huge way. And it's not the supply chain people think of. It's going to be technology supply chain. It's going to be third-party risk that is effectively the part that we have zero control over. We just saw it with Change Healthcare ransomware attacks. That's a very silly, small example to the grander scheme of things that we're talking about, but it's a prototype and an archetype of what they'll leverage in a larger way. These are all experiments for a grander plan.