Microsoft's Tom Burt on geopolitics and cybersecurity in the age of AI

Written by

Chen May Yee

Published

13 June, 2023

Category

Security

As digital threats proliferate across the world, it's getting harder to keep them at bay. Wars are now fought both on the ground and in cyberspace. New AI technologies can help ward off cyberattacks or could – in the absence of future regulation – help the bad actors.

night. We caught up with him during his trip through Asia. He talked about emerging cybersecurity threats in the region and his experience at the IIS Shangri-La Dialogue in Singapore, where defense chiefs met in early June to talk about security challenges in Asia.

Here is an edited transcript.

Q: You were just at the IISS security conference in Singapore. What jumped out at you? Any surprises?

A: Last year, the hybrid war in Ukraine was new and the use of destructive malware by Russia as part of its invasion of Ukraine was new. This year, everyone remains very interested in what the threat environment is and what they can do to address that.

The one part that was surprising, which has gotten quite a bit of press, was the appearance by both the Secretary of Defense of the United States – and his speech – and then his analog, General Li from the People's Republic of China and his somewhat fiery speech that I think took a number of us by surprise.

It made clear that the tensions between the two nations remain high.

It really reinforced the need for Microsoft to be great partners with the region's governments and especially to help them have strong, resilient cybersecurity.

Q: You have touched on cybersecurity threats by nation states. How is that evolving and what's been done since?

A: In terms of the nation state threat landscape, what we're seeing with Russia is an ongoing effort for its cyber activity to support its invasion and war with Ukraine. What we've seen just in the last

understanding of a wide range of targets within Ukraine as well as in the US, the UK and the EU, especially those that are supporting Ukraine's defense, including private enterprise.

Iran has been stepping up its aggression. Other than Russia in Ukraine, it's the only other nation state we see at this time utilizing any kind of destructive malware. We've seen Iran utilizing ransomware to actually steal money and engaging in a wider range of intelligence-gathering attacks.

Historically, they've largely worked in the Middle East and targeted the energy sector, but now we've seen them extending that much more broadly around the globe, especially targeting the US and a wider range of sectors.

North Korea has continued to engage in intelligence gathering especially in the region, particularly targeting Japan, but also in the US and other regional targets – especially in academia and think tanks as well as some military technology targets.

But the big development with North Korea is its great success in stealing cryptocurrency equivalent to hundreds of millions of dollars – enough so that their cyber operation has become an important funder of government operations.

And then there's China.

We've seen China continuing and even expanding its cyber operations to gather intelligence and information globally but with a particular focus on the Asia Pacific region, Southeast Asian countries in particular.

The Microsoft Threat Intelligence team recently published a blog on this great work that they did tracking a Chinese actor called Volt Typhoon who engaged in some very creative attacks

Q: You mentioned hybrid warfare in Ukraine continuing to be of interest. Are there implications or lessons here for Asia?

A: Maybe the most important lesson was the importance of the hyperscale cloud.

At the outset of the war, one of the first missiles launched by Russia targeted the Ukraine government datacenter. And Ukraine had just recently passed laws to allow them to move to the cloud.

We know it's the case that security in the hyperscale cloud is much greater than you can ever provide on premise. We proved that in Ukraine, when Microsoft's Defender for Endpoint used an AI algorithm to identify Russian wiper malware and stop it from being installed in the customer's network.

With the 65 trillion signals that we get into Microsoft from our global ecosystem every day, we will be able to train ever more capable AI to identify code and systems that are up to no good and protect our customers.

The other lesson we learned was how the work that the Microsoft Threat Intelligence team does to track these nation state actors provides a great resource to help defend against these attacks.

There have been times when we've been able to provide that threat intelligence quickly enough to prevent an attack, and there are other times when that threat intelligence has helped them recover more quickly.

Continuing to build partnerships across governments and working together on how we can better defend against cyberthreats is the right solution. The hybrid war in Ukraine makes clear how the

"With the 65 trillion signals that we get into Microsoft from our global ecosystem every day, we will be able to train ever more capable AI to identify code and systems that are up to no good and protect our customers."

Q: Do you also see attacks themselves getting more sophisticated because of AI?

A: Not yet.

What we are seeing is adversaries using AI to improve their influence operations, the propaganda that they create and distribute to try to influence the opinion of citizens in other countries. Both the Russians and the Chinese have extensively invested in their network of influence operations that operate around the globe. We are beginning to see AI tools being used to improve video, image and text propaganda, and I expect we will see this trend continue.

There've also been a number of reports of cyber criminals improving the quality of their phishing by utilizing large language models to create more persuasive language.

Q: Why do you think we are not seeing a lot of attackers using AI yet? Is it because AI requires the kind of resources in terms of computing that might not be easily accessible?

A: Yes, for that very reason. The expense and complexity of the resources needed – technical, engineering and financial, building

Now, it's going be important that we and others develop responsible AI in a way where we don't make those computation resources accessible to the bad actors.

That's addressed in more detail in our white paper from our Office of Responsible AI that describes the appropriate ways in which governments should be regulating AI.

"Now, it's going be important that we and others develop responsible AI in a way where we don't make those computation resources accessible to the bad actors."

Q: What's next?

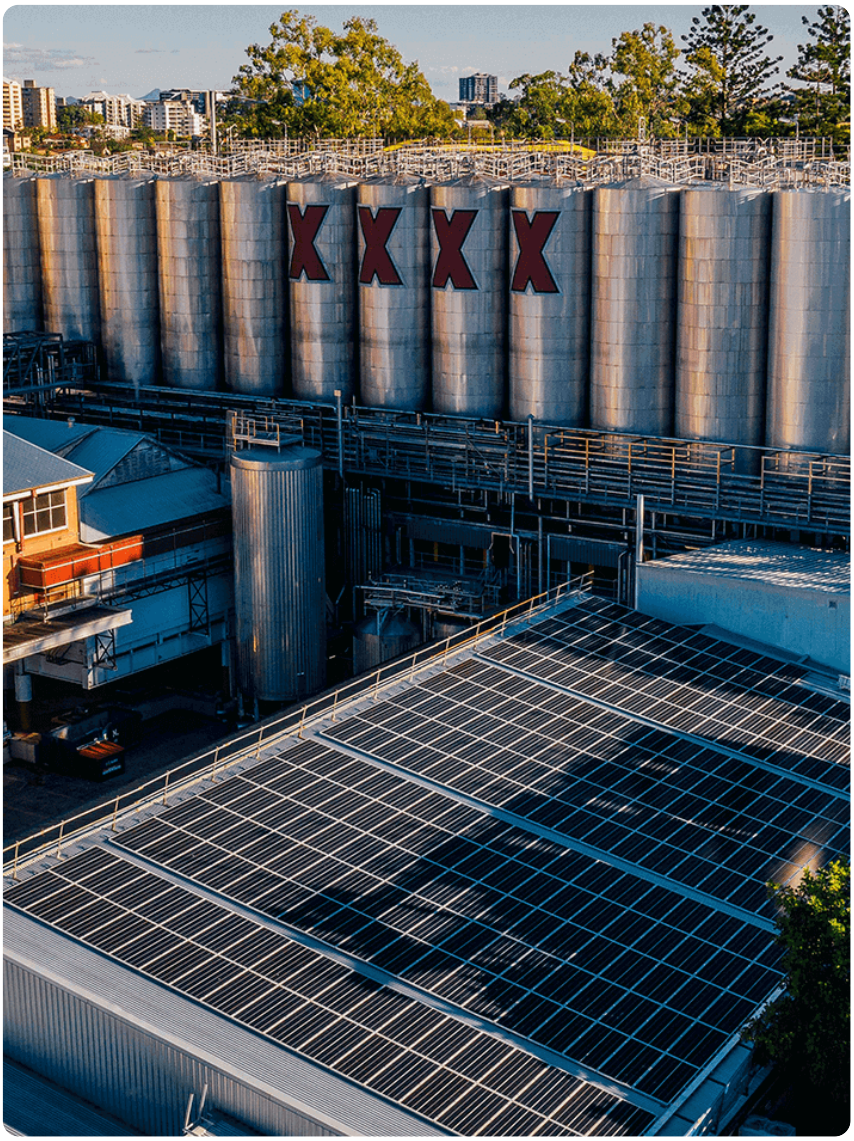
The next step in our evolution is Microsoft Security Copilot.

It's designed to help an incident responder use simple English language prompts to pull together all the data needed to respond to an incident from across multiple platforms in a customer's system. No longer does an incident responder have to have a great deal of expertise in a range of esoteric and challenging incident response tools. In this way, Security Copilot also helps address the significant gap we face in the supply of cybersecurity professionals.

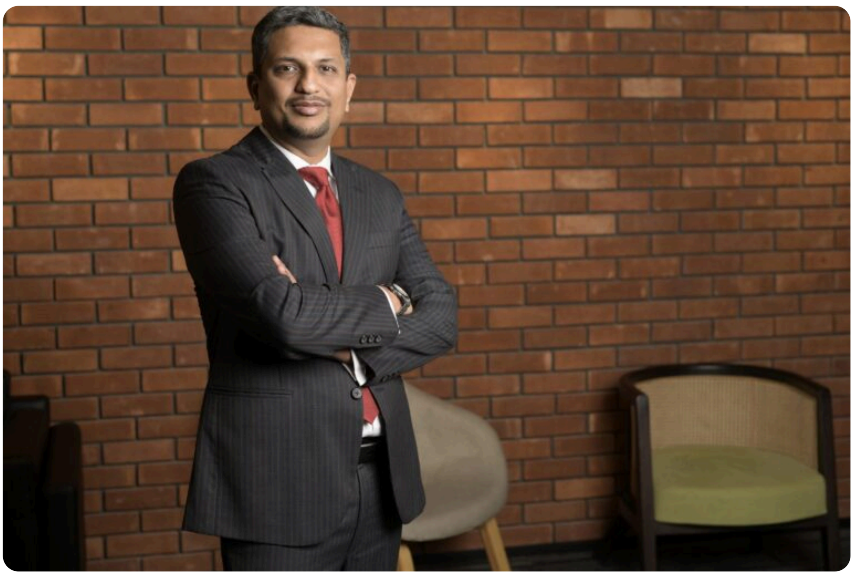
Our security team says that it will shorten response times in some cases from days to just hours by pulling this information together in new, more insightful and simpler ways.

AI Security

Related Stories



Security



Security

When it comes to security, you want Microsoft in your corner: Samir Aksekar, CISO, Tata Digital

Microsoft helped us extend enterprise security to employees' homes: Roman Rafiq, IGT Solutions