**Public Sector Future WWPS Podcast Series**

**Episode 58**

**Alvaro Vitta [host], Tom Burt [guest]**

**TRT: 40:56**

[TCR 00:00:02]

**OLIVIA NEAL:** Hello and welcome to Public Sector Future. This is a show for anyone who cares about delivering change in the Public Sector, and this week we're talking about a topic which is, or should be, at the heart of how we all think about working today.

October is cybersecurity awareness month, and we're joined today by Alvaro Vitta as guest host. You might remember Alvaro from our cybersecurity episodes last year. In today's episode, our guest is Tom Burt. Tom is the Corporate Vice President of Customer Security and Trust at Microsoft and he and his team have just published the Microsoft Digital Defence report.

This report shares publicly the findings from the trillions of signals which Microsoft track around the world. The conclusions are powerful, and show how increasing nation-state attacks are putting public sector organizations at higher levels of risk. As well as discussing those findings, and what they mean for public sector organizations, Tom shares his perspective on advances in AI and what these mean for both cybersecurity attacks and defense.

Over to Alvaro.

**ALVARO VITA:** Hi, Tom. Good to see you. Thank you for being with us.

Tom, can you remind our global audience what your role is at Microsoft and what you and your team are responsible for?

**TOM BURT:** Yes, so I manage a team that’s called Customer Security and Trust, and we actually have a very interesting portfolio. We’re responsible for advancing customer trust and the safety and security of the digital ecosystem.

And we do that in a number of ways. First of all, we work to disrupt both cyber-criminals and nation-state actors, trying to seize the infrastructure that they use to conduct their activities. We advocate globally for cybersecurity policy and sensible cybersecurity regulation.

The Microsoft Threat Analysis Center, which is one of my teams, works to investigate, understand and report on foreign influence operations, the way in which other nation-states surreptitiously seek to distribute their propaganda messages around the world. And that team also adds geopolitical analysis to the cyber-threat intelligence that Microsoft threat intelligence teams gather in our technical hunting for nation-state actors. And then we write reports regularly on that activity to inform the public.

And the Threat Analysis Center also has a new subscription service for access to its full range of analytical reports. It’s often dozens a week, and we’re offering that subscription service to democratic governments and enterprises.

And then I also have our national security team,

And I’ve got an engineering team that works to develop solutions to support all those other teams, and to make sure that we’re incorporating the power of AI in everything that we do.

**ALVARO VITA:** Thank you, Tom, and thank you for your service and that of your teams.

Tom, the 2023 Microsoft Digital Defense Report has just been published. Why does Microsoft invest so much time and resources to produce this annual report?

**TOM BURT:** You know, it’s because we actually have a vantage point that’s truly unique in all of the digital ecosystem. Because of the breadth of our ecosystem, the number and scale of all the different kinds of products that Microsoft has, and therefore the – the signals that we receive from our broad ecosystem, we have a truly unique view into what is happening in terms of cybersecurity.

Microsoft receives 65 trillion signals a day from our global ecosystem, and that is an incredible data resource that then the Microsoft threat analysis teams across the company can use to analyze that data for security information, for risks, for how we can improve our products, and for the kinds of analysis that I described that my team does, as well.

[TCR 00:03:12]

And we have over 10,000 security and threat intelligence experts, who work every day to try to improve the security and the safety of our customers and their ecosystem.

We also have incident response teams that go out and help customers respond when they’ve been attacked by a cyber-attacker. And we receive customer input, where they have input for us as to how we could do better, how our products can be better.

And when you take all of that intelligence together, we felt, starting four years ago, that we should pull together the complete picture across all of these different teams at Microsoft as to what we’re seeing, what we’re seeing in terms of cybersecurity, cyber-threats, and what our advice is for what customers and – and others can do to better protect themselves, and put that into a single annual report. And this is the fourth – the fourth of these Digital Defense Reports, and we’re – we think that they provide a unique perspective and a real value to the – to the ecosystem.

**ALVARO VITA:** Yeah, in looking at the report, which is very detailed, and it has a lot of insights, one of the things I noticed is that the nation sponsored cyber-threat activity has increased significantly since the publication of the last year’s report.

For example, the Microsoft Threat Intelligence observed state-sponsored cyber-threat activity against organizations in more than 120 countries and territories, with 53% of all of the threat notifications sent by Microsoft going to government and critical infrastructure organizations.

What are the key factors, from your perspective, driving this dramatic increase in state-sponsored cyber-activity?

**TOM BURT:** You know, it’s a great question, and from my perspective, there are a number of factors that are driving this significant increase in state-sponsored, malign cyber-activity, whether that is for intelligence and information gathering purposes. And that’s most of the attacks we see are, you know, espionage types of attacks like that. But also we’re seeing an increase in destructive attacks. And more recently, we’re seeing an increase in what seemed to be prepositioning, where a nation-state is seeking to get access to other networks for possible future activity, and I’ll talk about that in just a second.

But really, the – the reason we’re seeing that increase is because that kind of activity with nation-state hackers sponsored, or – or are actually employed hackers working for nation-states can conduct that activity without any constraint or any deterrence.

[TCR 00:06:01]

There simply is no international agreed set of norms of conduct, with enforcement of some kind, to constrain the activity of nation-states who engage in these attacks. And therefore, since they’re effective and useful, we’ve seen more and more nation-states stepping into this space, conducting more attacks, and doing so in a more sophisticated way, targeting cloud operations. And I think it’s also a product of the increasing tension in geopolitical climate in general. And we’re seeing that across the major actors that we track.

The Microsoft Threat Intelligence Team tracks over 300 nation-state actor groups, but they still largely operate from one of four countries: Russia, China, Iran, and North Korea.

And each of those countries has its own unique set of reasons why they’ve been really active over the last year. Russia obviously is continuing its hybrid war against Ukraine, and they continue to use both espionage gathering and destructive cyber-weapons as part of the arsenal of weapons they’re bringing to bear in that ongoing war. And we’re seeing them increasing their focus in espionage gathering outside of Ukraine, targeting government organizations and private sector organizations that are in one way or another supporting the Defense of Ukraine against the war. And so, it’s been a lot of activity from Russia focused primarily in that way.

They – they continue, their – their most expert teams also continue to engage in – in global espionage activity that isn’t necessarily tied directly to the Ukraine war, but most of their cyber-resources have been connected to their effort to – to wage war against Ukraine.

With Iran, we’re seeing Iran using increasingly sophisticated tradecraft, better cybersecurity techniques and operations, and using a wide variety of techniques, including they take advantage of newly-disclosed vulnerabilities, even those for which a patch is available, and they act really quickly to take advantage of those vulnerabilities before people apply the patch, and – and they conduct their operations in that way.

And we’ve also seen Iran engaging in destructive cyber-operations, where they try to cause impact to the networks that they are compromising. We’ve seen them do that in Israel and also in Albania in retaliation for the – the Albanian government harboring a dissident group called a MEK. And you might have seen in the news that in the long run, I think the Iranian efforts in that regard proved productive because Albania ultimately took steps to get MEK expelled from the country.

[TCR 00:09:02]

We’re seeing North Korea engaging in a broad range of espionage attacks, especially targeting their nearest neighbors, South Korea, Japan, and others that – including the U.S., that might have information of use to North Korea.

But the biggest focus of North Korean actors has been their very successful attacks against cryptocurrency organizations in order to steal cryptocurrency, and they’ve been successful to the tune of hundreds of millions of dollars. And there appears to be an almost direct relationship between those thefts of cryptocurrency and their activity funding their missile operations. And so, North Korea is actually using cyberattacks to steal money to fund their ability to develop intercontinental ballistic missiles.

And then, you know, we’re also seeing this unchecked expansion of the cyber-mercenary marketplace, where more and more companies are building espionage tools and selling them to any government agency or organization willing to pay, so that those organizations, whether it’s an authoritarian government, a democratic government, or even a business enterprise, can take advantage of these offensive tools to surreptitiously conduct espionage and gather information from citizens and other organizations without their knowledge.

And so, you have all of these different motivations, but what is key to all of them is these kinds of attacks are effective, they’re useful to these nation-states, and there is no way right now to meaningfully constrain or deter that activity.

**ALVARO VITA:** Yeah, and when we look at the nation-state and the cyber-criminal ecosystem, one of the things that – that we’ve seen and we’ve noticed in the report is that over the last 12 months, there’s been some efforts, right, and great momentum from governments around the world in trying to modernize and adopt their cybersecurity policies and regulations to the realities of what’s happening on the offensive side.

And what in, your opinion, is going well, and what are areas that need improvement in – in the policy side?

**TOM BURT:** Yeah, so what’s going well is it is good that governments are taking these kinds of cyber-threats seriously, are recognizing the risk to their national interest, to their economies, to their citizens, from both nation-state and cyber-criminal attacks. So it’s a great thing that governments are stepping into this space and looking for how they can regulate or legislate to better defend against cyberattacks.

[TCR 00:11:49]

The focus in particular on encouraging better design and manufacture of technology products and services in order to reduce vulnerabilities is a useful focus, and things like the National Institute of Standards and Technology Secure Software Development Framework which they published, or aspects of the Biden administration’s Executive Order on Cybersecurity, Executive Order 14028, has provisions that are intended to use the economic power of the federal government to drive stronger cybersecurity practices by all manufacturers. And we see increasing interest in those kinds of standards coming up in policy conversations and in proposed regulation globally.

And an awful lot of those approaches align really closely with the Microsoft Secure Development Framework or Security Development Framework and Security Development Lifecycle, I should say, also known as SDL, which we pioneered some time ago, and we’ve recently modernized our Security Development Lifecycle rules to ensure secure development practices in cloud – in cloud services. As the world has moved to the cloud, as Microsoft has moved to the cloud, we needed to look hard at how do we ensure that those services are developed and provided to customers in the most secure way. And there’s work to do in that space, but that’s an area where government has legitimate and useful contributions to make.

Another place is in thinking about the critical nature of those organizations that are most exposed to potential cyberattacks, and thinking about, as – as U.S. regulators are, to a great, great extent, thinking about critical infrastructure, and how we can improve the cyber-resilience of critical infrastructure, which is another place where governments can make significant improvements, thinking about how they can help provide the critical infrastructure organizations, which are often very small utility companies or other small organizations who have limited resources and are probably relying on very old technology, helping them modernize their technology, move to the cloud, and become more resilient is an important government effort that is underway.

And things like CISA, the Cybersecurity Infrastructure Security Agency, in the Department of Homeland Security, CISA has an initiative they call Shields Up, in which they have identified cybersecurity issues and publish alerts broadly to the public about areas in which cybersecurity needs to be improved. And that provision of key learnings and the ability of government to then distribute that information, with the authority of government, to help people voluntarily take steps is also really good.

[TCR 00:14:54]

On the other hand, there’s also ways in which government regulation is – is not off to such a great start. And one of the biggest challenges is we need governments to harmonize their regulation and make them consistent. And that’s even across agencies within the same government. We’re seeing this arise across United States government agencies where different agencies are taking different approaches to the same cybersecurity problems and creating a bit of chaos for the private sector, both in terms of the providers of services and the consumers of services and knowing how to be consistent with all these different regulations when they are not harmonized – harmonized.

And there is a part of the new National Cybersecurity Strategy from the U.S. government, from the White House, which focuses on exactly this, the need to harmonize regulation. And so, it’s great that government is seeing that need, but so far, we are well behind in actually finding ways to create harmonization.

A good example of that globally are all the different requirements for reporting on cybersecurity incidents. And Microsoft has been a supporter. We supported in Congress. Congress passed legislation requiring at least certain sectors, critical infrastructure sectors within the U.S. to report cybersecurity incidents, and CISA is in the process of going through, doing rulemaking in support of that legislation.

We supported that legislation, but one of the key provisions was that the – the reports should be sent within 72 hours of being aware of the cybersecurity incident. And we’re seeing in other jurisdictions that reports are required within 24 hours, or even as short as six hours.

And these are very poorly advised regulations that have not been well informed by the input of the private sector teams that actually do incident response. Because in that short period of time after one of these incidents, it is very, very rare that the incident responding teams have a good handle on what has happened, who the actor is, how the – the system has been compromised, and what needs to do – be done to expel the attacker from the system.

And so, by requiring reports in such a short time, you’re actually having two very counterproductive impacts. One is, you’re distracting people who should be focused on defending against and responding to that incident. You’re – you’re distracting them from the hard, hard work they’re doing in order to create some government report.

And secondly, you’re doing that when those incident responders are very much buried in the fog of war, where they’re still trying to understand exactly what the – the attacker is doing and how they’re doing it.

[TCR 00:17:44]

Recently, we’re seeing especially Chinese actors using what we call “living off the land” techniques, which means once they have gained access to a network, they intentionally do not install malware or other code in that system that could be detected. And instead, they use existing expected commands and processes within that network to conduct their espionage activity. It makes it very hard to find them and detect them.

And again, by requiring reports too quickly, what governments will be doing is not only distracting the incident responders, but building massive, useless databases of inconsistent and inaccurate information. And so that’s another place in which, you know, both harmonization, consistency and sensible regulation needs to be applied.

And now another new trend, like the Cyber Resilience Act that’s in conversation in the EU, it has a number of really strong and positive requirements that will help advance cybersecurity. But it also has some that are really going to be counterproductive.

An example of that is there’s a section of the Cyber Resilience Act that requires private sector to disclose any known vulnerabilities that are being actively used by an actor, even before a patch is available to protect the public against that vulnerability. And that is just very poorly considered because at that time, by providing that disclosure, you are putting at risk the entire ecosystem.

We’re seeing these actors, both nation-state and cyber-criminal actors, reducing to just hours how quickly they can take advantage of a disclosed vulnerability in order to engage in their attacks. And by requiring reporting of these vulnerabilities before a manufacturer has a patch ready is really ill advised and puts us all at greater risk.

And so, we’re working hard with the regulators and with the legislators who are considering that to help them understand why the provision is not a wise provision, and what we can do instead to improve the process of how we respond to vulnerabilities, how we reduce vulnerabilities, and how we help the public patch these vulnerabilities more regularly and more rapidly.

And the biggest thing we can do there is everybody gets – needs to over time, we need to get people to the cloud. Because not only is the cloud where we and our competitors can provide our best cybersecurity in the cloud and have the opportunity to provide incredibly powerful AI engines to help defend in the cloud, not only do we have that capability, but when there is an incident, in the cloud we can respond in a matter of hours or days instead of weeks or months. And when we do respond, we can patch that vulnerability and protect all of our customers almost instantly, rather than putting out a patch that customers have to apply in their own prom – in on premises environment.

And what we see is even for really important vulnerabilities, it’s hard to get more than about 30% of the ecosystem to apply patches, which leaves the ecosystem broadly exposed.

[TCR 00:21:07]

And so, getting government to come up with policies and systems and incentives to encourage move to the cloud, to encourage the security of the cloud, to encourage strong security engineering practices for cloud service providers, all of that makes perfect sense. But requiring disclosure of vulnerabilities before the private sector has a protection is very misguided.

**ALVARO VITA:** It looks like there’s been some progress, but more work to be done and more consultation with the private sector to be able to fine tune some of these policies.

Moving to the technology side of the house, in the last 10 months, there has been significant advances in generative AI capabilities, right? And cybercrime criminals have quickly adapted their own versions of GPT-based technology that don’t have the same rigorous safeguards and ethical controls found in commercially responsible vendors. Now, these cyber-criminal organizations are already weaponizing and monetizing these AI cyber-tools against organizations globally. Now, this early technology adoption obviously gives them an advantage, a significant advantage of sophistication, scale and speed over victim organizations.

What can public sector organizations start doing to prepare to counter these advanced AI-based threats?

**TOM BURT:** You know, there’s a number of things that we need to do, but the first thing is to understand what is the true scope of the AI threat today. And we are seeing both nation-states and cyber-criminals using AI, generative AI, but the principal way in which we’re seeing them do that so far, is to help them refine their phishing messages, their phishing attacks.

You know, one way that, if – if you’re thoughtful and careful when you receive email or text messages, one way to – to detect that a message is not authentic and is a phish and not click on it and not get compromised, is to pay attention to things like the language that’s used. Because often, especially in the cyber-criminal space, sometimes in the nation-state space, the – the language is a little awkward, or it doesn’t ring true as a native speaker of that language and how it would be presented. And generative AI is helping, and – and we’re already seeing, and government agencies are seeing the use of generative AI to improve the quality of the language used in those attacks.

We’re also seeing AI, and especially AI for image processing being used to improve the fake imagery that we are seeing being used in nation-state influence operations. As other countries are trying to spread their propaganda message outside their own boundary – boundaries, or even sometimes within their own geographic boundary, we’re seeing them using more sophisticated AI-powered capability to create more convincing imagery and video. And those are the places where we’re seeing actual deployment of AI by the bad guys.

[TCR 00:24:20]

There’s a lot of concern that over time, AI-powered programming tools or others might help bad guys create malware, or other attack vectors more rapidly or more readily. We’re not really seeing evidence of that to any significant extent so far, but it is something that – that we are watching for very carefully.

And as a result, Microsoft’s Office of Responsible AI is working to both articulate our own principles for how we deploy AI in a responsible manner and working with government officials on frameworks for government regulation of AI.

As you’ve probably heard, this is a space where Microsoft has been very public in stating that we think government should be regulating AI in responsible ways. And we are working as close partners with governments to help define what those rules and regulations should be and how we can control it.

All of that said, I’m actually really both optimistic and pessimistic about what AI means for the world of cybersecurity. And I want to start with the optimistic side, because in the intermediate to longer term, it should absolutely be the case that AI will give the defenders a disproportionate advantage.

And that’s because ultimately, deploying AI in the cybersecurity context is going to require three things. It’s going to require a team of really expert – really expert AI technologists, whether that’s in machine learning or data science, but the team of – of experts that are going to both devise and test and create these AI engines is a limited resource. And the private sector, the principal cloud services, companies have a lot of those people, and that’s an advantage.

Another advantage is it costs a lot of money to create and operate major AI engines. Microsoft had to build a specialized supercomputer for OpenAI to train ChatGPT-3, 3.5, and 4, and we are in the process of building other supercomputers for our own AI training.

And we need to add incredible processing power to all of our global data centers, because every time you prompt one of these AI engines, that prompt goes to one of these data centers, and it takes a lot of processing power to return the incredibly valuable responses you can get from something like Bing Chat.

[TCR 00:27:02]

But all of that takes an amazing investment, billions of dollars of investment. And again, the number of both governments and private sector entities with the resources to make that investment further constrains who can really play in this space.

But then the big advantage and an advantage that Microsoft certainly has, and a very small number of others might share, is the data. So in this case, we have the 65 trillion signals that I described that come in from our global ecosystem. And that’s everything from end user, end user devices, on-premises networks, cloud – cloud services consumers.

I mean, the full range of the Microsoft product portfolio, and all of the data that we get back from our customers’ use of our products and services, that dataset is something we can train against and build the algorithms that are going to detect anomalous activity in the fabric of the digital ecosystem and block malign activity.

And inform people this is, you know, someone we think is up to no good. Do you want to actually have this – this code enter your environment, enter your network? If so, we’ll let it happen. But, you know, you ought to be cautious because we think this is bad.

And doing that at the speed of AI and with the ability of AI to train against what it’s seeing in the – in the ecosystem, that’s a unique – a unique asset that is going to give the defenders an asymmetric advantage that attackers are not going to be able to meet because they don’t have access to that same incredible dataset.

On the other side. So that’s – that’s where I feel really optimistic. Where I feel much less optimistic is about government influence operations. And we talked about how already AI is being used to improve both the text and the imagery that we see nation-state actors using as they work to spread their propaganda globally.

And the reason that they will have an asymmetric advantage is because authoritarian governments don’t – aren’t constrained by principles of free speech and democracy, like most of the western democracies are, at least to some extent. And that’s why we’ve seen both Russia and China invest significant resources in building out their global influence operation networks. Both people and online and traditional media throughout all continents work to distribute and amplify the messages that those countries wish to amplify, to influence both citizens and governments around the world.

And they’re very effective at it, they’re very good at it, and frankly, they are way ahead of the West, both in the techniques that they use, the networks that they’ve created, and their willingness to use it for their nation-state geopolitical purposes. And it’s hard, it’s very hard to assess how the western democracies can respond effectively to those techniques.

[TCR 00:30:18]

**ALVARO VITA:** No, that – that makes sense. It looks like there’s a lot of channel – challenges, a lot of opportunities for governments across the planet. And it looks like Microsoft is well positioned in this era of AI to be able to help our governments around the world be able to level that playing field.

Now, when I look at the 2023 MDDR report, Microsoft Digital Defense Report, there’s some lessons and – and actionable recommendations that we can go over. So three things jumped at me in terms of lessons within the report.

One, government and critical infrastructure organizations have a big target on their backs, with nation-states attacking over 120 different countries and territories. The global cyber-criminal economy is a big economic stream for these cyber-criminal organizations, expected to hit $10.5 trillion by 2025. And then lastly, the cyber-talent market has an enormous deficit, 3.5 million jobs that will go unfilled through 2025.

And so, when we look at these three particular observations and lessons learned from the report, from your opinion, what are some practical actions that public sector organizations can start thinking about implementing to strengthen their cyber-resilience?

**TOM BURT:** You know, there’s a number of things that can be done, and we talk about these. As you go through the MDDR, one of the things we try to do is not just address both problems and challenges, but also our recommendations for what can be done. And so, I really encourage people to read through it. There’s a lot of useful information. And I’m just going to hit a couple of the high points in terms of our recommendations.

Really, our recommendations this year are the same as they were last year and the year before that. If we could all exercise the basics of cybersecurity, we could today protect against something like 99% of all of these attacks. And that’s things like deploying multifactor authentication on every account, and utilizing, if not multifactor authentication, even better is to utilize a modern authentication system, like Windows Hello, that does not even require a password, and uses biometrics or other means of identifying a user and ensuring that – that the individual who is seeking access to a computer resource is really entitled to have that access.

[TCR 00:33:06]

That alone, our recent – we recently updated our analysis of that – analysis of that, and we saw once again that deployment of multifactor authentication could protect against over 98% of all attacks that occurred over the past year.

And what’s interesting is we also looked at what if the attacker already has your password? Does multifactor authentication still protect? And the answer is yes. In well over 90% of the cases, you’d still be protected, because you have that second factor.

And there are cybersecurity professionals who rightly point out that there’s different qualities of multifactor, you know, processes, and that once they get one factor, they can use their fraudulent techniques or other techniques to get the second factor. And all of these things are true, but the reality is when you look at the data, multifactor authentication is the number one thing we could all do.

And it’s a place where Microsoft continues to invest to make it easier for our customers to utilize and deploy multifactor authentication. We – we work to make it required. But we allow our customers who need to, to opt out when their networks or their processes or systems for some reason won’t support multifactor authentication. But we are continuing to encourage all of our customers, in the best way we can, to apply that or some more modern form of authentication that’s not password-based.

Then the – the other thing you can do is within your network, make sure you are applying zero trust architecture principles. And there is a lot that has been written on this, but the basic concept is just because an account has access to a resource on your network, design your network so that they don’t necessarily get access to any other resource, unless you can confirm their identity and you know for sure that they are who they say they are and they should have access to that additional resource.

And limit access to the most critical resources you have. Don’t give everyone access to those critical resources, but limit that closely and protect against the potential. Assume that you’ve been compromised by an actor. How do you protect your most important assets? That would help defend against ransomware. It would defend against espionage related attacks, trying to steal your intellectual property, and so forth.

And of course, the number one, the next thing that people can do to really advance their cybersecurity is move to the cloud. Whether it’s Microsoft or one of our competitors, our best cybersecurity services and systems, our ability to react quickly, respond and help defend, and the – the advancement, the application of AI to cybersecurity is all going to happen and is happening right now in the cloud. And so, those are key things that people can do.

[TCR 00:36:00]

The other problem that we have is a significant lack of people who can provide the – the employment needs that we have for cybersecurity professionals. And there’s a couple of things the public sector can do there. One is, of course, help us and others invest in cybersecurity training, so we can train people to be – to take on those great jobs.

But then we can also deploy AI. And we will soon, at Microsoft, be releasing our Security Copilot, which is a tool that really helps incident responders and security professionals gather information, understand what’s happening in their network when they’re under attack, and respond to it with less technical expertise and less experience, and yet do that in English language very effectively. It’s a super powerful tool that will help both public sector and private sector organizations staff up with good people who can help them respond to incidents.

And so, those are just a few of the things that can be done. There’s more in the Microsoft Digital Defense Report.

**ALVARO VITA:** Yeah, it – it looks like there are a lot of opportunities for public sector organizations across the planet to be able to take some of these actionable insights you provided to be able to advance and modernize their cybersecurity capabilities to deal with these incredible challenges that they face.

Now, Tom, when we look at the modernization of cybersecurity capabilities across governments around the planet, and the ones that you speak to, are there any examples that – that jump out at you on cybersecurity governments – sorry, governments that are doing cybersecurity, that you consider to be examples, that you consider to be people that are doing it, where proven practices are being used that can be leveraged by others?

**TOM BURT:** Well, I think every government in the world has the opportunity to use AI and the cloud to advance their cybersecurity. And we do see that. You know, we see certain governments moving rapidly in that space, to help with national defense, to protect against health care, to help protect against critical infrastructure attacks, and to do that in a way that can be both efficient and effective.

You know, we’re seeing a lot of good work by the U.S. government, and I talked about some of that earlier, to really focus on cybersecurity and how to advance cybersecurity of the infrastructure of the U.S., critical infrastructure, enterprises and organizations, reducing cybercrime. And there’s just many examples of that across the U.S. government.

It’s really a question of – of going fast but going with care and with – and being well-informed by the experts who really have insight into what’s happening and can help advise policymakers and legislators.

[TCR 00:39:06]

So we need to move quickly, and we see that happening in many governments. But we need to do that in a thoughtful and responsible manner. I talked earlier about some of the challenges we have when governments advance their initiatives too quickly and without a real understanding of what it’s like on the frontlines of cyber-defense. We see California in the U.S. moving quickly. North Dakota is moving quickly. Virginia is figuring out some things and moving quickly as well.

We’re seeing other interesting advances. The United Arab Emirates is moving quickly to advanced cybersecurity and to, I think, create a site of excellence for their region and providing secure computation. And they’re moving quickly.

South Korea, and others in Southeast Asia, we see these governments moving quickly to advance cybersecurity.

We’re also seeing regional organizations, the G7, Indonesia, India, the quad in the Asia-Pacific region, we’re seeing these regional government organizations working together to collaborate on how they can advance cybersecurity.

So all of those are positive developments, as long as we can do that in a way that is consistent and not conflicting across different regulatory schemes and is done in a way that helps protect the ecosystem without unduly retarding innovation.

**ALVARO VITA:** That concludes our episode. Tom, thank you for your time, your insights, and for all the great work transparency and collaborative information sharing that you and your team continue to do for a safe and thriving digital ecosystem globally.

**TOM BURT:** Thank you have, Alvaro. It was a great conversation.

[TCR 00:40:56]

**OLIVIA NEAL:** Thank you to Alvaro and to Tom Burt for sharing their insights on these topics. It's sobering stuff, but absolutely critical that we're all aware of these trends - and what we can do about them. For more content on cybersecurity, visit our website, where you can also find all of our other podcast episodes. We're at aka.ms/publicsectorfuture

Thank you for joining us today and see you next time.

END