**Project: Public Sector Future podcast**

**Detail: Episode XX - Digital Collaboration: using technology to enable secure collaboration between coalitions**

**Talent: AT Ball (host), Perry Smith (guest)**

**TRT: 23:05**

[TCR 00:00:10]

**OLIVIA NEAL**: Hello and welcome to Public Sector Future. This is a show for anyone who cares about using digital approaches in the public sector in order to deliver better outcomes. Today we’re going to be continuing our focus on digital transformation in defense and intelligence organizations, with guest host, AT Ball, who you met in our last episode. AT is part of the Defense and Intelligence team here at Microsoft, and prior to joining, he had a 30 year career in the US military.

Today, AT is joined by Perry Smith of Myriad Technologies. Myriad were Microsoft's Defense and Intelligence Partner of the Year in 2022. Together, Perry and AT will be discussing using technology to allow secure collaboration in defense environments, experiences of success with the Australian Defense Department and Navy, and the potential to increase use of digital approaches to enable secure collaboration across coalition partners. Over to you, AT.

[TCR 00:01:32]

**A.T. BALL:** Perry, it’s great to have you today. So happy that Myriad has been partnering with Microsoft for several years now, and you and I have worked together for a long time. Can you describe a little bit about Myriad, the mission that you undertake, in terms of how you work with government and defense out there? I think it would be great for our audience to hear a little background.

**PERRY SMITH:** Good morning to you, and thanks for having me. So, so Myriad is a product company that specializes in producing a product called Secure Search and Information Exchange (S2IX), or as we affectionately call it, "STIX" for short.

So Myriad, as a company, has been around since 2007. We started as a one-man band. We’ve now grown to four offices across two countries. We primarily work with military folk in the Defense Departments, and what we really aim for is the operational effectiveness of STIX and the IT that it brings.

So this stems from our first encounters with Australian Defense,

Since that time, we’ve worked across each of the groups and services, and also extensively with joint operations, and specifically built those learnings into STIX to make it an effective platform.

**A.T. BALL:** That’s fantastic, Perry can you describe a little bit more about your particular role, and you know, how you came into this role, and – and what excites you about it right now?

**PERRY SMITH:** Yeah, honestly, I’ve got the best job in the world. it’s my job to go and find new customers and partners in different parts of the globe for us to work with, and then to land and enable those partners and those customers to be able to get the most out of STIX and it’s capabilities.

We especially focus on the defense and intelligence, but we’re equally applicable to

government data exchange scenarios where they’re trying to securely exchange information.

We were having great success with Navy. We were doing some small multinational scenarios, from the joint operations perspective.

But what we really wanted to understand was how applicable our technology was to, say, NATO or the U.S., the Five Eyes, et cetera.

So that’s where I think we first came across each other, where we became relevant to Microsoft, and where we started to explore together what were the use cases that we were trying to solve and that we had solved in –in our own military relevant to these other customers.

[04:14]

**A.T. BALL:** Perry, you and I became acquainted in the Australian market, and this was pre-COVID. But along came COVID, you know, and I think that might have been an inflection point in terms of governments recognizing perhaps that they weren’t quite as prepared as they had hoped to be in order to address the challenges that emanate, particularly during a crisis like COVID, but we’re past that right now, and what I’m interested in is, what do you think has changed in terms of the operating environment, both for enterprise IT, but also mission-critical systems, since COVID?

[04:57]

**PERRY SMITH:** So my observation during the COVID phase was many governments were really not ready and prepared to be able to manage true distributed working without nice, big connections between all the environments.

And I think COVID has taught us that, at scale, it’s only the major technology companies like Microsoft that can bring the scale and the solutions necessary to really answer the true challenge of global interoperability.

And the fact that Microsoft had the hyperscale cloud sitting behind that, to take on thousands of users in an incredibly short period of time, I think highlights some of the changes moving forward that governments really need to – to think through, that the – the days of is because I can lock up a box in my environment, I – I think they’re long gone.

**A.T. BALL:** I really believe that point is worthy of drilling down a little be more on, because I think you brought up – two things up, Perry, that are – are really, really critical. The first is the obvious, you know, how do these new technologies and the digital collaboration tools impact the way that you’re driving success for defense departments and governments around the world as they attempt to deliver mission-critical services, but the second part that you brought up about working with Microsoft. So can you lay this out a little bit more in detail for us?

[06:34]

**PERRY SMITH:** Our partnership with Microsoft is really based in trying to move the technology forward and being able to think of the technology in new ways that reflect the current era of technology, greater competition amongst countries, and really a greater need to protect yourself from cyberattacks and that sort of thing.

So what used to happen is militaries would just create closed-loop networks that were not connected to their partners. And the other challenge is – is more broader government challenge in that governments’ IT folks can’t really keep pace with the rate of change that is happening in technology.

The final point I’d make is around the approach government has taken to procuring this sort of software. I really think governments now need to find a way to be able to procure the software for effect much more quickly, and in a ready – market-ready, market-tested way, which is the approach Microsoft takes, which is fantastic.

**A.T. BALL:** When you and I first met, you were working very, very deeply inside the Australian Department of Defense, trying to deliver mission-critical capabilities. You know, using that case study as an example, can you talk more specifically about what Myriad and STIX enables for defense departments?

**PERRY SMITH:** So we work incredibly collaboratively with Australian Defense, and what we are solving is the ability to balance "need to know" and "need to share" and to allow data to flow independent of networks and independent of operating environments, so that we can get data from the point of generation to the point of consumption, or the point of decision making quickly, effectively and for that effect.

So what that means in Australian Defense is we’re currently rolling out to specific vessels. So we have worked with Army, Navy and Joint, but at the moment, we’re very focused on Australian Navy and their data sharing challenges, especially when you’re talking about a maritime environment.

So I’ll just expand on that slightly and go, we’re not an island in this. We work very closely with key partners such as Microsoft, Accenture, and Apex logic. And this is to bring together the operational effectiveness with the special sauce we bring around that data exchange scenario, with the scale and technology that Microsoft provides, especially the cloud technologies.

[09:45]

**A.T. BALL:** Perry, I want to think through the implications, though, of deploying STIX within a coalition environment. We talked about the success within the Australian Defense Department in the Navy case, for example, but in today’s world, defense forces don’t operate alone.

Clearly, they operate in these austere environments, like you’ve pointed out, but they need to share information with coalition partners. They need to share information across different classifications and schemas of classification. So what options are – are you presenting to address these sort of challenges.

**PERRY SMITH:** In particular, most modern technology is focused around a centralized set of control servers, and a centralized set of security and authorization. And if you’re talking about a federation of partners coming together to work together, you can’t have that because you’ve got varying levels of trust between those different countries, and also those different forces. So, what we bring is the ability to balance that need to know, need to share in these multi-level security, multi-domain operations.

A recent example would be our participation at the NATO Coalition Warrior Interoperability Exercise, so, CWIX 22, where we showcased STYX running on Azure cloud, and on accredited environments within that, to be able to demonstrate both the cloud technologies and secure information exchange at those higher grades of classification.

So, being able to protect at multiple layers, not just the network layer or the compute layer, but all the way up to the data layer itself and being able to do that with assurance in these multi-country operational scenarios is really where STYX shines and comes to the fore.

And I think that’s one of the wonderful things about working with Microsoft, is we don’t just operate in a vacuum. We work directly with the development teams to upshift the technology where needed, to be able to operate at this higher level of classifications.

**AT BALL:** Okay, we talked about the use case inside a defense force with the Australian Navy. We talked about your efforts in this NATO exercise to demonstrate capabilities across a coalition. I’m really interested more now, to inform our audience about a look forward. Where’s the potential, you think, in these digital tools in terms of how they will allow collaboration and sharing? And what do you think needs to change in order to enable that?

[12:59]

**PERRY SMITH:** So, one of the biggest changes that I look at the landscape of government and how they’re adopting and using technology, and I would say that some of the biggest changes is how government looks at its digital sovereignty, its control of that data, and its management of that data; and to be able to work more collaboratively with the hyperscale companies, such as Microsoft, to innovate on the tools and technologies which raised the trust, raise the assurance of the data, but not using the old approaches to technology, because they’re just too outdated to be cyber defended.

So, part of the approach is what we’re trying to do, is build a coalition of the willing within the defense industry base, to work with the military so that the militaries can have the assurance and buy off-the-shelf solutions that answers their problems and answers how they need to move forward.

So, what that raises is the second part of the challenge, which is essentially, the government procurement models were really built to buy technology and adopt and rollout technology to their environments in the 1970s and ‘80s. And so, that’s a big change for governments.

And I think industry has a huge role in trying to work with the customer to help them understand what that change can look like and should look like. And a call out to the local Australian chapter for this. This is something they are doing very intently with the Australian Defence Force. And I believe they’re being successful in helping them migrate and understand that change in procurement strategies.

**AT BALL:** I love that the two things you brought out there in terms of your answers to these challenges, and the way that this customer in particular is adjusting some of their procurement policies in order to quicken the pace of change and adoption.

And the second thing I loved in your answer is this notion of trust. And it couldn’t have come at a more relevant time with the publishing, the recent publishing of the DoD CIOs’ zero trust guidance out there.

So, all of that are ways, I see it, as ways to adapt and adjust and mitigate risk. What about other issues related to risk, supply chain issues, for example?

[15:43]v

**PERRY SMITH:** Yeah, risk is very much at the core of a lot of this. So, risk and trust, I think are the two core issues.

In the area of risk, there’s a couple of areas that represent very clear and imminent risks to these types of environments. So, part of the approach has to be to bring the concept of zero trust. So, trust no part of your supply chain, trust no part of your data assurance, and supply chain for data assurance. And with that, what you bring is the understanding that you don’t just need to assure the system of systems approach as a core competency to governments, but you also need to assure the technologies from a cyber defensive IP theft or direct attack sort of approach.

So, more broadly, what this is that governments need to do more to invest in the technologies that provide this attack and defense at the same time, and there are some key lessons that they could pick up from technology partners such as Myriad, and Microsoft.

So, the current or a posture from defense, from a risk management is to treat the industry supply chain more “adversarially,” because they feel that they’re trying to be sold something. I think that needs to change to manage the risk of… actual risk of an attack or a defense separated from buying a set of technologies that allow you to manage that risk itself.

**AT BALL:** Given the state we see right now, state-sponsored cyber activity, the war in Ukraine, regional conflicts, what do you recommend defense and intelligence organizations do right now, in order to be prepared for a continuation of this sort of instability around the world?

**PERRY SMITH:** Yeah, I really think that the posture of governments to adopt technology needs to change, particularly the military. So, what I mean specifically is with the current state of the world, the focus needs to be on technologies that are ready now, available now. And that means they’ve been military tested and validated. It means that they are backed by allied forces and allied companies.

And in that sense, STYX is very much in that mode and vein, because we’ve currently participated successfully in over 20 military exercises. We’ve got capability in theater. And a lot of technologies purport to do a lot of things, but they are not proven in these operating environments. And that’s a key thing.

And this is a key area, if you look at Ukraine, and Microsoft’s response to support Ukraine. That was one of the fastest responses of a technology company to a military scenario that I’ve ever seen. And I was recently at a presentation by the ambassador for Ukraine, and he had nothing but praise for Microsoft, and their support for his country.

[19:27]

**AT BALL:** I think that the fact that these technologies, and your technologies have been proven out in military exercises, and now, what we see, the role technology playing in Ukraine is very different than it has been in previous. So, let me go back to what role do you see industry playing in furthering the defense ecosystem, and that ecosystem’s modernization of military operations?

**PERRY SMITH:** Yeah, the defense industry base, I think, has a critical role to play. So, traditionally, the defense industry has been driven by defense saying, I need a new tank, I need a new truck, I need a new thing. And they just respond to the customer going, I just wanted x, and pushing all of the responsibility on to the customer to understand how all of their assets need to be brought together, and how that needs to occur.

One of the critical learnings that I think technology can bring to that is the concept of creating this digital logistics supply chain. And the defense industry base has a critical and pivotal role to play in helping defense to cohesively and, in a pre-integrated way, bring all of that technology together.

So, imagine if I want to plug in a new vehicle. I can just plug it into my supply chain. Defense instantly knows how to consume that information, how to manage and orchestrate that vehicle, how to get into theater and how to capture information back. Making that digital highway to and from industry, to the defense and out to a military environment and all the way back is a critical path that the defense industry base and the defense ecosystem can support and help.

**AT BALL:** Well, Perry, I want to thank you for spending so much time with me today and telling our audience about your partnership with Microsoft, and the work that you’re doing with your solution within defense forces, but also across coalitions, and how you’re reducing risk associated with adopting the technology through participation in military exercise, but also, as you mentioned, being a trusted source of military code and military solutions.

Where can people go to find out more about Myriad, to find out more about STYX and what you’re doing out there to support defense organizations around the world?

[22:22]

**PERRY SMITH:** Yeah, for sure. So, we’re pretty easily contactable. As I said, we’ve got officers, which locally supported, both Europe and Australasia. If they just simply go to [www.styx.com.au](http://www.styx.com.au), then all of the information they need around STYX, as a product, and Myriad, as a company, helping them implement and support, that will be there.

**AT BALL:** Hey, that’s outstanding. Perry, thank you so much for being with us today. Perry Smith, I know that I’ll be running across and working with you in various exercises and with various defense organizations around the world. Thank you very much, Perry.

**PERRY SMITH:** Thanks, AT. Great to be here.

**OLIVIA NEAL**: Thank you to Perry and AT for sharing their insights, and thank you to you for joining us today. Check out our show page for links to all of what was discussed today and visit us at wwps.microsoft.com. Please do reach out and send us your questions and your feedback.

As always, you can find me on Twitter. I’m @LivNeal. I’m also on LinkedIn, where you can also find guest host AT Ball. Or you can email us at Ask-PS@microsoft.com.

Thank you and see you next time.

END