In this episode of our #TechTalk we are joined by Tom Burt, the head of Microsoft's Customer Security and Trust team, for a conversation on the future of cybersecurity and the role of AI in addressing the evolving threat landscape.

He shares his insights on how to protect the digital ecosystem against emerging cyberthreats, steps we need to take to safeguard the integrity of elections, why we need to strive for globally harmonized cybersecurity legislation and makes the case for more collaboration and new strategic alliances to fend off bad actors.

In the age of AI, cybersecurity faces new challenges and opportunities, as both attackers and defenders leverage the power of artificial intelligence to achieve their goals.

AI can help improve the security of AI systems and enhance cybersecurity by enabling faster and more accurate detection of threats, automated response and mitigation, and proactive prevention of attacks. However, AI can also pose new risks to cybersecurity, by creating more sophisticated attacks and generating fake or misleading information.

In our latest #TechTalk, we are joined by Tom Burt, the head of Microsoft’s Customer Security and Trust team, for a conversation on the future of cybersecurity and the role of AI in addressing the evolving threat landscape.

In the episode, Tom shares more about the work of his team whose mission is to improve the safety and security of the digital ecosystem. It covers cybersecurity policy work as well as disrupting cybercrime around the world, advocating for enforceable rules of nation-state conduct in cyberspace and analyzing cyber-influence operations of nation states.

The war in Ukraine has shown the strategic alignment of kinetic weapons, cyber weapons, and influence operations. Tom believes that this is just the beginning of the future of conflict and that nation states will become even more adept at combining these aspects of conflict.

While adversaries are using AI to generate deepfakes and synthetic media, Tom believes that AI can give defenders a disproportionate advantage. By building algorithms that recognize malign code or concerning conduct online, AI can help protect customers automatically.

Policy is a strong driver for the security of the digital space, and Tom recognizes the EU’s leadership, for example as part of the Cyber Resilience Act. However, he notes that there is a vast proliferation of legislation and regulation around the world, often in conflict with one another, which does not only present a compliance challenge but weakens defenses against threat actors operating globally. He calls for leaders to drive harmonization globally.

Looking ahead to 2024, Tom sees both huge challenges and huge opportunities. The volume of cybercrime and nation-state activity is increasing, but there is also the opportunity for the private and public sectors to work together and build new forms of strategic alliances to counter these threats, including influencing election outcomes. By deploying AI, enacting thoughtful regulation, and working in partnership, he believes that we can advance the common interest of a safe and secure digital ecosystem. “I’m hoping that by the time we get to this time next year, we will look back on 2024 as a real time of transition from losing these battles to winning these battles and getting ahead of the bad guys.”

Welcome to Tech talk my name is Nana

Louisa Linda I'm vice president for

European government Affairs I'm here

today with Tom Bert our corporate vice

president for customer security and

Trust welcome thank you good to be

[Music]

here Tom you had a very long and

What does your team do

interesting career at Microsoft leading

up to the role that you have today can

you tell us a little bit more about what

your team does and what's so unique

about it absolutely um the customer

security and Trust team has this really

wonderful and empowering mission to do

what we can to improve the Safety and

Security of the digital ecosystem and we

do that through a number of different

teams but we have the um digital crimes

unit that works to disrupt cyber crime

around the world we have our digital

diplomacy team that works with

governments and other stakeholders to

advocate for enforceable rules of nation

state conduct in cyberspace we do cyber

security policy work and we have the

Microsoft threat analysis Center that

works to analyze nation states use of

cyber weapons as well as influence

operations and how they use those to

extend their power and influence outside

their borders to impact

um other countries and citizens of other

countries and the threat landscape cyber

How do you see AI evolving

threat landscape is constantly evolving

and uh AI has come into the play as a

powerful tool to help address some of

these challenges but also as a weapon

for Bad actors how do you see the role

of AI evolving in that context I'm

excited about the role of AI but of

course you have to be cautiously excited

and the reason I say that is obviously

AI because it's going to be such a

powerful tool it is now and it will

continue to evolve we can see

adversaries taking advantage of of the

impact of AI to do their work more

effectively but what we're seeing today

really is um the adversaries are using

AI mostly to help them generate uh video

and audio so-called deep fakes or

synthetic media and that's the principal

way in which we're seeing AI being

deployed we're not seeing AI being used

by our adversaries to create some new

form of cyber weapon or some other new

scary way of attacking um uh others but

we are seeing it being used in that in

the influence operation space but the

reason that I'm optimistic is I really

feel confident that we are going to be

able to over time use AI to give the

Defenders a disproportionate Advantage

we should be able able to build

algorithms that take the data that

Microsoft especially sees across our

broad ecosystem that goes from endpoints

to cloud services and everything in

between and we should be able to build

into that uh and train against that data

set um AI algorithms that are going to

be recognizing malign code or um

concerning conduct online and and

protect our customers automatically with

the power of AI we're already seeing us

do that we saw it work really well um to

protect one of our customers our

Defender for endpoint customers in

Ukraine at the beginning of the war an

AI detected a Russian wiper package and

and blocked it from being effective to

to impact that customer and that's just

the beginning of what our security

engineering teams are going to be able

to do so I feel really optimistic that

in the coming years we will see our AI

Technologies playing a remarkable role

in helping defend um and and protect

customers against threats online the war

Lessons learned from the Ukraine war

in Ukraine it's the first time that

we've seen such a large scale cyber and

influence

strategy what do you think after two

years now and I know that you've been

also very much involved yourself in what

Microsoft has has has done to help

what's the lessons learned well I think

there are a number of Lessons Learned

maybe the most important one is the way

in which we've seen uh Russia utilize uh

three different zones of of threat and

to do that in a very strategic way so

kinetic weapons um but they've coupled

that with the deployment of cyber

weapons and destructive malware as well

as cyber intelligence gathering um

capabilities and then they couple that

with their influence oper operations

sophisticated propaganda and what we've

seen is they've deployed those things

together strategically with strategic

alignment now some would say they

haven't been as impactful or as

effective as perhaps we thought they

might be with say cyber weapons um but

they continue to work on it and they're

they're now deploying new forms of

destructive malware that they they did

not have at the beginning of the war um

and they're beginning to be you know

more success ful at times with those new

forms of of cyber weapons but more

importantly this is just the beginning

of I think the future of conflict

because it it's showing um that you can

combine these three different aspects of

conflict together strategically and we

will undoubtedly see that um

continuously and repeated repeatedly in

the future um in Conflict scenarios

between nation states and we're already

seeing that happen we're seeing it

happen with Iran targeting Albania

because Albania was harboring a

dissident group The me group and Al and

Iran used both influence operations and

cyber um destructive cyber operations

targeting Albania um in retribution for

that um we're seeing it obviously being

played out in many ways in the Israeli

Hamas war in Gaza um and we're seeing

nation states utilizing cyber um

techniques to prepare for the future for

the potential future conflict and so all

of these uh you know certainly raise

concern um about the extent to which

nation states in the future will use

cyber domain and especially both um in

terms of destructive malware and

destructive techniques and influence

operations in a strategic alignment and

we will undoubtedly see nation states

become even more um uh Adept and

therefore more successful in combining

those things together in a strategic way

Role of the private sector

we've also seen in Ukraine attacks on

infrastructure in that context how

important is the efforts from the EU to

harmonize rules and uh get more

resilient and what role does the private

sector play in that regard well you're

absolutely right we have seen um Russia

Target Ukrainian infrastructure in a

number of ways critical infrastructure

and the provision of key services to

civilians um and that has been the

energy sector agriculture water um and

even Communications and media but we've

seen them targeting all of these in an

effort to persuade the the citizens of

Ukraine to lose confidence in their

government and their government's effort

to defend against the the Russian inv

Invasion um and that's not the only

place where we've seen that and we see

governments around the world concerned

about the extent to which adversaries

can use cyber techniques to impact the

provision of these critical um services

to civilians as part of of

conflict the the work that the EU has

done in um and working on the Cyber

resilience act has been a a strong

contribution to the Future security of

the ecosystem um and it's a a broad

ranging new set of of legislation and

the implementing um rules and

regulations that the private sector will

need to comply with and it's a it's a an

effective means by which government can

help ensure greater security and safety

for the ecosystem the private sector

needs to ensure that we can comply with

that and the other regulations one of

the challenges we have in this space is

we're seeing a vast proliferation of

legislation and regulation around the

world often in conflict with one another

um which makes it very challenging for

the private sector to comply with these

different rules so we do need um you

know leaders in this space like in uh

the eu's work to to work to try to drive

harmonization globally so that we can

actually have an effective

um Global regulation because this is

technology whether you're a hyperscale

cloud provider like Microsoft or even a

much smaller company with a a great

technological innovation you want to

compete globally um in this these

markets and so you need to be able to

comply globally so it's a great initial

step in uh discharging government's

responsibility to help set the guard

rails for what is secure and safe

software and um and Services um

development and operations but we do

need that to evolve into a consistent

framework that enables Safety and

Security does not Innovation and

does not put the thumb on the scale of

competition I think that global point is

Election integrity

is a very important one 2024 is the

biggest election year in history four

billion people will be voting have the

American elections we have uh

parliamentarian elections in Europe

including the European Parliament

elections what can governments and

private

companies do together to address or to

ensure that these elections are without

interference from foreign actors and

that there's uh election Integrity you

know I think it's going to be a big

challenge for the private and public

sectors to help address um this this

risk um during the course of of this

year but there's a lot we can do

especially if we can work in close

partnership between the private and

public sectors and that really means

building new forms of strategic

collaboration that still don't exist

today where we can work together to

identify the greatest risks and how to

address those risks you know what we see

in the private sector what government

sees um can be quite different but if we

can work together to share that um

understanding then we can better then

decide what role is there for the

private sector what role is there for

government to address those risks and

try to minimize them there are key

things that we can do um we can work

together on identifying the ways in

which AI might be used for example to

try to influence the outcome of an

election and that could be done by um

providing you know so-called deep fakes

or synthetic media that misre represents

the actions or um positions or uh

otherwise tries to influence by by

convincing the voting public about

something that's false and inauthentic

about a candidate or a party um and so

that's one thing and the other thing

that we need to really be um aware of

and thoughtful about is how to ensure

that a foreign power cannot affect the

Democratic process itself the voting um

process and while there's in the past

there's been a lot of concern about the

extent to which um cyber uh tools and

weapons could be used to to influence

the counting of the vote and and to

distort counting of the vote I actually

think that's probably a less significant

concern today than the ability of nation

states to use um sophisticated cyber

enabled influence operations to try to

distort the vote to convince people for

example that they don't need to vote

today that the vote's going to continue

tomorrow for some reason or to send them

to the wrong polling place or to utilize

the wrong approach and technique to vote

so their vote isn't counted and that can

actually happen in a way that could

influence the outcome of an election and

so that's a place where public and

private sectors need to work closely

together um to counter those risks

Cyber crime

Microsoft's number one priority is of

course to keep our customers safe and

often we see the private sector in the

first line of defense at the same time

we see a rise in cyber crime and Bad Bad

actors can you say something about this

Challenge and a possible path forward

well um you know es especially in terms

of cyber crime there's uh several things

that we're doing um we're working with

law enforcement around the globe to try

to disrupt the infrastructure structure

that cyber criminals use to conduct

cyber uh enabled crime um they they have

to use um you know uh what different

forms of of the the systems that enable

the internet they have to use different

um Technologies and techniques and if we

can identify those and uh disrupt their

ability to use them so that it's much

harder to conduct cybercriminal activity

that would be one way that we could

reduce cyber crime at scale and we're

also working with the financial

community and governments on how we can

disrupt the way in which cyber criminals

get paid how the money that they steal

gets um ultimately transformed into

currency that they can access how Ransom

payments that might be made in Bitcoin

for example how we can track and disrupt

that and recapture those those funds for

the victims um we're doing all the that

work but I think the longer run is as I

mentioned earlier our ability to utilize

Ai and AI um uh Technologies to

recognize when cybercriminal activity is

underway and stop it in the fabric of

the ecosystem before the victim is ever

uh is is ever um compromised my last

Cyber security in 2024

question when you look at the year of

2024 what do you see on the horizon for

cyber security well I see 2024 as a year

of both huge um Challenge and huge

opportunity the reality is today the

volume of cyber crime the volume and

impact of nation state activity um is

increasing um and so those of us who are

defending against those uh those threats

and trying to make the digital ecosystem

a more safe and secure place we're

losing that battle battle today um and I

am concerned that especially as you

point out with this being such an

important election year um and with the

rise in the the amount of money that

cyber criminals are able to extract from

the system and the actual

commercialization of cyber crime cyber

crime as a business um which we've seen

develop over the last several years all

of these are are great threats that we

need to overcome and so that's the

challenge but the real opportunity comes

from the ability of the private sector

and the public sector working together

to counter those threats in some of the

ways um that that we can counter those

threats through the deployment of AI

through effective thoughtful regulation

um by governments of the private sector

to ensure that products and services are

developed and deployed in a secure way

um and uh and working together in

Partnership between the public and

private sector to advance that common

interest of a safe and secure digital

ecosystem I think we've got great

opportunity I think there are a number

of things underway things that we're

doing at Microsoft things the

governments are doing things and

projects that others in the private

sector have uh underway that show real

promise um of of achieving greater

Safety and Security but it's going to be

a challenging difficult hard year and

I'm hoping that by the time we get to

this time next year we will look back on

2024 as a real time of transition from

losing these battles to winning these

battles and getting ahead of the bad

guys let's hope we'll win that battle

thank you so much for coming thank