

**Transcript of Keynote Address at the RSA Conference 2017
“The Need for a Digital Geneva Convention”**

**Brad Smith
President
Microsoft Corporation**

**San Francisco, California
February 14, 2017**

BRAD SMITH: Good morning. As we’ve already heard this morning, we come together in San Francisco at a remarkable time. We live in a world of constant and at times turbulent change.

And when we think about the issues that we're here to talk about this week, when we think about cybersecurity, we are clearly dealing with a growing problem – a problem in need of new solutions.

I would like to take a few minutes this morning to ground ourselves in the problem and then talk together about some of the solutions I believe we have the opportunity to pursue together.


A growing problem in need of **new solutions**



74%
of the **world's businesses**
expect to be **hacked**
in the coming year

But let's start with the problems. The problems are clear. We see them everywhere. We see them in the customers who are worrying about being hacked. We see this in the data about the economic loss that will be suffered.

Increasing **nation-state** attacks



But more than anything, if you think about what has happened over the past year, if you think about the changes in cyberattacks, I think we should come together and reflect on one thing, one thing that has clearly made the situation even more challenging – that is the entry of more nation-state attacks. We've seen

cyberattacks move from enthusiasts to financial thieves to now governments around the world.

THE CHRISTIAN SCIENCE MONITOR

World | USA | Commentary | Business | Energy/Environment | Technology | Science | Culture | Books | Take Action | Q

USA


How Stuxnet cyber weapon targeted Iran nuclear plant

Researchers from California and Germany dove into the Stuxnet code and found it sought out specialized components used in Iran nuclear centrifuges -- and could cause them to explode.

By Mark Clayton, Staff writer | NOVEMBER 16, 2010

Stuxnet, the world's first known "cyber missile," was designed to sabotage special power supplies used almost exclusively in nuclear fuel-refining centrifuge systems, researchers studying its code have revealed. The discovery is another puzzle piece experts say points to Iran's nuclear centrifuge plants as the likely target.

While the discovery may seem just another bit of circumstantial evidence, it is a critical one that appears to all but answer a central mystery.



Iranian President Mahmoud Ahmadinejad visits the Natanz nuclear fuel enrichment facility outside Tehran in April 2008. (Reuters)

And think about the decade we are traversing. The decade began with a report about a prominent nation-state attack.

abc NEWS | U.S. | World | Politics | Lifestyle | Entertainment | Health | ...

US Charges 5 Chinese Military Hackers in '21st Century Burglary'

By PIERRE THOMAS and MIKE LEVINE
May 19, 2014

Five Chinese military officers were indicted by the U.S. today and charged with hacking U.S. companies to steal industry secrets about nuclear and solar power in what one official called "21st century burglary."

It's the first time ever that the U.S. government has formally accused another nation of using the Internet to break into U.S. businesses and shortly after the indictment was announced China suspended the China-U.S. Cyber Working Group.



ABC news video

We've seen these issues burst into the news in terms of geopolitical controversies.

Bloomberg Businessweek | Markets | Tech | Pursuits | Politics | Opinion

How Hackers Took Down a Power Grid

Ukraine was an easy target—but the U.S. has its own weaknesses.

by Jordan Robertson and Michael Riley
January 14, 2016 12:55 PM PST
From BloombergBusinessweek | Subscribe | Reprints

It was an unseasonably warm afternoon in Ukraine on Dec. 23 when the power suddenly went out for thousands of people in the capital, Kiev, and western parts of the country. While technicians struggled for several hours to turn the lights back on, frustrated customers sat motionless at their unlit tables in their offices' call centers.

We've seen them become even more pronounced.

The Washington Post


National Security

Sony Pictures hack appears to be linked to North Korea, investigators say

By Ellen Nakashima, Craig Timberg and Andrea Peterson December 3, 2014

Investigators say a crippling cyberattack against Sony Pictures Entertainment was probably the work of North Korea, in what would be the first known case of the reclusive nation using its growing hacking capability to cause major disruptions to a company in the United States.

The attack brought Sony, one of Hollywood's biggest studios, to a near-standstill last week, forcing employees to use paper and pens instead of their computers. Hackers also deleted files from hard drives, uploaded several unleased films to the Internet and leaked sensitive personal information



Sony Pictures Entertainment headquarters in Culver City, Calif. (AP/Wide World)

The Sony attack, I believe, in many ways was a turning point. Here was a nation-state attack not for espionage, not related to the military, but to attack a private company for engaging in freedom of expression around, as it turned out, not a terribly popular movie. (Laughter.)

CBS NEWS

NEWS SHOWS VIDEO MORE SEARCH

CBSAP October 15, 2014, 4:47 PM

The John Podesta emails released by WikiLeaks

144 Comments / 1 Share / 1 Tweet / 1 Stumble / 1 Email

Last Updated Nov 3, 2015 11:50 AM EDT

Katiana Kravchenko, Donald Judd, Nancy Cordes, Julianne Goldman, Reema Flores, Rebecca Shabad, Emily Schulheis, Alexander Romano, Steve Chingaris and the Associated Press contributed to this compilation

WikiLeaks says it has some 50,000 Hillary Clinton campaign emails, and on Fri. Oct. 7, it began leaking the personal emails Clinton campaign chairman John Podesta. The group said it would release emails every day until Election Day. Podesta acknowledged his emails were hacked, but has not verified the authenticity of the emails. He warned that messages may have been altered or edited to inflict political damage but has not pointed to any specific case of this.

Cybersecurity experts said on Thursday that Fancy Bear, a group of Russian-linked hackers, had infiltrated Podesta's email. U.S. intelligence officials last week blamed the Russian government for a series of breaches intended to influence the presidential election, and the FBI is investigating the breach. CBS News' Sherry

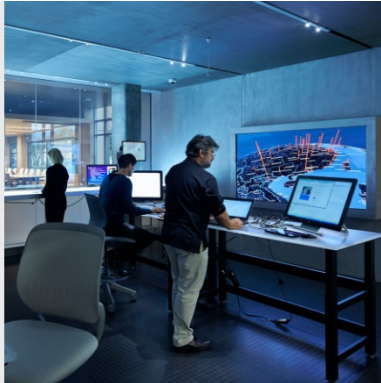


Podesta wrote:

CBS News

But it got our attention. And in the two and a half years since, we've seen these issues evolve even further.

Cyberspace is the new battlefield

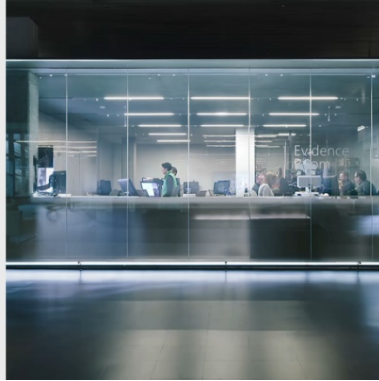


Let's face it, cyberspace is the new battlefield. The world of potential war has migrated from land to sea to air and now cyberspace.

But cyberspace is a different kind of space. Not only can we not find it in the physical world, but cyberspace is us. For all of us in this room, it is us.

Cyberspace is owned and operated by the private sector. It is private property, whether it's submarine cables or datacenters or servers or laptops or smartphones. It is a different kind of battlefield than the world has seen before.

We are the
first responders



And that puts us in a different position. It puts you in a different position, because when it comes to these attacks in cyberspace, we not only are the plane of battle, we are the world's first responders.

Instead of nation-state attacks being met by responses from other nation-states, they are being met by us.

From protecting civilians
in times of war...



And as we think about that change in the world, we should reflect upon one other as well. It's a sobering thing to think about, but consider this: For over two-thirds of a century, the world's governments have been committed to protecting civilians in times of war.

To attacking civilians
in times of peace...




But when it comes to cyberattacks, nation-state hacking has evolved into attacks on civilians in times of peace.

This is not the world that the internet's inventors envisioned a quarter of a century ago, but it is the world that we inhabit today.

What will we do?

And above all else, I think nation-state attacks call on us as employees, as an industry, as private citizens to ask ourselves one fundamental question: What are we going to do?



We **each** need to do more

We need to call on **governments** to do more

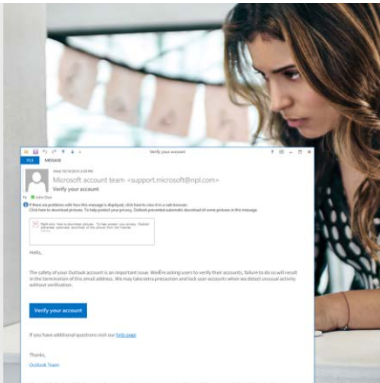
We need to act **collectively** to do more

I think there's three things that we should consider, and I'd like to talk about each of these three this morning.

The first is to start with what each of us has the opportunity to do ourselves, because everybody in this room and every company that is here is doing new and important things. We have all recognized that we each need to do more.

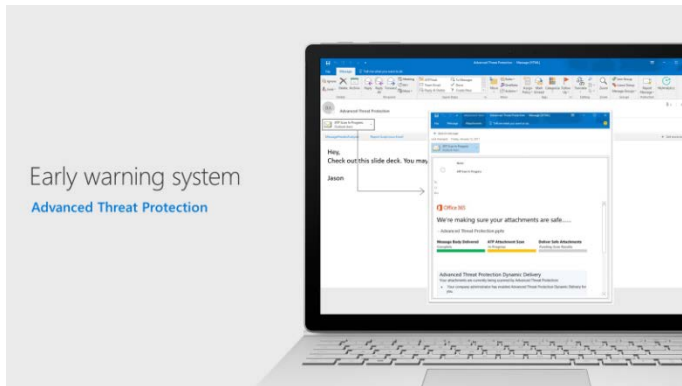
The first is to start with what each of us has the opportunity to do ourselves, because everybody in this room and every company that is here

At Microsoft, we're doing many things. In many ways, it starts with an obvious reflection. Just a few minutes ago, before I came on stage, somebody here in the audience tweeted that every company has at least one employee that will click on anything. (Laughter.)



90% of intrusions begin with a **phishing email**

That's why 90 percent of intrusions begin, unfortunately, with a phishing email. That's why we as a company, as one of the major email providers in the world, are so focused on strengthening email protection.



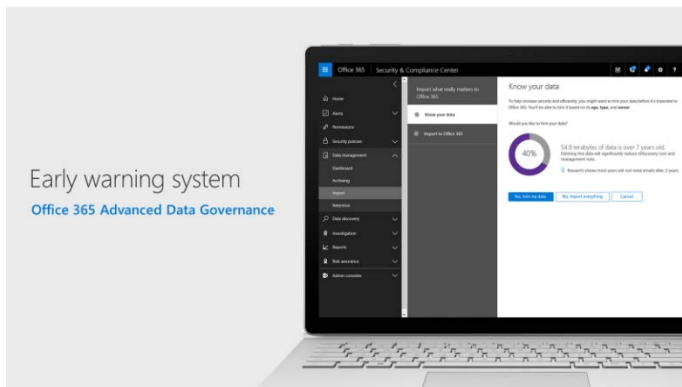
Early warning system
Advanced Threat Protection

Whether it was last year through our Office 365 Advanced Threat Protection that scans email, spots malware and destroys them before they can do damage ...



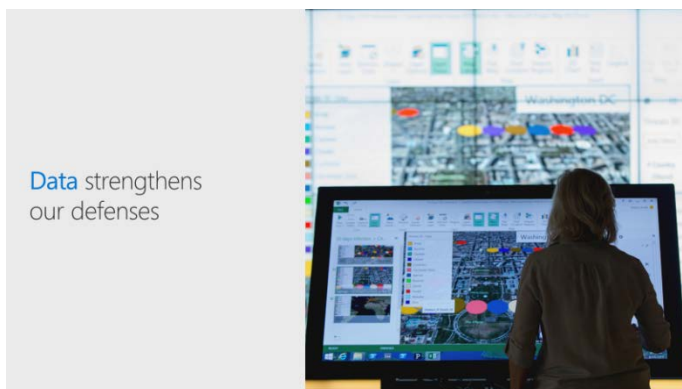
Early warning system
Threat intelligence

or the addition of our Advanced Threat Intelligence that informs enterprises of the nature of attacks and the people who are being attacked and makes recommendations....



Early warning system
Office 365 Advanced Data Governance

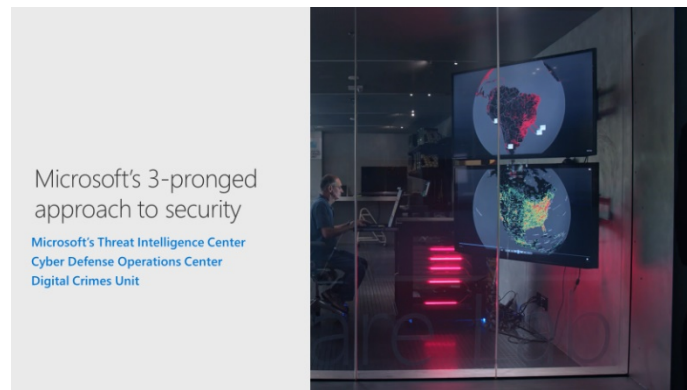
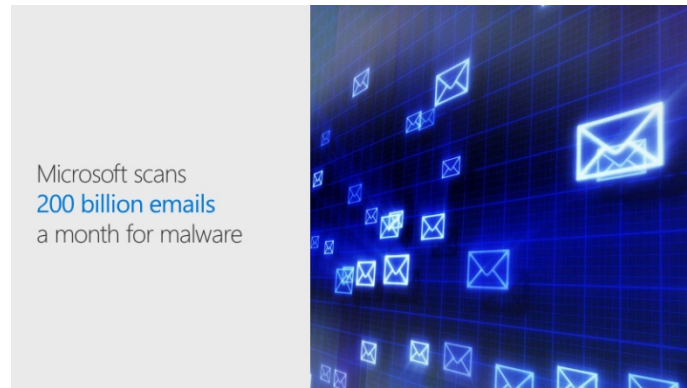
Or the announcement that we made last week about advanced data governance tools, tools that include alerts that let enterprise administrators and others know when someone is trying to download an email inbox.



Data strengthens our defenses

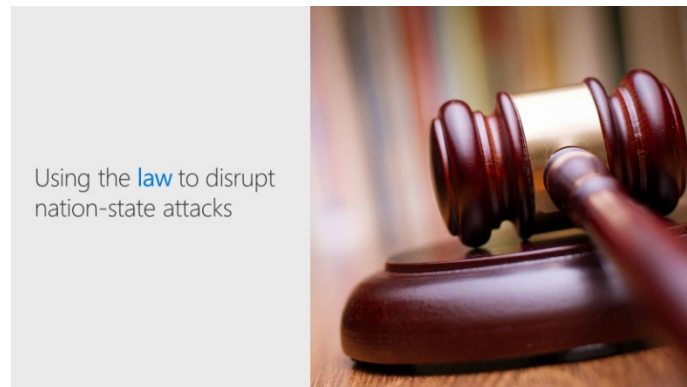
But I think we've all learned over the last couple of years that our single biggest advance in fighting all forms of cybercrime is probably not features, as important as they are, but instead, our ability to harness the power of data.

As a company, our datacenters are connected to over a billion end points. We get over a trillion data points each and every day. Our Advanced Threat Protection and our email scans 200 billion emails a month for malware. All of that data is the game-changing defense mechanism in our ability to combat this problem.



At Microsoft, we've built three groups and we've brought them together in what I think is a pretty unique partnership. It relies in the first instance on our Threat Intelligence Center, our reconnaissance arm, our people who are reviewing the data that is coming in from our 200 different cloud services.

When they spot a problem, they hand it off to our Cyber Defense Operations Center so they can go to work not only to protect our own services, but customers as well. And they, in turn, work with our Digital Crimes Unit so we can innovate in legal processes to take action.



Using the law to disrupt nation-state attacks

Starting last summer, we began to see new nation-state attacks that were aimed at creating fake domains, getting people through phishing attacks to click on them, and then using them, as we often see in these circumstances, to use malware to extract email from customers.



We innovated, we went to court, we got a new form of court order so that domain could be transferred to us and the data that was coming back from customers that were infected would go not to the attacker, but to sink holes that we created.

Using this approach, we've been able to address nation-state attacks and transfer 60 domains on six continents, letting the customers know that they were the victim of a nation-state attack and helping them clean up their system.

We are **far away** from declaring victory.

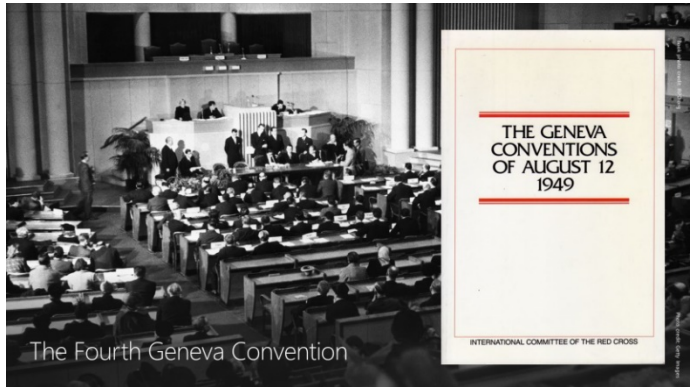
That's a step forward. But more than that, I think we all need to recognize the obvious. We are far away from declaring victory.

We are going to need to do more and we are going to need to do more together if we are going to address this problem effectively.



We need to recognize that the time has come for us to come together as an industry around the world to call on the world's governments.

We need to call on the world's governments to come together.



They came together in 1949 in Geneva, Switzerland, and that is what led to the recognition that they needed the Fourth Geneva Convention to protect civilians in times of war.

Now is the time for us to call on governments to protect civilians on the internet in times of peace. And there is progress on which we can build.

POLITICO

U.N. body agrees to U.S. norms in cyberspace

By JOSEPH MARKS | 07/09/15 12:44 PM EDT

A United Nations body has agreed for the first time that there are rules of the road in cyberspace that all nations should respect, even during peacetime, a senior State Department official tells POLITICO.

It's a breakthrough for U.S. diplomats, who have been pushing these "norms" as an alternative to formal treaties as a way to help tame the lawless frontier of cyberspace.

The norms agreed by the U.N.'s Group of Governmental Experts include understandings that nations should not intentionally damage each other's critical infrastructure with cyberattacks; should not target each other's cyber emergency responders; and should assist other nations investigating cyberattacks and cybercrime launched from their territories.



BERLIN, GERMANY — DECEMBER 27: A participant looks at lines of code on a laptop on the first day of the 28th Chaos Communication Congress (28CC) — Behind Enemy Lines computer hacker conference on December 27, 2011 in Berlin, Germany. The Chaos Computer Club is Europe's biggest network of computer hackers and its annual congress draws up to 3,000 participants. (Photo by Adam Berry/Getty Images)

Just two years ago, in the summer of 2015, experts from 20 nations came together and put forward a new set of norms, principles that governments could consider. It represented a big step forward in terms of international agreement.

US-China agree to not conduct cybertheft of intellectual property

Everett Rosenfeld with Reuters
Friday, 25 Sep 2015 | 1:39 PM ET

The U.S. and China have agreed that neither government would support or conduct cyber-enabled theft of intellectual property, U.S. President **Barack Obama** said in a joint media conference with Chinese President Xi Jinping on Friday.

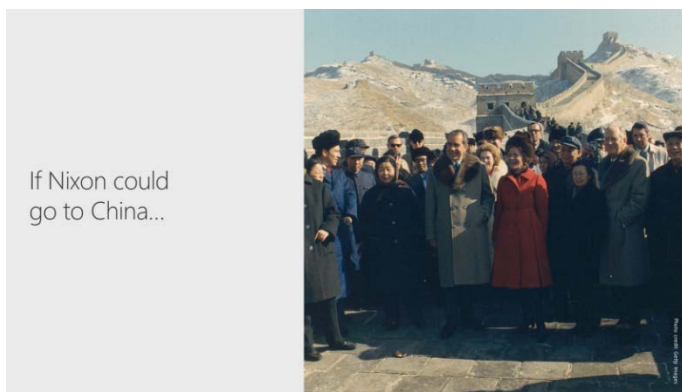
The Obama administration said that both countries are committed to finding appropriate norms of state behavior in cyberspace within the international community. The countries also agreed to create a senior experts group for further cyber affairs discussion, the White House said.

OBAMA, XI OUTLINE GOAL FOR CLIMATE CHANGE PACT

CNBC video

And more encouraging in many ways still was what happened a few months later when the United States and China sat down across the negotiating table, talked directly and frankly about an issue that was important to both of them, and came up with a new pledge and plan to put the cybertheft of intellectual property

out of bounds. That was then endorsed by the G20 two months after that.



Let's face the obvious. There are new issues that we need governments to come together and address in 2017. There is an opportunity for a new president in the United States to sit across the table with the president from Russia and take another step forward to address the attacks that concern the world.

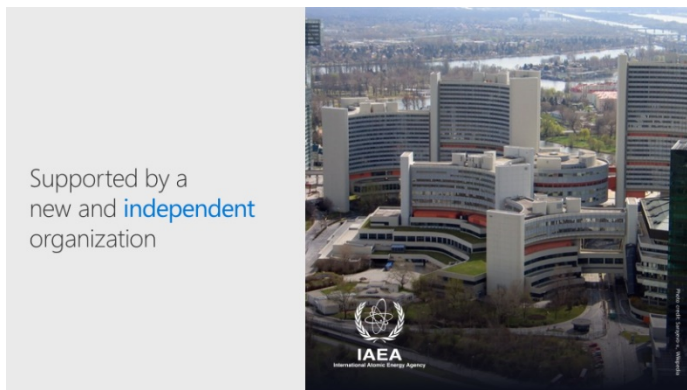
A Digital Geneva Convention

1. No targeting of tech companies, private sector, or critical infrastructure
2. Assist private sector efforts to detect, contain, respond to, and recover from events
3. Report vulnerabilities to vendors rather than to stockpile, sell or exploit them
4. Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise, and not reusable
5. Commit to nonproliferation activities to cyberweapons
6. Limit offensive operation to avoid a mass event

And we then need to build on that with a global convention. What we need now is a Digital Geneva Convention. We need a convention that will call on the world's governments to pledge that they will not engage in cyberattacks on the private sector, that they will not target civilian infrastructure, whether it's of

the electrical or the economic or the political variety.

We need governments to pledge that, instead, they will work with the private sector to respond to vulnerabilities, that they will not stockpile vulnerabilities, and they will take additional measures.



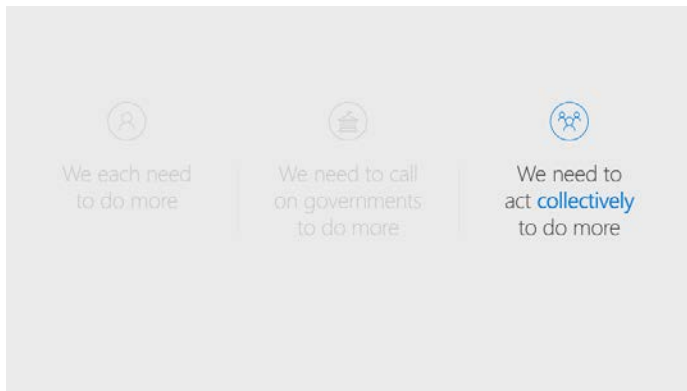
Supported by a new and **independent** organization

And, perhaps as much as anything else, we need governments to take a page out of the 1949 Geneva Convention and other instruments that have followed. What the world needs is a new independent organization, a bit like the International Atomic Energy Agency that has addressed nuclear

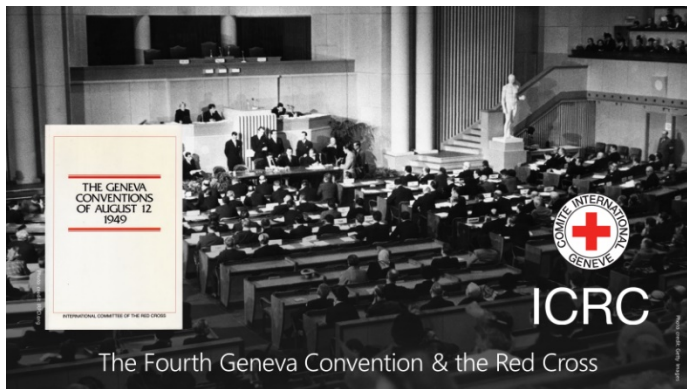
nonproliferation for decades.

We need an agency that brings together the best and the brightest in the private sector, the best and the brightest in academia and the public sector. We need an agency that has the international credibility not only to observe what's happening, but to call the question and even identify the attackers when nation-state attacks happen.

That is the only way that governments will come to recognize that this is not a program that will continue to pay off. That is all in the area of steps we need governments to take.



But there's a third area we should touch upon as well. It also calls on us. It's great that we do so many things alone. We now need to do more together.



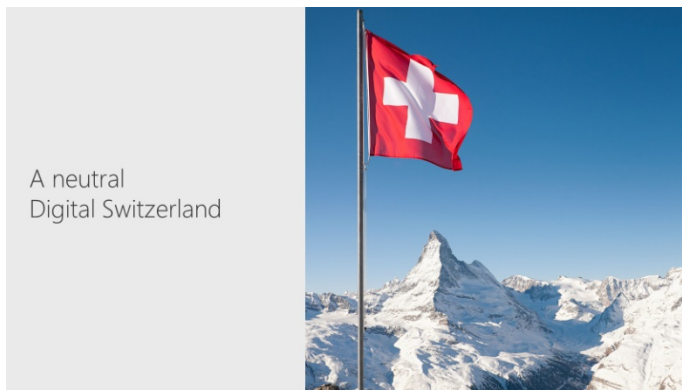
If you look back at what happened in 1949, the world's governments realized that they could not protect civilians in times of war without a private organization – the International Committee of the Red Cross.

While we don't have the same kind of organization, we have within these walls many people from many organizations. And as a global technology sector, we need to come together as the ICRC did in 1949. We need to sign our own pledge in conjunction with the world's states.

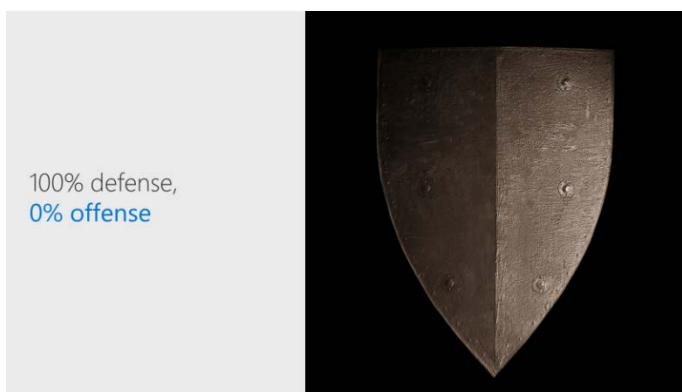


We need to pledge that we will protect customers, that we will focus on defense. We need to be concrete in showing and pledging how we will collaborate with each other to respond to attacks. That we will provide patches to all customers everywhere, regardless of the attacks that they face. That we will do our

part to address the world's needs.



In effective, even in an age of rising nationalism, we as a global technology sector need to become a trusted and neutral Digital Switzerland.



We need to be a global industry that the world can rely on to play 100 percent defense and zero percent offense.

We will assist and protect customers **everywhere**.

We need to make clear that there are certain principles for which we stand.

We need to be clear that we will assist and protect customers everywhere. That is what we do regardless of the country from which we come.

We will not aid in attacking customers **anywhere**.

We need to be clear that we will not aid in attacking customers anywhere, regardless of the government that may ask us to do so.

These two principles have been at the heart and soul of what we've been doing at our company, at your company, and across the industry. We need to stay on that path.

We need to retain the **world's trust**.

We need to make the case to the world that the world needs to retain its trust in technology. We need to retain the world's trust.

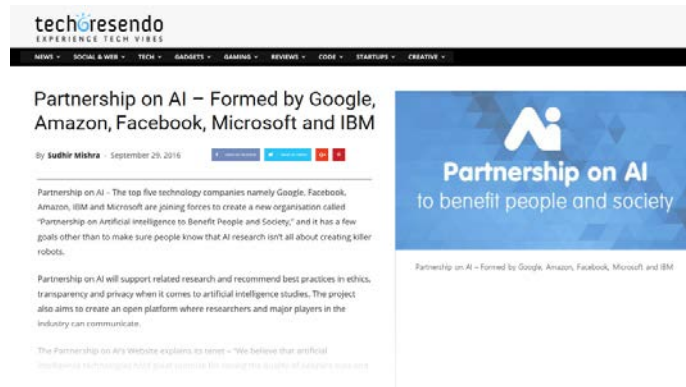
Every government, regardless of its policies or politics, needs a national and global IT infrastructure that it can trust.

And regardless of a government's politics or policies or individual issues at any moment in time, we need to persuade every government that it needs a national and global IT infrastructure that it can trust. And the only way it can have that is if it knows that our industry is focused on protecting everyone everywhere, and

attacking or assisting in attacking no one, anywhere, at any time.

As we think about all of these things, I think there's a lot on which we can build.

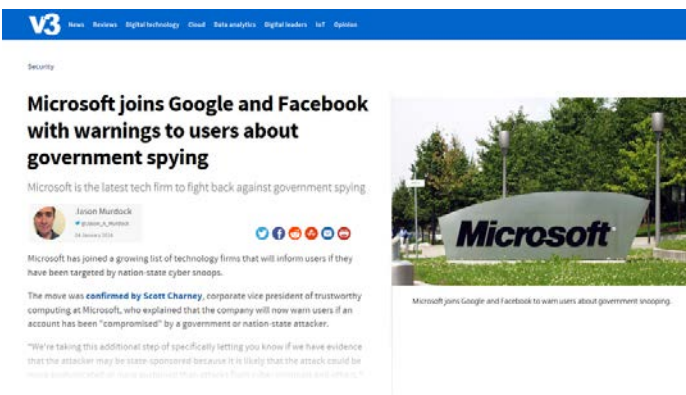
Because the truth of the matter is even though we work in a hypercompetitive and fast-changing industry, I would say that our industry has never been more united. It is coming together to address new and challenging issues, whether it's the questions around artificial intelligence that the world is increasingly talking about.



We're not just working together in new and important ways, we are learning from each other. I think a sense of humility is a positive force that can affect and help us all.

Certainly at Microsoft, we've appreciated the leadership that Google and Facebook first took with respect to nation-state attacks.

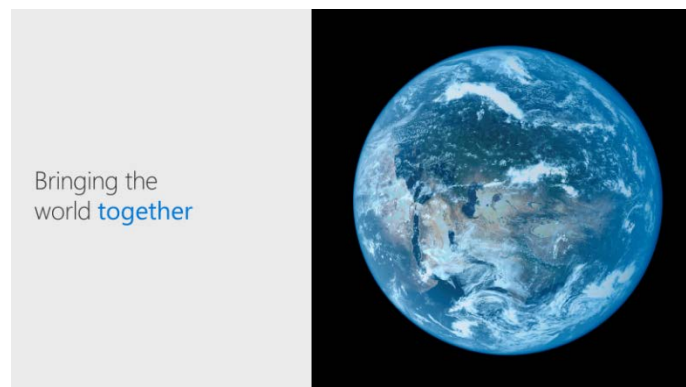
And we quite obviously, adopted what was working for them because



we believed it would work for everyone.

And as we think about the opportunities that we have to work together, as we think about our role in the world today, just as we came together last year at an important moment in time when everyone was focused on the Apple case, there is an obvious

issue that is uniting our industry today that I think has some relevance as well.



As the country and the world talk about immigration, they look at the technology sector. And they recognize that as an industry, we in many ways have brought the world together.

We bring the world together through our technology and our products and the connections that we forge with people across borders every day.



But it's more than that. We almost uniquely have brought the world together under our own roofs.

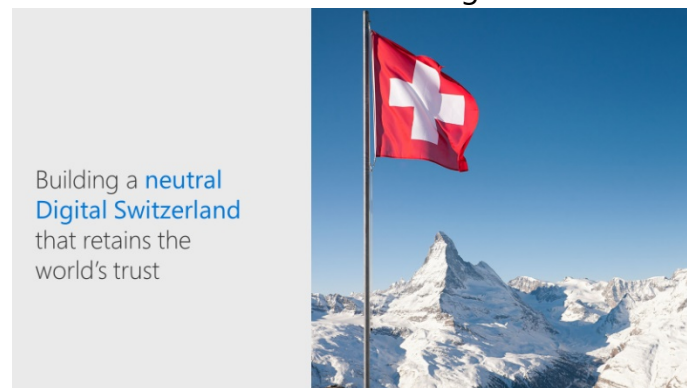
At Microsoft in Washington State where I work, a high majority of our employees were born and grew up in the United States. But we also have employees from 157 countries. Every

day, when I park my car and I walk into the office, I sometimes reflect upon the fact that I feel that I work at the United Nations of information technology. And our company is not unique. Every company in our industry is like that.

We have brought the world together. And it has put us in a position to forge perhaps almost a unique level of mutual understanding and respect for the needs of people around the planet.

As we think about protecting the planet, as we think about addressing nation-state attacks, that is a powerful force that should inspire us, and on which we can build.

Let's use that inspiration. Let's use what we have learned. Let's build on what we can share with each other. And let's go forward and show the world that it needs us to be



what we can be when we're at our best – an industry that can serve the world. An industry that earns everyone's trust every day. An industry that even in an age of nationalism, is a neutral Digital Switzerland on which everyone can depend and rely.

Thank you very much. (Applause.)

END