Speech by Vice-President Ansip on cybersecurity at the RSA Conference 2018

"Ladies and gentlemen,

It is a pleasure to be with you today. Many thanks for inviting me to San Francisco.

When it comes to cyber-attacks, you could say my experience is somehow special.

Estonia is a small Baltic nation on the edge of Europe. We not only share a border with Russia, we also have a long and difficult history together.

In 2007, I was Prime Minister of Estonia. Over three weeks, my country was the target of an orchestrated cyber-campaign to destabilise parts of our online presence and civilian infrastructure. It was a watershed moment. I learned a lot of lessons in 2007.

The main one was that there is no substitute for informal and rapid information exchange – internally and with our allies. That is how Estonia got through its cyber-crisis – thanks to the support of others, including the United States. Realistically, no country can succeed alone.

Now, I am using that experience at the European Commission in Brussels, where I am responsible for creating a Digital Single Market for the European Union.

In 2007, cyber-attacks were used as a weapon to achieve political goals. This was a strong signal to the whole world that cyber space would very likely be used in the future to attack independent countries. Since then, we have seen that many other countries have been on the receiving end.

Malicious cyber-activity has proliferated. It has become more brazen and sophisticated, more imaginative and international.

Misinformation is another widely used tool of political influence.

In Russia, for example, military doctrine sees cyber operations as part of its tactics for information warfare. Deception, false data, and destabilising propaganda are deemed legitimate tools to convince people to 'buy' the disinformation message as credible information.

It is a sad truth – but if you repeat false information often enough, sooner or later some people start to accept it as true.

Three years ago, EU leaders decided they had had enough – and so a special team was set up to improve Europe's forecasting and response to pro-Kremlin 'information weaponising'.

In its first two years, it identified more than 3,500 examples that contradicted publicly available facts. Here are some from the last month that name the United States directly:

Take this one:

"Americans poisoned Russian ex-spy Skripal and daughter to spread Russophobia". That came from the "60 minutes" programme broadcast by the Russia 24 channel. It is owned by the Russian state.

Or this one, from NTV – controlled by Gazprom Media: "The US intelligence services are planning to kill one of the presidential candidates in Russia".

Both examples push a conspiracy theory, but with no evidence to back it up. And it continues today, multiplied across many languages and repeated daily.

A huge propaganda machine. Who would be in a position to pay for that, if not a government?

In Europe, as in the United States, we remain on the frontlines of these assaults on democracy, threatening to undermine institutions.

A welcome development in this cyber-gloom is that there is now more willingness to name perpetrators, even if it concerns a specific country rather than individuals.

Given the scale and scope of the threats, people should name names, if they can. Collective attribution makes us stronger against the threat, wherever it is from.

The world faces a new strategic environment: one where we should help each other even more.

To me, it is why the EU-US partnership needs to stay strong: for security and prosperity of both sides of the Atlantic.

On cybersecurity, Europe is already working with the United States.

I would like to see more cooperation – perhaps to explore the idea of a secure transatlantic cyber area to deter cyber-attackers.

For example, we have proposed EU certification for cybersecurity products and services. This should be a good basis to discuss and make sure that our cyber standards are aligned on both sides of the Atlantic.

If both sides could agree on common security standards for the IoT, this would set a global standard. Exchanging detailed information about cyber incidents will help to prevent future attacks. We are in the same boat here: if Europe is the target today, the United States could easily be under attack tomorrow.

Transatlantic cooperation on cybersecurity will help to maintain secure and open data flows between the United States and Europe: they are the world's

highest, after all. But that also depends on trust.

Trust is easy to break – and difficult to rebuild, as the world has seen with the recent case of Cambridge Analytica.

If people feel their privacy has been violated, their digital profiles misused, then they will react accordingly. And when online trust is eroded, any digital economy will find it hard to advance.

As you probably know, the EU's GDPR enters into full force next month:

– it will reinforce all our data protection rules, give people more control of their data, and set the rules on profiling and data portability.

– it will force companies to be more responsible and accountable in how they deal with our data.

– and it is practical: companies will no longer have to follow 28 different country laws: just one for all of Europe.

While it contains financial penalties for non-compliance, this is a last resort – we have to make sure that the rules work in practice. They are fit to tackle the constant hunger for increased monetisation of data and targeted advertising. They have already changed how businesses deal with our data, and not only in Europe.

Frankly, I would advise companies to invest in data privacy in the first place. Both the EU and United States have a strong commitment in this area.

Here, I am thinking of the Privacy Shield. This makes sure that privacy is respected when the data of Europeans is sent to the United States. It is already being used by more than 2,700 companies; incidentally, also by Cambridge Analytica.

This just shows how crucial it is for the Privacy Shield to be an effective and enforceable instrument. There is a lot still to be done, certainly in the United States.

We are also closely following the FTC's investigation into the Cambridge Analytica case.

Artificial intelligence (AI) is another example. This technology is already with us – globally – and evolving fast. It raises issues of cybersecurity, privacy, ethics as well as protection of fundamental liberties.

These issues concern us all, which is why we should lay down some common principles on how AI is developed and deployed. And we need to do this now.

If we fail to do so, if the West fails to unify – we risk being exploited by those who would use cyberspace as a weapon to harm our free and open societies and economies.

By not acting, we make ourselves an easy target.

Digital innovation should not be abused like this, I think you would agree. The perpetrators are operating on a global and daily basis, and that is not about to change. We have to fight it together – to prevent, deter and respond. Constant vigilance and cooperation. But it is not only about defeating threats. There is a lot to be positive about, especially when we work together.

After all, this is about building a thriving transatlantic digital economy, so that we all benefit. A bright global digital future.

Thank you."

ESMA updates bonds transparency calculations for MiFID II/MiFIR

18 April 2018

MiFID – Secondary Markets

The European Securities and Markets Authority (ESMA) has updated today its MiFID II/ MiFIR transitional transparency calculations (TTC) for bonds.

The update relates to the liquidity assessment for bond instruments except for ETCs and ETNs. Trading venues are expected to apply the new results from 23 April 2018.

Speech: Syria: International Impartial and Independent Mechanism

Thank you very much, Mr Chairman, and we associate ourselves with the statement made earlier by the European Union. This first report of the International Impartial and Independent Mechanism is extremely welcome. It's an important initiative from Lichtenstein and Qatar and we join other colleagues in congratulating Catherine Marchi-Uhel, on her professionalism in setting it up.

The establishment of the IIIM was an important step forward in ensuring accountability for the horrific atrocities that have been committed in Syria.

These include torture in Asad's prisons, the unlawful targeting of civilians and civilian objects, including medical facilities, and as everyone knows, the use of chemical weapons. It's up to all of us to support the IIM in building and bringing cases against perpetrators before any competent tribunal.

The UK strongly supports the IIIM. We co-sponsored the UNGA resolution in December 2016 that set it up and we have contributed over a quarter million dollars to its start-up costs. We will make a further contribution later this year and I take this opportunity to encourage all Member States financially to support this important mechanism.

The barbaric chemical weapons attack in Douma on the Syrian people 11 days ago cost up to 75 lives including those of young children. But it was only the latest atrocity in this seven year conflict. We must ensure that those responsible for this crime are held to account. And I would like to take this opportunity to take a few moments now to set out the UK's response along with French and American allies to the attack on Douma. Mr Chairman, the military action we took last week was a strictly limited operation. We have published our legal position on our action. As it sets out, the action was taken to alleviate the extreme humanitarian suffering of the Syrian people by degrading the Asad regime's chemical weapons capability and by deterring their further use. We determined that there was no practicable alternative to the use of force if lives were to be saved and that the strikes were necessary and proportionate, the minimum necessary.

Mr President, it cannot be illegal to use force to prevent the killing of such numbers of people. We hope our actions will also uphold the international norms prohibiting the use of chemical weapons. I would like to stress this is not about intervening in a civil war or about regime change. And it was not about a one-off use of chemical weapons by the Asad regime. Four cases, including one of Sarin, were documented by JIM before it was shut down in 2017. We cannot allow the use of chemical weapons, which as everyone knows are prohibited under international law, to become normal, either within Syria or elsewhere.

In 2014 Russia vetoed a resolution calling for the situation in Syria to be referred to the ICC so that there could be accountability for all the atrocities that we have seen in Syria. To date, Russia has vetoed 12 Security Council resolutions aimed at alleviating the plight of the Syrian people. This makes the work of the IIIM even more important.

We commend the work that it has already undertaken to establish cooperation with Syrian civil society, international organizations including the UN Commission of Inquiry and Member States. We encourage the IIIM to investigate CW attacks, particularly in the absence of any international attribution mechanism for CW.

We must demonstrate that those who have committed the most serious crimes of international concern can have no place to hide. There must be no impunity for the horrendous acts taking place on a daily basis in Syria. There must be justice for the victims. It may take a long time. Sadly, I fear it will take

a long time but there must be justice. I'd like to close if I may Mr President by just endorsing what the French ambassador had to say about next steps on the political side and assuring the General Assembly that the United Kingdom will devote every effort to that end.

Thank you.

Press release: PM meeting with New Zealand Prime Minister: 18 April 2018

A Downing Street spokesperson said:

> The Prime Minister held a bilateral meeting with the New Zealand Prime Minister Jacinda Ardern at Downing Street earlier today.
>
> They agreed the bond between the UK and New Zealand was unique and enduring, based on friendship and shared values, and underpinned by strong security, prosperity and people-to-people links.
>
> The Prime Minister said New Zealand was an indispensable partner for the UK, noting the relationship has always been important, but is arguably even more vital today, given our shared commitment to free trade and protecting the rules-based international system.
>
> The Prime Minister thanked Prime Minister Ardern for New Zealand's support over the attack against the Assad regime, and following the chemical nerve agent attack in Salisbury. They agreed it was essential to reassert the international norm against chemical weapons use.
>
> They agreed that part of reinvigorating the Commonwealth was about fostering more intra-Commonwealth support, and to explore the possibility of working together on development assistance in the Pacific region.
>
> They also discussed the bilateral trade and investment relationship, agreeing that UK-New Zealand trade working group discussions were progressing well and confirming our shared ambition to form a new bilateral UK-New Zealand Free Trade Agreement once we have left the EU. They welcomed the approach agreed at the March European Council to provide continuity during the implementation period for international agreements, which could be swiftly transitioned into new bilateral agreements once the implementation period ends.

Second defeat in one night for the Government on Brexit!

An amendment providing enhanced protections for employment, equality, health and safety entitlements, rights and protections, and consumer and environmental standards has been passed in the Lords.

Go to Source
Author: