A Comprehensive Approach to Evolving Cyber Threats

26 January 2017, Oxford

It is a pleasure to be here.

The threats we face as societies are in flux. Terrorism, radicalisation, and organised crime remain firmly in the top five. But as everybody in this room knows there is a virtual threat with real consequences that is growing in strength, in impact and in prevalence. Cyber-attacks, cyber security and cyber resilience are issues that have morphed from being in the background to being front and centre to national and global security. And because this is a digital rather than an analogue threat, the pace of evolution poses a real challenge to those of us tasked with countering it.

But you all know that already...which is why I'm looking forward to tonight's discussion.

This does not mean other threats have disappeared – organised crime has not gone away, and there are worrying signs from radical groups on the extreme left and extreme right. Threats can change very quickly and we must remain vigilant. But right now, the most persistent and present threats are not only those posed by jihadi inspired terrorism but also cyber threats, in all their forms.

From where I sit in Brussels, it seems that although the threats posed by cyber are not new, what has changed is the scale of them and their increasing diversity. The actors are not only criminals – with ransomware, malware and phishing – driven by a profit motive; but also state and non-state actors who see cyber as a valuable – and deniable weapon. As Eric Schmidt and Jarad Cohen noted recently "in future all wars will begin as cyberwars".

In terms of the criminal threat - reports last week highlighted that cyber offences accounted for about half of all criminal offences in the UK. Online fraud is now the most common. crime in the UK with almost one in ten people falling victim. Half of all companies in Europe have experienced at least one cybersecurity incident. Globally, the cost to society of cyberattacks and cyber hacking in 2015 was estimated by Grant Thornton to be around $315 billion. The growth in this area has been exponential. The increasing interconnection of our systems and networks means these numbers will only grow in years to come.

The World Economic Forum's Global Risks Report 2017 lists "massive incident of data fraud or theft" as one of the five major global risks in terms of likelihood.

In terms of the threat from state and non-state actors, we have moved from a situation a decade ago where cyber-attacks were used as a form of punishment – against Estonia in 2007 for moving a statue – through cyber as a non-military means of achieving a military objective – the 2010 Stuxnet attack on the Iranian nuclear enrichment programme - to one where they are used in Death Star style demonstrations of power – the 2016 closing down of Ukraine's power grid. Added to this – and worryingly for an EU with several national elections this year - is the new found capacity for cyber to be used to manipulate democratic processes. It is not hard to see how a false email inserted in a hack of thousands laundered through Wikileaks could have a powerful influence on public opinion.

An indicator of the seriousness with which this threat is being treated comes from the fact that it has been highlighted by the heads of the Secret Services in countries like the UK and Germany. Our first response must be to talk about these attacks – because those who commit them want to stay in the shadows and we must shine a light on them and their activities. That's our first line of defence.

So the risks posed from cyber seem to be ever more present, and ever more dangerous. And we're all concerned as some attacks target you and me as the average consumer on their computer at home or at work; others target companies – big and small, government and all other institutions. In the Commission, we saw an increase of 20% in the attacks on our servers in 2016 compared to 2015.

Although the source and nature of these threats is extremely varied, our response to them will have much in common. Principally, we need to make ourselves less vulnerable – strengthening our protection and resilience to attacks. We also need to be able to manage and mitigate attacks when they do happen, and prosecute those who carry them out.

It's these issues I want to develop with you this evening.

***

Cyber-attacks do not take into account geographical borders and can be achieved at a low cost with devastating effects including posing a risk to our internal security. I'm reliably informed that I can rent a Botnet for the afternoon on the Dark Web for a modest sum which I could use to launch a Distributed Denial of Service attack against anyone I felt like... So let's hope the evening goes well...

As the Internet of Things grows we are inadvertently lowering the threshold both in terms of cost and availability for these attacks. My smart fridge and TV have factory set security codes – insecurity by design. This needs to change.

Our policy response has four strands:

1/strengthening our cyber resilience

2/stepping up the fight against cybercrime

3/increasing support for innovation in the field of cybersecurity

4/strengthening international cooperation

I. Strengthening our cyber resilience

The NIS Directive (NIS) on the security of networks and critical information was adopted last July. It aims to ensure that:

— All EU Member States have a national Cyber Security Strategy, a national authority responsible for network and information security, and Computer Security Incident Response Teams (CSIRTs) in place by the time the Directive enters fully into effect - i.e. by May 2018.

—cooperation between CSIRTs and EU Member States at EU-level is strengthened;

—critical networks are appropriately protected. This means that Operators of Essential Services need to be designated (in the energy, water, health, transport, banking, financial markets, and digital infrastructure sectors). These Operators will be obliged to report "incidents of significance" having an impact on the continuity of essential services.

In addition, in 2012, an emergency response team (CERT-EU) was put in place to respond to cyber threats and attacks within the European institutions and agencies. CERT-EU also works in cooperation with the Member States.

Implementation of this directive by all Member States is the most important step we can take to ensure greater protection of our key infrastructure, and a greater shared understanding and cooperation between all the main actors. But it's of course not enough.

We also need law enforcement and judicial authorities to have the necessary means to find and punish cyber-criminals.

II. Step up the fight against cybercrime

The European Cybercrime Centre at Europol (EC3) has a key role to play in that respect.

In recent months, it has worked with the Dutch Police and the private sector to launch an initiative against ransomware. This initiative helps alert victims and provide them with the necessary tools to decrypt their software and recuperate information. More than 2500 machines have been decrypted – free of charge – thanks to this initiative.

Let me give you another recent example. On 30 November 2016, law enforcement authorities took down a vast international criminal infrastructure known as Avalanche.

The operation involved law enforcement and judicial authorities of 30 countries – and coordinated by Europol and Eurojust.

As a result, five individuals were arrested, 37 premises were searched, and 39 servers were seized. Victims of malware were identified in over 180 countries. This example underlines the importance of European and international cooperation on cybercrime.

Eurojust has also recently stepped up its work with the introduction of a European network to fight cybercrime, and bring together judicial authorities.

Setting up an appropriate legal framework at an EU level is also necessary. Access to evidence is vital in the fight against cybercrime. The European Commission has launched a consultation to discuss solutions to facilitate this access, including by working more closely with online service providers. The Commission is also working to simplify and speed up requests for mutual legal assistance.

The issue of encryption is a sensitive but an important one in this context. Encryption is essential in terms of data protection and should not be called into question. However, in the context of criminal investigations, in particular relating to terrorist cases, judicial authorities also legitimately need access to data – both potentially to prevent further attacks and in prosecution cases. We need to think about solutions to that effect, of course fully respecting the protection of fundamental rights and individual freedoms.

And in all thus, we need to continue to work together with the private sector, as a key partner in the fight against cybercrime and cyber security threats.

III. Increasing support for innovation in the field of cybersecurity

If we want to be better protected against cyber threats, we need to build in "security by design" and we must support and assist companies operating and innovating in the field of cybersecurity.

There is lots of great research going on – and many of you around this table are involved in it and I hope to hear more about the projects you're involved in. But we need to make sure the findings of research - when appropriate - are properly disseminated and there is market take-up.

The EU helps with funding– in numerous ways. Last summer, we launched a new public-private partnership that is expected to trigger EUR 1,8 of investment by 2020, with the EU providing EUR 450 million through Horizon 2020.

And cybersecurity market players, represented by the European Cyber Security Organisation are expected to invest three times more. This partnership will also include members from national, regional, and local public administrations, research centres, and academia; with the aim fostering cooperation at early stages of the research and innovation process and building cybersecurity solutions for various sectors, such as energy, health, transport, and finance.

In addition, the Commission is working on different measures to tackle the fragmentation of the EU cybersecurity market. Currently an ICT company might need to go through different certification processes to sell its products and services in several Member States. With ENISA, the European Agency for Network and Information Security, the Commission is looking into the possibility of setting up an EU certification framework for ICT security products.

IV. Reinforcing international cooperation

Before concluding, I would just like to touch on the importance of the international dimension in the field of cyber security. The European Commission supports cyber capacity building in third countries as well as international cooperation in the field of cyber-security. 45 million euros have already been invested by the EU in this field.

Moreover, the European Union is a founding member of the Global Forum on the expertise of cybercrime (GFCE), a multi-country platform enabling countries, international organisations and participating companies (currently 55 participants, including 11 EU Member States and Europol) to exchange good practices and expertise in order to facilitate the establishment of partnerships to build capacity.

Conclusion

The interconnected world in which we live today offers many opportunities for citizens, governments and public and private actors. However, it also offers unprecedented opportunities to criminals, terrorists, and hostile states. That is why it is essential to work together to build resilience and to drive technological innovation, at a European level and in the context of our relations with third countries, in order to strengthen our collective efforts to combat cybercrime and cyber security threats.

Finally, we need to plan for the future – because cyber threats are not going to go away. The EU's cybersecurity strategy dates back to 2013. It's ancient history in a world that is moving so fast. We must be ready for whatever the future holds.

***