Keynote Speech “Building an effective and sustainable Security Union”

# Speech at the Seminar on the "EU Global Strategy on Security and Defence" organised by the Former Members' Association of the European Parliament

# Brussels, 30th November 2017

## Introduction

Security has long been regarded as a major issue for national authorities; and that remains the case. But with this Commission that perception has begun to shift.

Now we are beginning to see how easily the terrorist threat crosses borders with no respect for national boundaries.

There is a common terror threat, from those inspired or trained by Da'esh. They plot attacks targeting public places which people visit from across Europe and the world. Their focus is to destroy the values that we share as Europeans: openness and tolerance.

And we have seen their tactics evolve; with the emergence of "low-tech" terrorism, carried out with little more than a truck or a knife. from Nice, to Berlin, to London and Barcelona.

But we have also seen cyber attacks that have struck many different countries. Major attacks such as WannaCry and ongoing concern about foreign cyber interference, have shown the potentially devastating impact cyber attacks can have on our internal security, even raising questions on our democratic institutions themselves.

Faced with such cross-border, transnational threats, there has been a growing realisation of the role the EU can play. A common threat merits a common response.

This has an institutional implication. The Commission President created – for the first time – a Commissioner for security.

The European Parliament has formed a new special committee on terrorism.

And the Member States, are cooperating ever more. They share ever more law enforcement information with each other. And through cooperation between their different intelligence services – albeit not under an EU framework.

Earlier this week I spoke to the national Parliaments of the EU, in the COSAC plenary. And they, too, are well aware and supportive of the need to work together to improve our collective security, online and off.

The EU acts where it can add value. And today I'd like to set out the various ways the EU can do so, supporting the work of national authorities whose primary role it is to keep us all secure.

**Using the single market**

First, of course, we can use the power and scale of our single market.
Take cyber security. All the new billions of devices coming online for the internet of things will need to demonstrate they are secure. It is far easier, for all concerned, if manufacturers have to do that once, rather than 27 times. Last September, we proposed an EU certification framework for ICT products and services.
Mr KALFIN will speak about it in more detail.

Cooperation on research can also help us build digital investment, capability and security within the single market. We already have a Public-Private

Partnership on cybersecurity, and can build on that: through a network of cybersecurity competence centres, with a new European Cybersecurity Research and Competence Centre at its heart.

## Cutting terrorists' means and money

Second, we can close down the space in which terrorists and attackers operate.

We have already legislated, for example, to cut access to the firearms and explosives used by terrorists; to tackle money laundering; to criminalise those who travel to the Middle East for terrorist purposes, or those who help or train or fund them. But we can strengthen our response further.

Many recent attacks have used the explosive TATP; it is a weapon of choice for Da'esh, and, in spite of existing EU legislation in this area, it is evidently still too easy for attackers to get their hands on it.

So we will be reviewing the EU legislation on explosive precursors. Ahead of that review we have set out a Recommendation with immediate steps Member States can take to prevent misuse and tighten controls.

We are clamping down on terrorist financing; we have already largely implemented our 2016 Action Plan. But we need to make it easier for law enforcement to get access to financial information held in another country; which can be a big issue in terrorism investigations. We will continue to work to ensure national authorities have the tools they need.

## Sharing best practice

Third, we can share experience and best practice. Authorities in many different countries are seeing similar trends, facing similar problems, asking similar questions. We can learn from each other's expertise and experience.

We are seeing a common and mounting threat of terrorist attacks against public spaces - the city squares, tourist sites, and sporting venues. We will provide guidance about the best way to protect those public spaces, without changing their fundamentally open character. The EU is providing 120 million euros to help put those measures into practice.

Many European countries are also asking themselves similar questions about radicalisation – what drives people, in many cases Europeans, to such poisonous ideologies and violent actions? I think many of us were taken by surprise by the number who have travelled to Iraq and Syria to fight for Da'esh; or the number of Europeans inspired to acts of murder by propaganda they have seen online.

Across Europe people are asking similar questions: how can frontline workers like teachers, social workers or prison staff spot the warning signs?  What is the role of policy makers, practitioners and researchers?  How can civil society spread an alternative message to those at risk?

Some of the solutions lie in government policies. Others in local and civil society initiatives: schools, youth clubs, social services. But there is a real question about how those different groups – policymakers and practitioners - should fit their work together.

And European networks are helping to answer them.

The High Level Expert Group on Radicalisation has just issued its interim report. The Radicalisation Awareness Network continues to provide support and guidance to teachers, probation officers and the like.

And we are working directly with internet companies to ensure terrorist propaganda never gets online, or is taken down immediately. We have been clear that there'll be legislation if there has to be, and if voluntary measures don't go far enough.

## Sharing information

Beyond sharing experience, we can also share information about specific threats and people.

In the terror attacks we have seen, sometimes suspects have travelled between Member States; sometimes they have been known to the authorities in one Member State but not others; sometimes they have even registered with different identities in different Member States.

We need to get better at closing these information gaps.

We already have measures on air passenger information PNR – which can help us detect and prevent terrorist incidents. I hope the few remaining Member States who have yet to transpose the Directive do so before the deadline in May 2018.

Existing EU tools help police, border guards and judicial authorities share this information to carry out their tasks. The evidence is that they appreciate them. The number of checks against the EU's Schengen information system rose 40% in just one year. If police in one country want to talk to Mr X, and Mr X is detected by the authorities elsewhere, he can be picked up.

We need to get better at how we use information. This is something I hear again and again. But the flip side to that: we need to make it easier for law enforcement to be able to do so. Not by gathering new piles of data, or by creating or merging databases. But by better using the information we already have available.

Currently, police or the authorities have access to an incomplete picture. The Berlin attacker was able to have separate identities in different countries. We want to remove those blind spots and close the information gap.

In the next couple of weeks we will come forward with proposals to make systems "interoperable" and work together. A European search portal will help frontline police and customs officers access different EU information systems simultaneously, getting combined results on one single screen. A shared biometric matching service for fingerprints will mean authorities can search all systems at the click of a button. And a common identity repository will store the core identity data, such as names, dates of birth and gender, underpinning all systems, to deal with those with multiple identities. By better use of the data we already have we can enhance our security, protect our borders and help national authorities do their jobs.

Next year, we will look at what other information will help law enforcement in their work such as financial information, or electronic evidence for crimes that have an online component.

**External action**

These are some of the ways in which we can add value to our security within Europe. But of course there is also an international dimension to our work.

If there's one thing these new security threats have in common, it is that they cross borders. Not only national borders; but also policy borders. They straddle and test the boundaries of our different policies: internal and external; military and civilian. Things that happen overseas often have a direct impact on Europe.

Born from a conflict in the Middle East, Da'esh invites European citizens to fight in Syria; its propaganda, often spread online, incites people to commit acts of terrorism in Europe. Conditions in North Africa and Turkey have a direct implication on migration into the EU. Cyber attacks plotted from beyond our borders impact our critical infrastructure, or our democratic institutions.

As such, our external action has a direct impact, not just on our partners and allies, but for our own citizens.

We need to maintain and strengthen our joint work on counter terrorism with Middle East, North Africa, the Western Balkans and Turkey.

Agencies traditionally associated with internal policies – Europol, or the border and coast guard – also need to cooperate more with those associated with common defence and security policy. We will soon be proposing that Europol work more closely in sharing information with agencies from a host of North African and Middle Eastern countries, to enable each party to more effectively tackle terrorism and serious crime.

We are also giving new and substantial impetus to the EU-NATO partnership, after the agreement reached last year. We are different organisations but with many of the same goals – and in large part many of the same members.

We are working together in many practical and operational ways: through joint exercises; in counter terrorism, but also in areas such as cyber and hybrid threats.

And of course we now also have greater military cooperation within the EU itself, through permanent structured cooperation and the European Defence Fund. I'm sure Mr Gahler will go into more detail on this. Pooling some capability and working together makes economic sense; but also strategic sense. That 23 Member States signed up — voluntarily — shows that they see its advantages.

## Conclusion

The security threats we face are not going to go away. Cyber threats are here to stay. While we are making welcome progress against Da'esh in the Middle East, I don't think they are going to go away either. Sadly.

I wish we could reduce these risks to zero; but zero risk rarely exists in this field.

What we can do is cut the risk, cut the threat surface, cut the means attackers have available. We do that best when we work together. Thank you.