INTERPOL

SPEECH • DISCOURS • DISCURSO • خطابات

REMARKS

by

Ronald K. Noble

Secretary General

EUROPEAN POLICE CHIEFS CONVENTION

30 June 2011

The Hague, Netherlands

Mr Chairman
Europol Director, Mr Rob Wainwright,
Chiefs of Police,
Heads of European Union bodies and agencies,
Dear Police colleagues from Europe and around the world,
Ladies and gentlemen,

Good afternoon.

It is my pleasure to be here today for this European Police Chiefs Convention.

I am particularly happy to see that Europol is now housed in state-of-the-art headquarters. In combating today's criminals and terrorists, who are extremely fast at adapting and taking advantage of new technologies, it has become more important than ever for law enforcement to be equipped with true cutting edge facilities. These facilities reflect the importance and weight of the responsibility resting on Europol's shoulders. I would like to take this occasion to commend Europol, its Director, European leaders, and especially the

Dutch authorities, for their vision and commitment to European and global security.

Before I start, I would also like to thank my friend Rob for inviting me to participate in today's panel. Cooperation between INTERPOL and Europol has truly gained new momentum over the past few years and this is in large part due to the Europol Director's vision and commitment to international police cooperation, in Europe and beyond.

Rob asked me to speak on the future of terrorism. Nearly ten years after the September 11th attacks, I think we are at a point where we need to take a step back, see what has been accomplished and what may lie ahead of us in the years to come.
I will approach the issue of the future of terrorism differently.

I would like to contribute to this discussion by addressing what I believe are the two most important areas of concern in relation to terrorism for the years to come — without focusing on ideology, types of groups or specific persons, I

will focus on the threats posed by air travel and cyberterrorism.

Air Travel

We all know that airplanes have been a weapon of choice for terrorists since as far back as the 1960s. Between 1968 and 1977, for example, an incredible average of 41 airline hijackings took place each year.

The September 11th attacks then brought in a totally new dimension to using planes for terrorist purposes — using planes, not as a means of taking hostages, but as weapons.

After 9/11, Al Qaeda attempted several times to destroy airplanes in mid-air. In 2006 when the British police uncovered and stopped a plot to detonate liquid explosives in at least ten airliners bound for Canada and the US. Then on Christmas Day 2009, when a man tried to detonate explosives sewn in his underwear just before landing in Detroit. And recently again, when Al Qaeda in the Arabic Peninsula attempted to bring down planes using parcel bombs.

The good news is that, since 9/11, all attempts by terrorists to use airplanes failed. What is worrying, however, is that in every one of these three examples terrorists have been able to identify and expose a new security gap.

What is also worrying is that, with the expected increase in air passengers worldwide from 2.4 billion in 2010 to 3 billion in 2014 and possibly to as much as 16 billion by 2050, we may very well find ourselves in a situation where our current strategy of physically screening every passenger before boarding may no longer be viable.

It is therefore crucial to put other tripwires in place to disrupt and prevent future terrorist attacks involving aircraft.

For almost 10 years INTERPOL and I have been advocating for the systematic screening of passports of international air travellers against global databases, on departure, transit and arrival.

INTERPOL maintains the only global database of stolen and lost travel documents, currently containing over 28 million documents, including more than 16 million passports. Every one of these is a potential weapon for terrorists or other criminals.

Thanks to a technological solution developed by INTERPOL and called MIND/FIND, border guards in our member countries can check travellers' documents against INTERPOL's database at the same time as they check them against their own national database.

With no additional delay and at minimal costs, this integration gives an additional layer of security by giving border guards real-time access to data shared by 158 countries. Last year there were almost 500 million consultations of this database, producing more than 40,000 hits.

As we speak, 17 of the 27 European Member States have installed INTERPOL's MIND/FIND system. With more than 68 million searches since January of this year, the United

Kingdom is the most important European user of this database, thanks to their implementation of the system at all UK border points, enabling the systematic screening of all travellers entering the United Kingdom. Since the beginning of the year, this INTERPOL system generated more than 5,000 hits in the UK alone. I let you appreciate the security benefits for British and European Union citizens.

When one considers that INTERPOL's MIND/FIND system gives border guards across Europe access to data shared by 131 non-EU countries, data that is not contained in the Schengen Information System, the fact that more than one third of EU Member States are not using it represents an incomprehensible security gap in Europe's security architecture.

At a time when increasing pressures on Europe's borders pushes some to consider re-establishing internal borders within the Schengen area, I am convinced that there is another solution. All EU countries should implement the 2005 European Union Common Position on using INTERPOL's global Stolen and Lost Travel Documents database within the

EU. This approach would much better serve the security of European citizens and would avoid controversy.

To give you just one topical example, you all know that alleged war criminal Ratko Mladic is now being detained in this very city, awaiting his trial at the International Criminal Court for the Former Yugoslavia. Let me pause to congratulate the Serbian government, Ministry of Interior, the Serbian Police and the Serbian people for their determination to bring Ratko Mladic to justice. Well, another former Yugoslavia war criminal, General Ante Gotovina, was able to escape justice for over four years before his arrest in 2005, thanks to a stolen passport he used to travel extensively throughout Europe and beyond. The stolen passport had been reported to and registered in INTERPOL's database, but none of the fifteen countries he travelled to during these four years had installed INTERPOL's system, nor screened his passport against INTERPOL's databases.

We may not clearly foresee which shape terrorism will take in five, ten or twenty years from now. But we know one thing – – terrorists will need fraudulent travel documents at one step

or another of their deadly logistics, and INTERPOL's MIND/FIND system is one important tripwire to stop them before they are ready to pull the trigger.

Cyberterrorism

What we can also be sure of, is that terrorists will be creative and continue to make use of every means at their disposal. I share the view expressed by Professor Raufer there is every chance that terrorists will make an increasing use of the internet, not just to radicalize and recruit, but to commit attacks — cyberterrorism, I am afraid, is just around the corner.

A recent study by the Center for Strategic and International Studies revealed that about 70 percent of the 200 interviewed IT security executives working in critical infrastructure-related companies said they frequently found malware designed to sabotage their systems. More than 40 percent of these executives also said they expected a major cyber attack within the next 12 months.

Cyber attacks will one day or another be used by terrorists against critical infrastructure companies in Europe and elsewhere in the world. Just imagine the dramatic consequences of a Stuxnet-like attack against electrical power generation and distribution systems, the water supply, the transportation network or the financial system.

Defending our critical infrastructures against cyber attacks is of course an immense technical challenge for law enforcement, especially at a time of financial constraints. But it is also a totally new type of challenge in the sense that today's critical infrastructure is largely private owned.

In short I believe that it is urgent that we step up international cooperation in order to be able to collectively face the cyber threat.

Thank you very much.