



Counter Terrorism Working Group Conclusions

What can be the future for terrorism?

Further fragmentation of some terrorist and extremist groups

Networks will become looser, terrorists and extremists groups will be able to setup and close more quickly. Technology and the internet, in particular, deliver the capacity for terrorism groups to build a loose network, even from a virtual community, at a very high speed.

An explanation for this could be the lack of leading ideologies in some terrorist forms.

The changing dynamics in our societies, together with technological advances, may encourage isolated, disaffected individuals to turn into violent extremists, to the extreme of becoming 'lone wolf' terrorists.

Terrorism and extremism will shift to more hybrid forms. New types of terrorism such as eco anarchism will come to the scene.

Jihadi terrorism going from a strategic threat to a more tactical threat

The decrease of Al Qaeda's central influence becomes more and more obvious.

The shape of Al Qaeda is not the main issue, the problem is the seeds that were planted a long time ago have grown within European society.

Al Qaeda's current capacity could be measured by any attack carried out. Such a show of strength might ignite passions on both sides of the divide.

The consequences of the Arab spring cannot yet be fully assessed although it presents a huge opportunity for terrorists.

The EU Member States' involvement in conflict zones will continue to impact on terrorist motivations.

Growing immigration flows will impact on terrorism and extremism

The insular nature of some immigration and the lack of integration into societies could lead to an increase in right-wing extremism in the EU. The traditional clashes between right wing and left wing might therefore increase.

Some immigrants from countries with important terrorist activities could offer a bridge between the EU and conflict zones.

Regional shifts

EU-based terrorist groups try to shelter in other countries due to successful law enforcement activities. This will lead to a displacement of terrorist activities in those Member States traditionally less impacted by terrorist activities.

The virtual world will be a tool, a target and a weapon

Society has become more and more dependent upon technology which has the potential for exploitation by terrorists. Almost total dependency on web-based technology may appear as a weakness.

The internet will not only be used as a tool for recruitment, training, planning, as well as being a potential target itself but will also be used as a weapon, for instance on critical infrastructure, and for intelligence gathering.

Terrorists will always study and invest in new technologies in any way possible to facilitate their activities, but the traditional means of attack will remain an easy, cost-effective option for the near future.

Potential economical impact on flows of commercial goods

A non-intentional impact of the cargo bombs was the banning of Yemeni imports into the USA. Similar techniques could have a devastating impact on the flows of global commercial goods.

Symbiosis between organised crime and terrorism

The border between organised crime and terrorism will become more and more blurred. Funding through organised crime activities will become common, and it is still not known whether some terrorist actors will change their motives to those of more personal interest. Organised crime groups might also use terrorist tactics.

What can we do about this?

De-radicalisation and prevention of radicalisation

As radicalisation has been rather intensively studied in past years, the key action needed is the de-radicalisation of radicalised individuals in society. This is the only future we can offer to them. Intensive investment is needed in this area.

Prevention of radicalisation also has to be enhanced.

Tactics and strategies in all dimensions of society must be emphasised. A more integrated approach is needed with all social actors involved: schools, media, police, justice, etc.

Interoperability

Criminal and intelligence databases have to be harmonised and interconnected as soon as possible. Concrete best practices and pragmatic training should then create a real European law enforcement culture.

Flexible private partnerships should also be encouraged as well as dialogue with vulnerable communities.

Police and intelligence services need to reinforce their current collaboration while keeping a high level of source protection.

The use of Interpol's Stolen and Lost Travel Document (SLTD) database must be reinforced by EU and non-EU countries.

Comprehensive strategy for security matters that encompasses all types of threats

The increasing number of strategies and action plans leads to a silo mentality. A clearly defined strategy, identifying the appropriate actors, is essential. The EU security architecture would benefit from integrated approaches to different crime areas including terrorism, border management, serious and organised crime...

Coordinated cost-efficient approach to EU internal and external policy

It is essential that the administrative boundaries that currently exist between key agencies (Europol, SITCEN, Frontex, etc) are eased to facilitate cooperation and information exchange in a more pragmatic way. Is it cost effective that sometimes two organisations analyse the same information?

External policy aspects should also be coordinated, integrating some security dimension.

Changing status of Europol

The borderless dimension of modern crime and terrorism calls for a more ambitious role for Europol. The necessity of two Member States being affected by a criminal act before Europol may legally become involved is redundant in the case of a borderless crime. Europol should be able to engage itself more easily.

In that field, executive powers for Europol may become necessary in some respects.

Obligatory reporting to Europol of all terrorist events in Member States is essential.