FRENCH-BRITISH ACTION PLAN

Paris, 13 June 2017

Terrorists, and the people they influence, are using the internet, websites, e-mail services and social networks to gather information, organise, spread propaganda and operating methods, send and receive instructions, and claim responsibility for their acts.

At a meeting in Paris on 13 June 2017, Prime Minister May and President Macron agreed to a joint UK/France initiative to ensure the internet cannot be used as a safe space for terrorists and criminals. They stressed that coordination with G7 and EU partners will be sought on these issues.

The following four points were agreed as priorities:

1/ Improve methods to remove illegal content from the internet

While efforts have been observed from companies regarding removing terrorist content, we need industry to move from their current position of reactively removing content when it is notified to them, to proactively identifying content and preventing it from being made available on their platforms in the first place.

Proposals:

We will urgently press the companies to establish the industry led forum, as agreed at the G7, to develop shared technical and policy solutions to rapidly remove terrorist content on the internet. This would complement the efforts of our respective referral units – the Europol Internet Referral Unit and the EU Internet Forum. At a minimum, the industry led forum will:

- Automate the detection and suspension or removal of content, based on both *who* posts, as well as *what* they post (e.g. companies should freeze, suspend, block or remove categories of account/user based on key identifiers);
- Support younger companies which can benefit from the expertise and experiences of more established ones;
- Support the efforts of civil society organisations to promote alternative and counter-narratives.

It may be necessary to clarify what constitutes unacceptable content online to ensure action: this process may require regulation. We will jointly develop proposals about how to do this.

In particular, we must ensure that hateful and radical content is quickly removed from the internet (derived from the EU Code of Conduct on Countering Illegal Hate Speech Online adopted on 31 May 2016, which should be strengthened), as set out by the public authorities and with sanctions for those who fail to comply. Terrorist content should be permanently removed (under the “Notice and Stay Down” principle).

France and the UK will continue to take a leading role in tackling terrorist content on the Francophone and Anglophone internet respectively.

2/ Support the efforts of civil society organisations to promote alternative and counter-narratives

This will include efforts to:

- Train and support those civil society actors that promote relevant counter narratives, including through the EU Internet Forum or the European Radicalisation Awareness Network (RAN);
- Promote their web-ranking, while targeting the right audience, and redirect positive content as appropriate;
- Better protect those civil society actors involved in developing counter narratives, including parody accounts, through, amongst other things, certification of their accounts and their inscription on a white list.

3/ Work together to ensure our countries can access data for investigative purposes

3.1 Seek to preserve the retention and access to traffic and location data

Under current terrorist threat levels, the ability to retain data useful to investigations remains essential.

3.2 Enable subscription holders to be identified in all circumstances

A single Internet Protocol (IP) address can be shared between hundreds of users accessing the internet or social platforms via their smartphones. The capability to identify specific users is important, particularly where suspects have accessed terrorist content.

Proposals:

- Share expertise and legislative experience regarding these issues, including with EUROPOL, with a view to intensifying dialogue with industry.

3.3 Allow access to encrypted content

When encryption technologies are used by criminal groups, and terrorists, it must be possible to access the content of communications and their metadata. This is not about backdoors or banning encryption, but ensuring Governments and companies develop shared solutions to this issue.

Proposals

- Share strategies on the challenge of accessing content from encrypted services, and coordinate our engagement with the major Communications Service Providers.

4/ Improve access to digital evidence across borders

We should work together to ensure that data and content of communications can be rapidly accessed for law enforcement across borders, wherever it is stored.

Proposals:

- Welcome the commitment of the US Administration and Congress to seek to pass legislation that removes blocks in US laws, and allows for Bilateral Agreements to be signed.

Way ahead:

France and the UK will:

- Ask for an **early meeting of the G7 Interior Ministers**, as required by the Taormina Statement on the Fight Against Terrorism and Violent Extremism, in order to widen support for this action plan;

- Press technology companies to meet our ambitions for the **industry-led forum for combatting terrorism** and to present concrete measures on the occasion of the G7 Interior Ministers meeting;

- Recognising that action may not be taken by the companies through voluntary cooperation alone, to jointly consider how to create **possible liability for companies** (for example through regulation or legislation);

- Lead a group of concerned countries to follow up on the **implementation of the G7 initiatives** and develop new measures when needed;

- Welcome the commitment of the US Administration and Congress to seek to **pass legislation that removes blocks in US laws**, and allows for Bilateral Agreements to be signed;

- Encourage an **acceleration of EU work** on: the implementation of the European code of conduct; the review of the Audiovisual Media Services (AMS) Directive; encryption; e-

evidence; the review of the E-Commerce Directive; and support the strengthening of Europol's work, in particular its Internet Referral Unit; and

- **Share strategies on the challenge of accessing content from encrypted services**, and coordinate engagement with the major Communications Service Providers.