Speech: Baroness Shields opening speech at the Global Counter Terrorism Forum

I would like to thank our Swiss counterparts who co-lead this crucial work alongside the UK and the UAE as co-chairs of the GCTF, who believe as we do that this forum has the potential to pave the way for a significant step change in how we as nations, working in partnership, can challenge this evolving global threat.

The next 3 days provide us with an opportunity to improve our understanding of the complex challenges we face. And to drive forward a collective agenda to develop communications and co-governance approaches that tackle the exploitation and manipulation of the open internet by terrorists and violent extremists.

Sadly, we begin 2017 in the same way we began 2016, in the shadow of multiple deadly terrorist incidents. There were literally dozens of attacks inspired or promoted by Daesh throughout the world in 2016.

Over the past year, we have seen new developments of terrorists using social media during attacks to document their actions as they unfolded. Footage that has later been used in instructional videos released officially by Daesh to inspire and incite more violence.

We have seen perpetrators repeatedly updating their social media during attacks and others live broadcasting their actions before, during and after committing these unspeakable acts of violence.

The hatred of terrorists and violent extremists across the world does not differentiate between the market places of Baghdad and Berlin. Yesterday's deadly vehicle attack in Jerusalem, follows the now tragically familiar pattern we saw in Nice on Bastille Day, at Ohio State in November and in Berlin's Christmas market in December.

It is clear that the internet and social media platforms have become much more than simply a method to distribute information or to claim responsibility for attacks.

Whether directed, inspired or promoted by Daesh, these attacks, the sources and methods they use are coming part of the modus operandi for terrorists and extremists worldwide; weaponising the platforms and applications we all use in our everyday lives.

And whilst the physical presence of Daesh in Iraq and Syria is diminishing, the ability of Daesh and other extremist groups to inspire and incite followers to commit acts of terror has not.

Consequently, collectively addressing the 'strategic communications and

social media dimension to preventing and countering violent extremism' remains an urgent and unrelenting challenge.

This Global Counter Terrorism Forum can enable a much needed change in how we combat terrorist use of the internet and how we develop the communications initiatives and internet governance that will deliver results.

But to be successful, we need to be coordinated.

We need new and innovative methods to more quickly identify and remove terrorist and violent extremist content and to deliver more effective strategic communications to counter these deadly narratives in all our countries.

Today we have the right people in the room to bring about this change. We can, and we must, act.

To focus our thinking, let me address a few key points:

- first, the specific nature of the global threat we face and how it is evolving and changing
- second, our collective response and our progress to date
- and third, what further preventative action needs to be taken

The threat

In terms of the threat, before we shape any response we must be sure we understand the threat we face.

I am sure we are all familiar now with the fact that social media platforms, and applications provide the opportunity to radicalise a global audience. An audience who would otherwise never have been reachable.

These platforms also provide the ability to normalise behaviours and attitudes that would be considered unacceptable or inappropriate offline.

These same platforms algorithmically connect like-minded individuals creating an illusion of strength in numbers.

Research by Paul Gill et al (2015) shows that 54% of convicted UK terrorists have used the internet to learn about some aspect of their intended terrorist activity.

This proportion increases to 74% when looking at terrorist actors since 2012. In 61% of cases, there is evidence that individuals had engaged in online activity that was directly related to their ultimate attacks or conviction.

But the threat we face continues to evolve and diversify, and significantly

so over the past twelve months.

Let’s be clear, physically Daesh is collapsing in Iraq and Syria.

But as military success draws down, their attention is focused on inspiring and inciting violence through online propaganda.

A powerful new brand is emerging, aiming for relevance in the global virtual space.

This brand is based on the appeal of a virtual borderless presence repeatedly calling on followers to carry out acts of terrorism across the world.

Following the claim by Daesh of responsibility for the atrocious attack on Berlin’s Christmas market, Daesh released a statement on Telegram in Arabic, French and English encouraging their supporters to carry out lone actor attacks in the West and Europe during the Christmas and New Year period, specifically advising supporters to target ‘celebrations, clubs, hospitals, markets and movie theatres’. Tragically, foretelling the Reina nightclub attack in Istanbul on New Year’s Eve. In the same message they encouraged further attacks on consulates and embassies.

We have seen this message before. Earlier this year Daesh published an audio message from its then spokesman, Abu Muhammad al-Adnani, in which he renewed calls for the group’s supporters to carry out terrorist attacks during Ramadan. At the time, the speech did not precipitate international media scrutiny and even some terrorism analysts regarded it as less persuasive than his previous fatwas.

However, Adnani’s words were linked to more than 400 deaths across the globe during the Islamic holy month.

It was the bloodiest Ramadan this century with attacks in Paris, Orlando, Baghdad, Medina and Dhaka.

This ability to inspire and incite attacks globally, exemplifies the new direction and shift in Daesh’s own brand communications. As the following slides demonstrate

The one on the left is an original version of its Dabiq magazine encouraging its supporters to embrace the new caliphate and build a new state, the second its new magazine Rumiya calls on its followers to carry out acts of terrorism wherever they live and wherever they can.

The second edition of Rumiya reinforced support for lone actor attacks using knives with a full demonstration on a frightened hostage. This modus operandi was used in the heinous murder of the French priest in Normandy and attacks in the Minnesota shopping mall last year.

Daesh’s third edition of Rumiya magazine, again released via Twitter and Telegram, specifically advised it supporters to carry out vehicle-based lone actor attacks targeting high profile events.

It praised the Bastille Day Nice attack and proposed that supporters mimic it with the use of large and heavy vehicles, all too familiar to us now.

Daesh continues to make prolific use of video and film to spread their propaganda online.

As I mentioned, in a recent video, a bound hostage is stabbed to death on camera to demonstrate to viewers the most efficient technique for murdering a civilian with a knife.

This was followed by a scene showing how to build a shrapnel-filled IED in a kitchen. More than 100 links to this video were posted to twenty-nine platforms. Dissemination was organised on Telegram, distributed on Twitter and the video was hosted on YouTube, Archive, Send Vid and Google Drive.

Twenty-four hours after the video's release, despite best efforts, half of these links were still active.

So, to be clear. Since 2013, Daesh's approach to online communications has been characterised by constant innovation in attempt to ensure its propaganda reaches the vulnerable people it is designed to influence.

As early as 2014, before the majority of the public were aware of the group's threat, Daesh were using bots to game Twitter and amplify their messaging.

Today this is complemented by the use of Telegram to coordinate thousands of messages promoting the latest Daesh film within hours of release.

Last year, we saw Daesh use drones to film propaganda, propaganda apps for children, and even attempt to develop their own social network.

And, as the heinous killing of the policeman in Paris has shown us, attackers have already begun to make use of live video streaming technology to promote attacks as they take place.

It is highly likely that the group will continue to expand into new technologies in the year to come, as it attempts to remain relevant whilst its physical presence collapses.

And, in addition to a shift in Daesh's own brand communications, with devastating consequences, we see a resurgent Al Qaida. Only last week, its leader issued a statement on Telegram and Twitter calling for attacks on the US as a 'top priority'.

And worldwide, extreme right wing groups are developing their own social media communications capabilities representing a new threat with an alarming rise in incidents of extreme, right-wing motivated violence.

So let's be clear about the threat today as we begin 2017.

We face an increasingly potent 'cycle of hate' across multiple extreme groups and ideologies with dynamic shifts in terrorist communications tactics.

Our response

And so to my second point, as the threat we face on these multiple vectors is delivering influence at a sustained pace and scale, then we must develop and rapidly deliver an ever stronger response at a greater pace and scale.

Research conducted by the UK government shows that the majority of links to Daesh content are shared within 2 hours of first release.

We know this is not a single platform issue.

We know that terrorists use different platforms for different purposes – to first distribute their propaganda as far and wide as possible, then to lure individuals into direct conversations.

And over the last 2 years we have all become acutely aware that no one country, company, organisation or individual can defeat this highly complex and evolving threat alone.

It must be a collective effort.

A new partnership is required where all parties – governments, civil society, industry, the media – work together to tackle terrorist and violent extremist use of the internet.

These durable partnerships, as represented by the GCTF, must generate a whole new scale of effective response.

So in addressing this 'cycle of hate' we must build new capacity – both national and international – that is holistic, targeted and dynamic.

The progress

Some progress has already been made.

Last year Australia set up a national capacity to remove terrorist and extremist propaganda and amplify counter narratives.

The Global Coalition Strategic Communications Cell have provided a core co-ordination function which has distributed counter narratives and campaign ideas to coalition members on a weekly basis.

Last year, Microsoft, Google, Facebook and Twitter signed the EU Commission's Code of Conduct, agreeing to take the lead in countering the spread of illegal hate speech online.

Facebook launched the online civil courage initiative in Germany and Google developed and initiated the 'redirect method' to deliver a curated counter narrative content response to search queries. YouTube has expanded its 'trusted flagger' scheme so problematic videos can be taken down quickly.

And Microsoft have strengthened their terms and conditions with zero tolerance language prohibiting violent extremist propaganda and hate speech

and are developing new technologies to scan for terrorist and extremist images.

And Twitter has updated its terms and conditions to prohibit promoting violence against others and shut down 360,000 accounts for threatening or promoting terrorist acts.

At the EU Internet Forum in December, we saw the announcement of a proposal by industry to build a shared hash database.

This is a welcome and encouraging first step and we need industry to move quickly to implement this shared platform to improve our ability to clear caches of known terrorist content from the internet and to keep that content from being reposted.

But more still needs to be done.

We must understand the influence of terror groups online and deploy the use of strong data analytics to understand how terrorists amplify their messages across all social media platforms and communication apps.

To curtain this viral influence, we need to understand how these messages are amplified and how their deadly influence is generated.

We should all play close attention to work of the GCTF on developing 2 work streams of co-governance and communications to challenge terrorist and violent extremist content online – not just on social media platforms, but also on the traditional news media platforms online.

The recommendation documents, which will be produced by the GCTF laying out the principles of engagement for governments to counter violent extremism and provide GCTF members with an invaluable toolkit, will be a potentially invaluable in our arsenal to respond effectively to terrorist use of the internet and the developing capabilities of more and more extremist groups.

This work will help to develop national capacity to deal with this issue.

In the UK, our response for tackling terrorist and violent extremist use of the internet focuses on two areas of work.

One, working with industry to voluntarily remove terrorist and violent extremist content online through the Counter Terrorism Internet Referral Unit, and 2, bringing communication experts and civil society groups together to develop and run targeted and more effective counter campaigns.

But while this is world leading in terms of volume of referrals and speed of takedowns, this is not enough. We need the whole of industry to come together to innovate and automate these processes to tackle terrorist and extremist content online.

Since February 2010, when the CTIRU was first set up, it has secured the removal of over 250,000 pieces of propaganda. Based on this model, the EU Internet Referral Unit, was launched to secure the removal of content in a

wider range of languages. To date the unit has secured the removal of over 16,000 pieces of online propaganda.

Conclusion

So, in conclusion. The Global Counter Terrorism Forum can and should pave the way for a step change in how we respond as national governments, industry and as global partners.

We all have a shared interest in ensuring that the internet continues to be a safe, free and open space.

If we can come together and herald an era of shared responsibility we will defeat those that seek to divide us.

Thank you very much.