Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes

Strengthening Dialogue and Building Trust

February 2017

Presentation by Adam Hadley
adamhadley@ict4peace.org

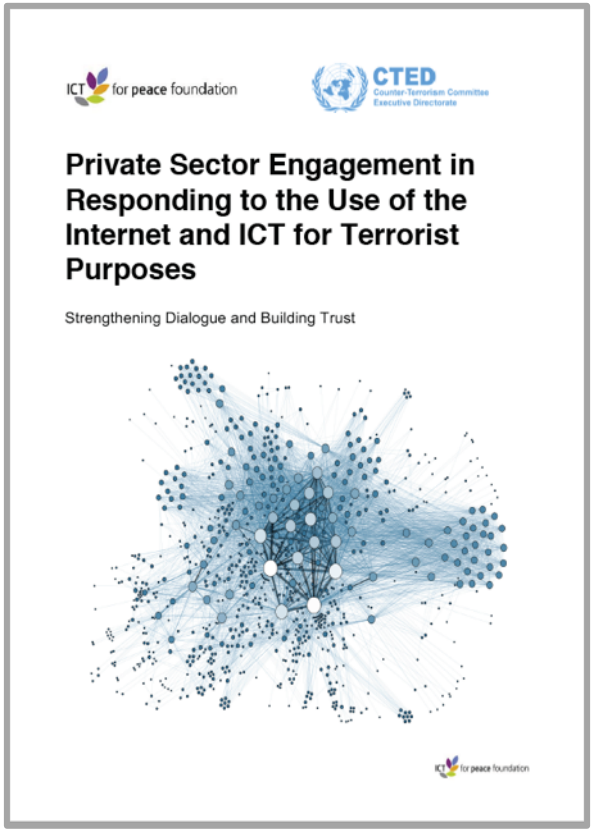
Objectives of the joint ICT4Peace and UN CTED project in 2016

- **Phase 1: April – December 2016**
  - The purpose of Phase 1 was to deepen the knowledge base:
    1. *Identify and analyse existing and emerging threats*
    2. *Understand industry approaches and the principles and norms*
    3. *Understand trends in multi-stakeholder and public-private engagement*
    4. *Scope appropriate mechanisms / platforms for knowledge sharing*

  How? Consultations via three workshops in **Zurich**, **Kuala Lumpur**, and **Silicon Valley** with major stakeholders from the ICT industry, civil society, and inter-governmental agencies + interviews + desk research.

  - We reported our initial findings to a Special Meeting of the UN CTC in Dec 2016 and there will be further follow-up with the CTC in Feb. 2017

We presented our summary report for Phase 1 at the UN in December



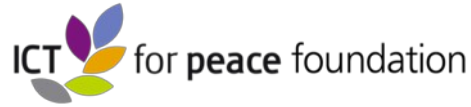
http://bit.ly/2kMBDZJ

Google: UN private sector engagement ICT For Peace

ICT for peace foundation

UN CTED
Counter-Terrorism Committee
Executive Directorate

Our advisory group: Leading technology companies and a range of academic, civil society groups, and inter-governmental organisations



ICT4Peace Global workshops held in 2016: Industry representatives from technology, media, telecommunications, finance, and advisory

ICT4Peace Global workshops held in 2016:
Governments and inter-governmental organisations were key stakeholders in the consultation

ICT4Peace Global workshops held in 2016: Leading civil society organisations and human rights groups were prominent

ICT4Peace Global workshops held in 2016: Academic institutions and think tanks contributed papers for each of the global meetings

ICT for peace foundation

UN CTED
Counter-Terrorism Committee
Executive Directorate

Context: Social media and internet technologies are used by almost half the world's population with adoption rising quickly

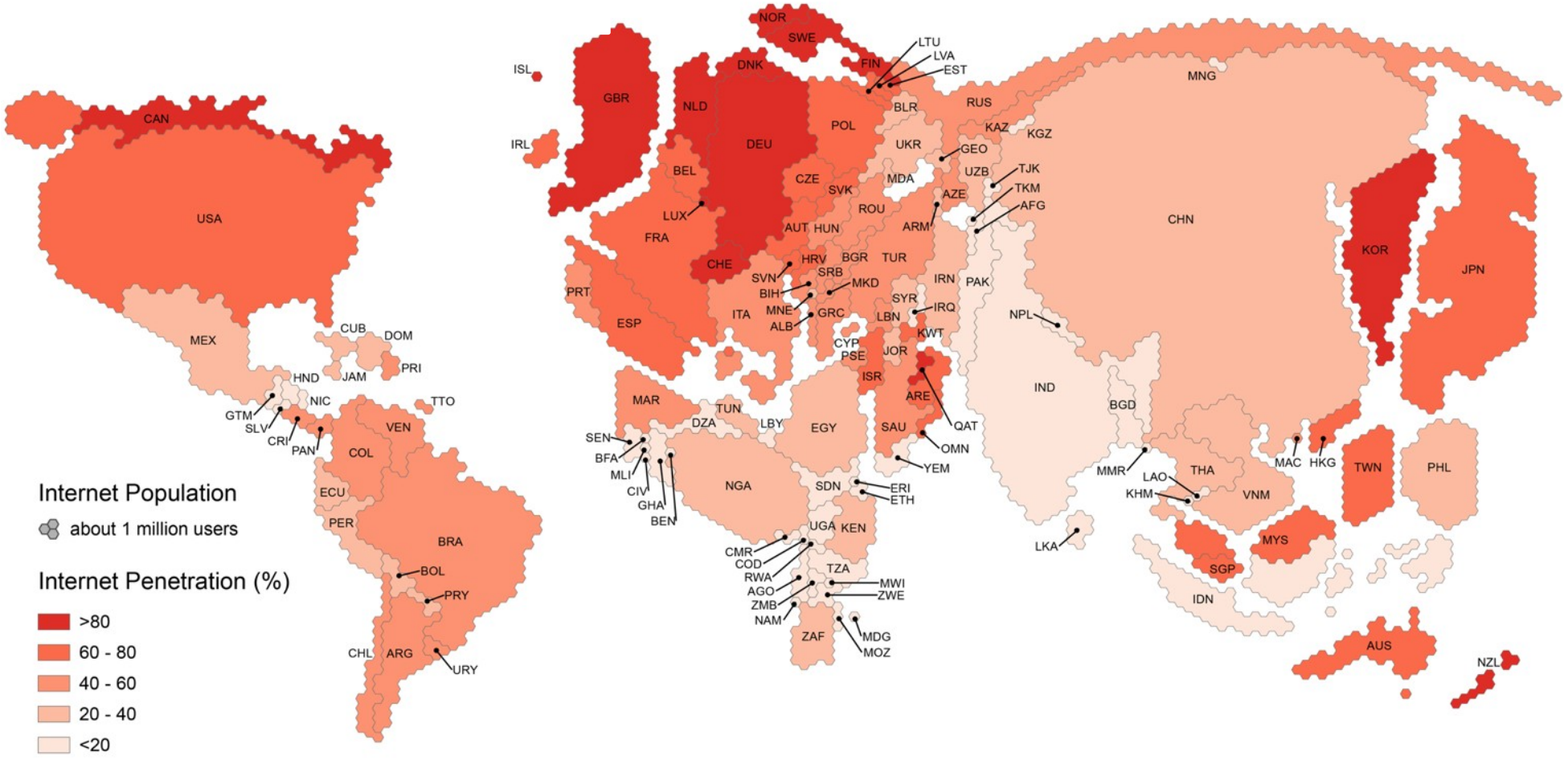
- Worldwide population: 7.5 billion
- The internet has 3.17 billion users = nearly 50% of the population
- 2.3m Google searches per minute - 6000 Tweets per second; 17 trillion webpages indexed by Google as of Jan 2016
- 2.3 billion active social media users (1.5bn on Facebook)
- Internet users have an average of 6 social media accounts
- Social media users have risen by 200 million in the last year
- There are 1.65 billion active mobile social accounts globally with 1m more every day

ICT for peace foundation

UN CTED Counter-Terrorism Committee Executive Directorate

Source: Google, Mashable, Brandwatch

Context: Within the next decade, communications technologies powered by the internet will become more influential in Central Asia



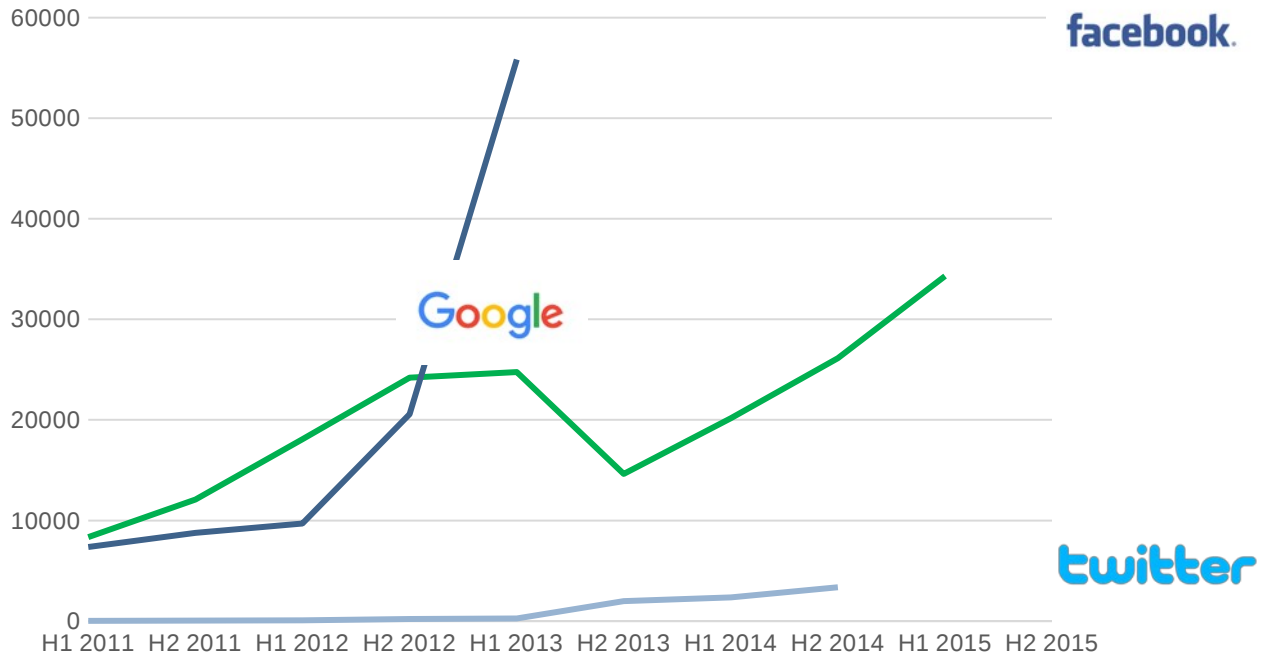
ICT for peace foundation

UN CTED Counter-Terrorism Committee Executive Directorate

Source: Oxford Internet Institute, World Bank, IMF

Industry response: In 2015 the top tech companies took down over 160,000 items of concern for governments

Content takedowns requested by governments (2011-2015)

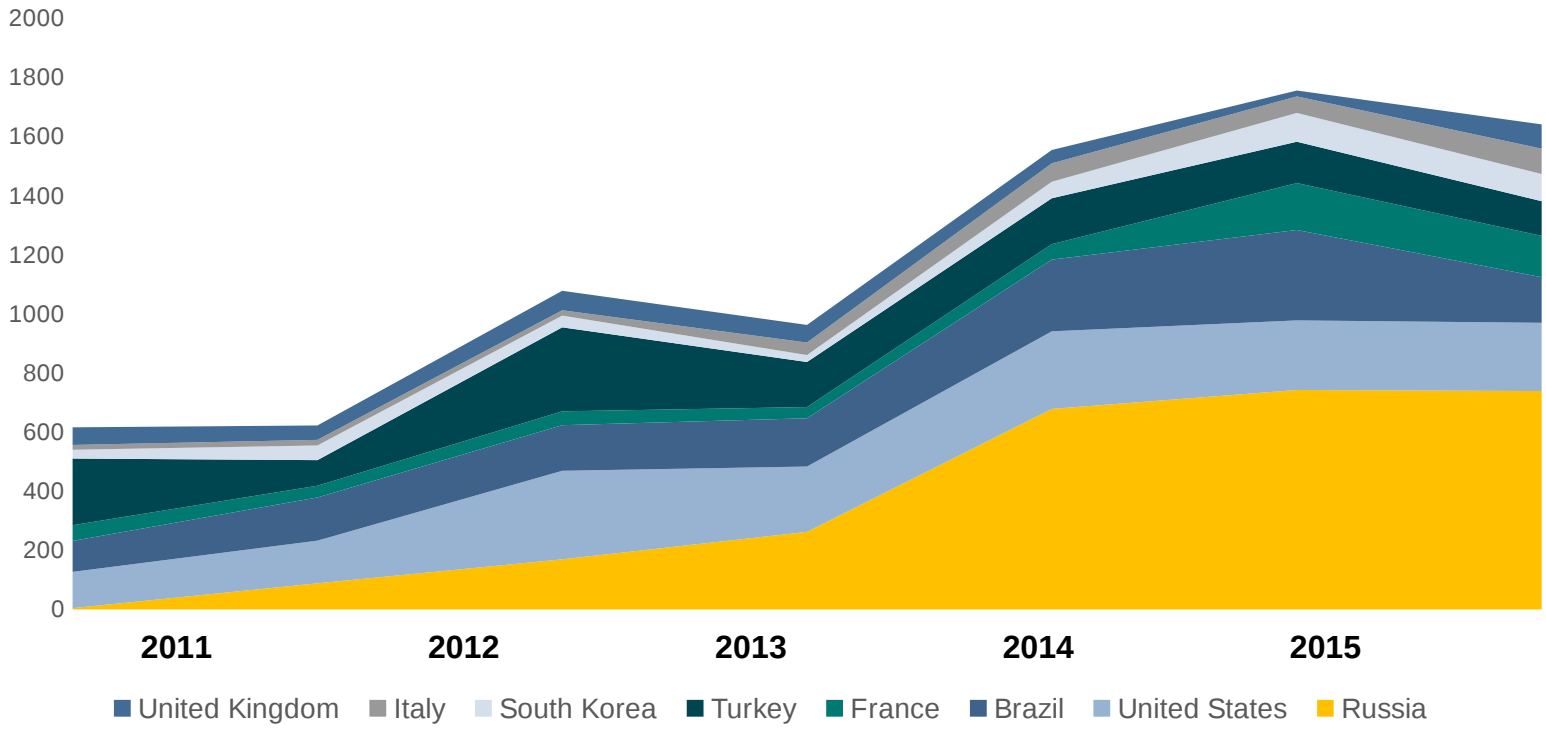


ICT for peace foundation

UN CTED Counter-Terrorism Committee Executive Directorate

In 2015 Google agreed to over 600 take-down requests from the Russian government and is working harder to support governments

Partially or completed complied requests for Google content by country by year



ICT for peace foundation

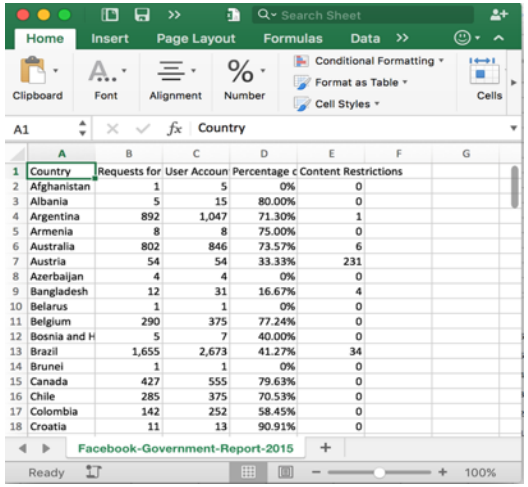
UN CTED Counter-Terrorism Committee Executive Directorate

Based on the principle of openness, major technology companies now regularly produce Transparency Reports

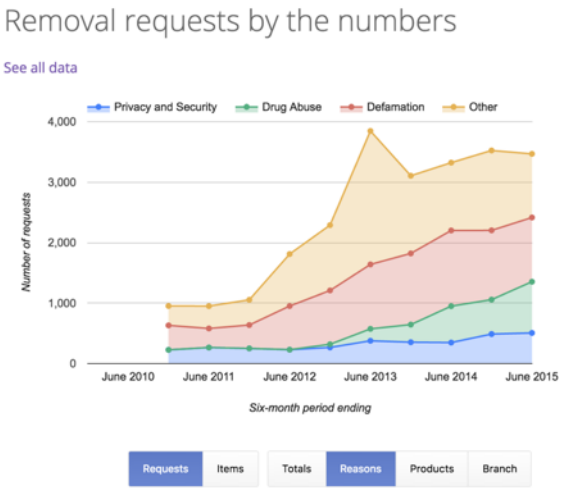
facebook

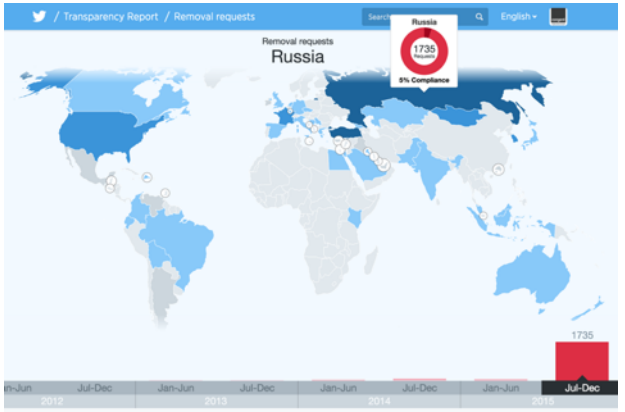
Google

twitter



	A	B	C	D	E
1	Country	Requests for	User Accoun	Percentage c	Content Restrictions
2	Afghanistan	1	5	0%	0
3	Albania	5	15	80.00%	0
4	Argentina	892	1,047	71.30%	1
5	Armenia	8	8	75.00%	0
6	Australia	802	846	73.57%	6
7	Austria	54	54	33.33%	231
8	Azerbaijan	4	4	0%	0
9	Bangladesh	12	31	16.67%	4
10	Belarus	1	1	0%	0
11	Belgium	290	375	77.24%	0
12	Bosnia and H	5	7	40.00%	0
13	Brazil	1,655	2,673	41.27%	34
14	Brunei	1	1	0%	0
15	Canada	427	555	79.63%	0
16	Chile	285	375	70.53%	0
17	Colombia	142	252	58.45%	0
18	Croatia	11	13	90.91%	0





ICT for peace foundation

UN CTED
Counter-Terrorism Committee
Executive Directorate

Industry responses: The industry is already developing an emerging voluntary policy framework e.g. around Terms of Service

Defining terrorism using sanctions lists

- Challenges in defining **terrorism -** some companies use international, regional or national **sanctions lists**
- Microsoft has announced it is using the **consolidated UN sanctions list** to inform its decisions

"Terms of Service" and emerging policy

- Some companies are adapting "Terms of Service" and using community guidelines to **prohibit certain content**
- Companies have a **zero- tolerance policy** for terrorist content their platforms and committed to ensuring safety

Global Network Initiative (GNI) and other industry initiatives

- Many companies participate in the **Global Network Initiative** or other industry initiatives which set guiding principles for industry action on a number of issues
- These initiatives are generally linked to the UN Business and Human Rights principles

ICT for peace foundation

UN CTED Counter-Terrorism Committee Executive Directorate

Industry responses: Other than developing policy, industry is taking proactive steps to counter the terrorist use of their platforms

Developing guidance systems	•Developing **guidance and systems** for content flagging, referral and content/ account removal and for remedial action – **artificial intelligence**
Building policy and legal teams	•Employ **specialist legal teams** •**Content policy teams** now play critical roles
Co-operation with Internet Referral Units (IRUs)	•Cooperating with **government** or **regional internet referral units** (IRUs), e.g. UK CTIRU, Netherlands, EU IRU based in the Hague
Investment in counter-narrative	•Developing tools and mechanisms to **counter the narratives of terrorist** and **violent extremist groups** •Carried out **with government agencies** and/ **or civil society** and **community organizations**

ICT for peace foundation

UN CTED Counter-Terrorism Committee Executive Directorate

Industry responses: Other concerns raised in our consultations

Legitimacy of the private sector in terms of shaping norms of behaviour

Small companies have **limited capacity**, resources, knowledge of the issues

Disconnect between ONLINE and OFFLINE PVE efforts

Limited evidential basis for responses / what does or does not work

Limited investment in long-term **education** and critical thinking

Respecting human rights

Recommendations from our report: Our focus for 2017-2018

1. Build on existing policy initiatives and avoid duplication of effort
2. **Strengthen dialogue on the emerging normative framework through multi-stakeholder engagement (policy & tech liaison)**
3. Promote coordination between inter-governmental initiatives
4. **Establish a Global Knowledge Sharing/ Capacity Building Platform focused on Policy & Practice**
5. Build capacity and raise awareness (companies, gov. agencies, civil society etc.)
6. Strengthen the Links Between Offline Prevention Efforts and Online Content Management and Counter-Narrative Efforts
7. Support data-driven research on effectiveness
8. Promote Critical Thinking and Media/ Digital Literacy

Implementing the recommendations: Initiatives the joint UNCTED/ICT4Peace will focus on in 2017-2018

1 UN CTED / ICT4P Multi-Stakeholder Series

Strengthening Dialogue and Building Trust

Objectives:

1. Support continued dialogue around emerging policy, principles and norms
2. Share experiences, lessons, policy and practice on public-private partnerships
3. Focus on capacity building for start ups
4. Supporting States to understand how to engage better with private companies

2 Global Knowledge Sharing Platform

- Target audiences (industry actors; government agencies; civil society groups)
- What will be shared on the “one stop shop” platform:
  - norms, standards, principles
  - sample Terms of Service, sample government legislation
  - examples of public-private/ multi-stakeholder initiatives
  - policy-relevant research on changing nature of the threat
  - tool-kits for capacity building

ICT for peace foundation

UN CTED Counter-Terrorism Committee Executive Directorate

Conclusions

- The private sector is developing sophisticated capability to counter the use of technology by terrorists including through taking down large amounts of terrorist content
- There is risk a of over-regulation by governments –measures by governments should be proportionate to the size of the danger and not over-react to the problem
- The private sector is already supporting the emergence of a voluntary framework e.g. self-regulation
- Public-private partnerships are successful – more support is required to build capacity in States and smaller technology companies