UN CTED
Counter-Terrorism Committee
Executive Directorate

ICT for peace foundation

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

Strengthening Dialogue and Building Trust

April 2017

Presentation by Adam Hadley
adamhadley@ict4peace.org

Objectives of the joint ICT4Peace and UN CTED project in 2016

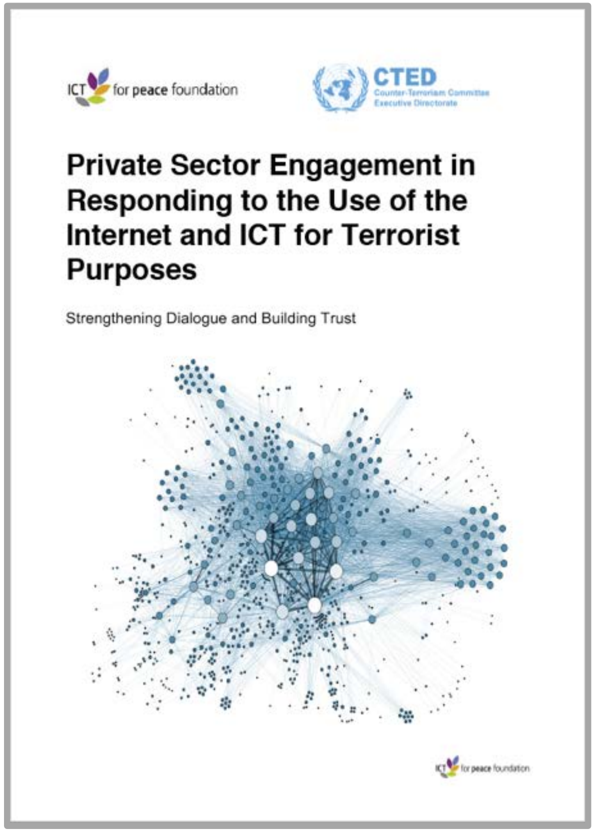
- **Phase 1: April – December 2016**

- 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 was a further follow-up with the CTC in Feb. 2017

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



ICT for peace foundation

CTED Counter-Terrorism Committee Executive Directorate

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

Strengthening Dialogue and Building Trust

ICT for peace foundation

techagainst**terrorism**.org

Google: UN private sector engagement ICT For Peace

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

UN CTED Counter-Terrorism Committee Executive Directorate

HOME

Microsoft

facebook

Google

EUROPOL

SecDev

KASPERSKY lab

ICT for peace foundation

ASKfm

Global Network Initiative

Institute of Strategic & International Studies (ISIS) Malaysia

OXFORD MARTIN SCHOOL

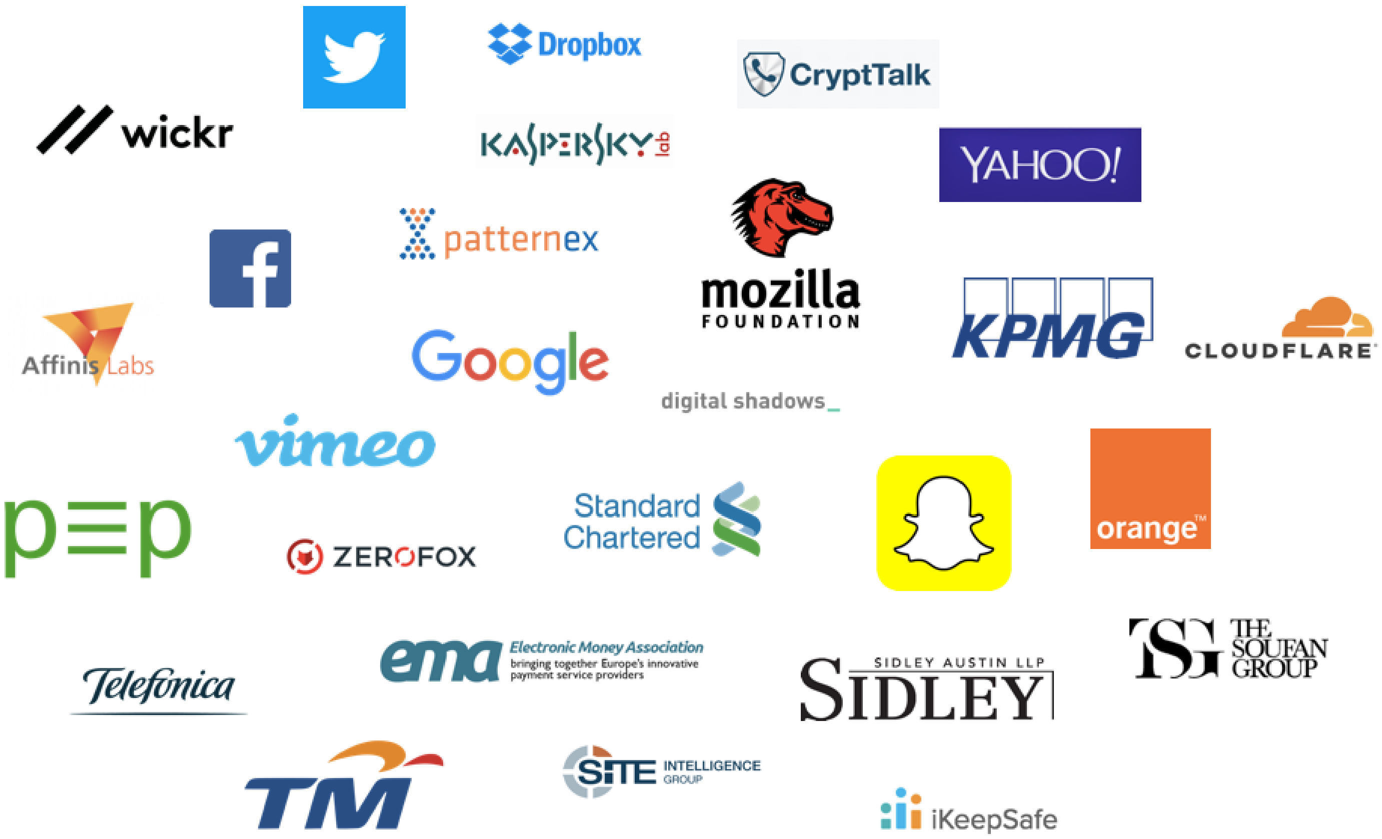
UNIVERSITY OF OXFORD

JustPaste.it

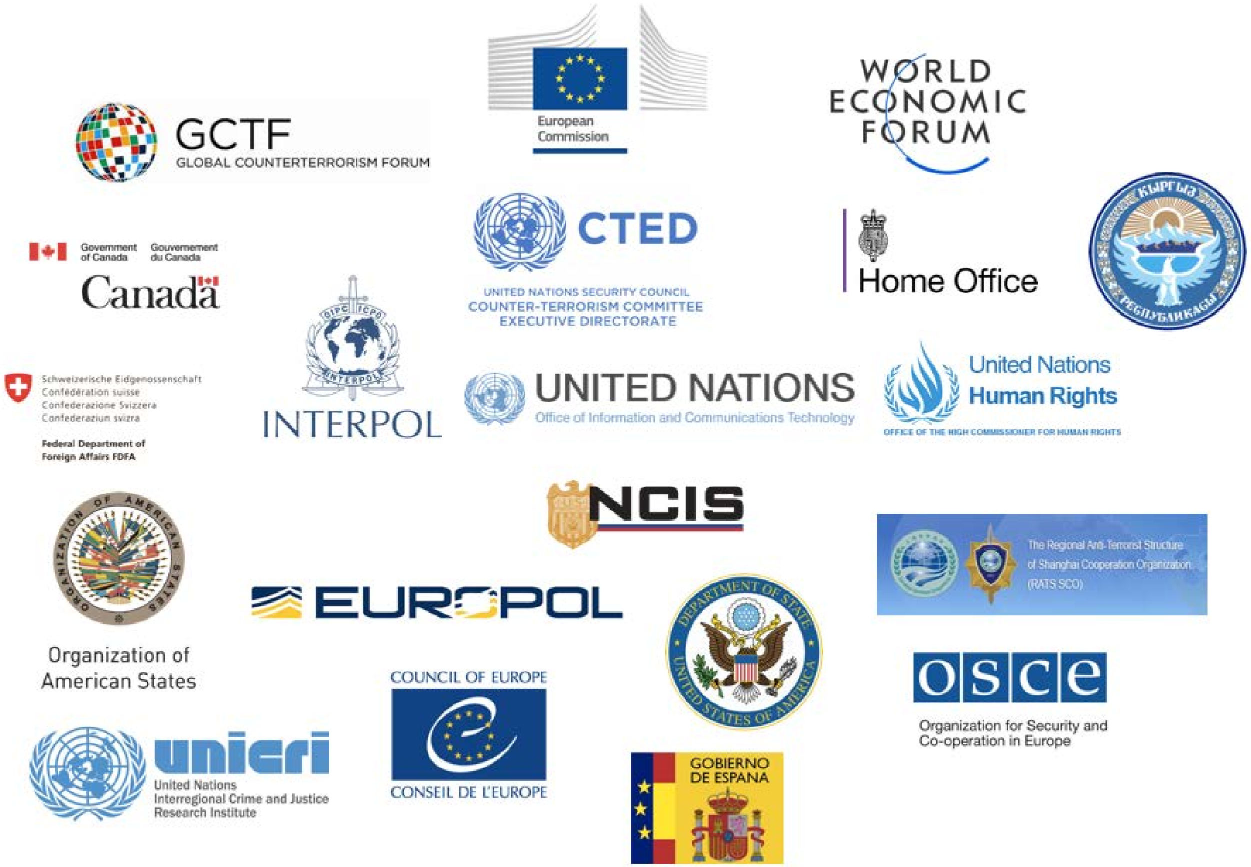
Telefonica

VOX Pol

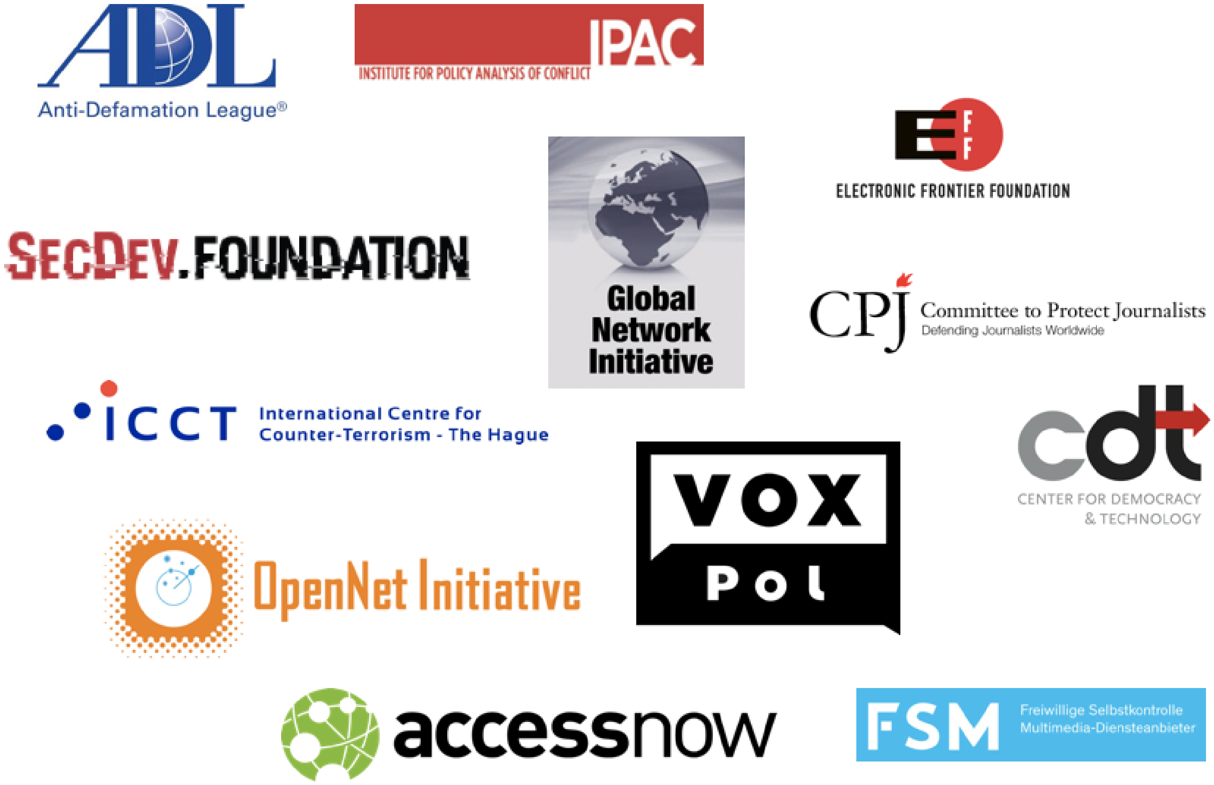
ICT4Peace Global workshops: Industry representatives from technology, media, telecommunications, finance, and advisory



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


GCTF
GLOBAL COUNTERTERRORISM FORUM
European Commission
WORLD ECONOMIC FORUM
Government of Canada Gouvernement du Canada
Canadä
CTED
UNITED NATIONS SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE
Home Office
КЫРГЫЗ РЕСПУБЛИКАСЫ
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Federal Department of Foreign Affairs FDFA
INTERPOL
UNITED NATIONS
Office of Information and Communications Technology
United Nations Human Rights
OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS
NCIS
The Regional Anti-Terrorist Structure of Shanghai Cooperation Organization (RATS SCO)
Organization of American States
EUROPOL
DEPARTMENT OF STATE UNITED STATES OF AMERICA
osce
Organization for Security and Co-operation in Europe
unicri
United Nations Interregional Crime and Justice Research Institute
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
GOBIERNO DE ESPANA

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


ADL
Anti-Defamation League®
IPAC
INSTITUTE FOR POLICY ANALYSIS OF CONFLICT
EFF
ELECTRONIC FRONTIER FOUNDATION
SECDEV.FOUNDATION
Global Network Initiative
CPJ Committee to Protect Journalists
Defending Journalists Worldwide
ICCT International Centre for Counter-Terrorism - The Hague
cdt
CENTER FOR DEMOCRACY & TECHNOLOGY
VOX Pol
OpenNet Initiative
accessnow
FSM Freiwillige Selbstkontrolle Multimedia-Diensteanbieter

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

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

NANYANG TECHNOLOGICAL UNIVERSITY

DCU

ISIS MALAYSIA

SCHOOL OF LAW
UNIVERSITY of CALIFORNIA · IRVINE

BRENNAN CENTER FOR JUSTICE
at New York University School of Law

KING'S College LONDON

ETH Zürich

॥न्यायस्तत्र प्रमाण स्यात्॥
NLU
DELHI

OXFORD MARTIN SCHOOL

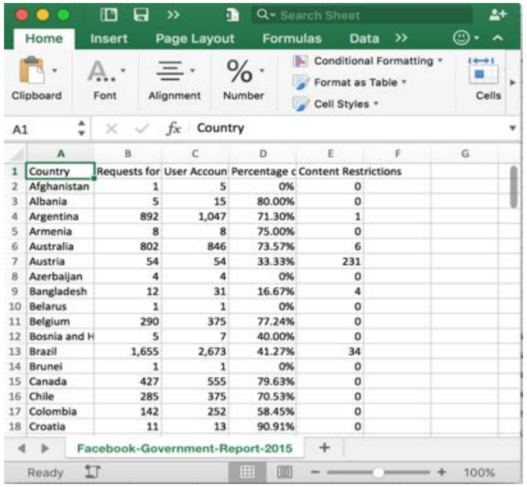
UNIVERSITY OF OXFORD

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

facebook

Google

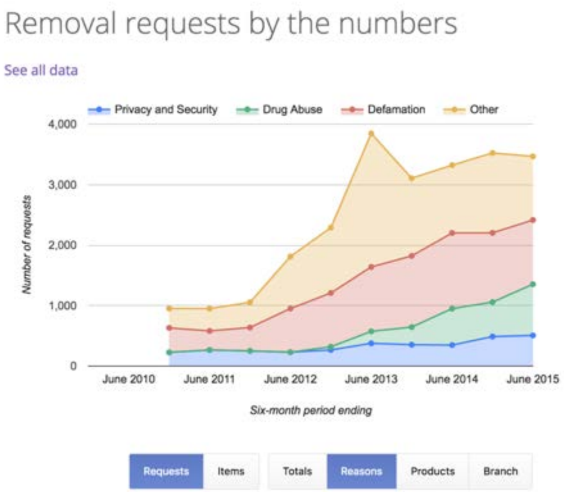
twitter



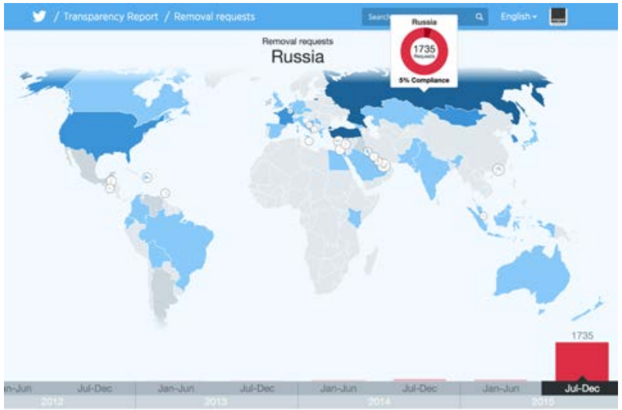
A1 | *fx* Country

	A	B	C	D	E	F	G
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		

Facebook-Government-Report-2015


Removal requests by the numbers

See all data



ICT for peace foundation

UN CTED
Counter-Terrorism Committee Executive Directorate

Industry responses: Other concerns raised in our consultations

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

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

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

Conclusions from Phase I of the project

- The private sector is developing sophisticated capability to counter the use of technology by terrorists including through take downs
- In some regions there is risk a of over-regulation by States – 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 for smaller technology companies and some States

Phase I Recommendations: In Phase II we will focus on the two major recommendations from the initial phase of the project

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 and raise awareness**
5. Build capacity between 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

There are two workstreams in Phase II: (1) Multi-stakeholder engagement and (2) Building the Knowledge Sharing Platform

1 Multi-Stakeholder Knowledge Networks

Strengthening Dialogue and Building Trust through establishing topic-specific Knowledge Networks and related workshops / consultations

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 practical capacity building in 5 areas:** the Knowledge Networks are: Startups, Finance, Legal, Social Impact & CVE, States that need Capacity Building

2 Knowledge Sharing Platform (KSP)

Objectives:

1. **Leverage Knowledge Networks** to inform practical capacity-building requirements
2. **Create a resource to consolidate findings** and recommendations from Workstream 1 Knowledge Networks
3. **Build a tool to help stakeholders** build capacity and improve their ability to counter the use of technology by terrorists

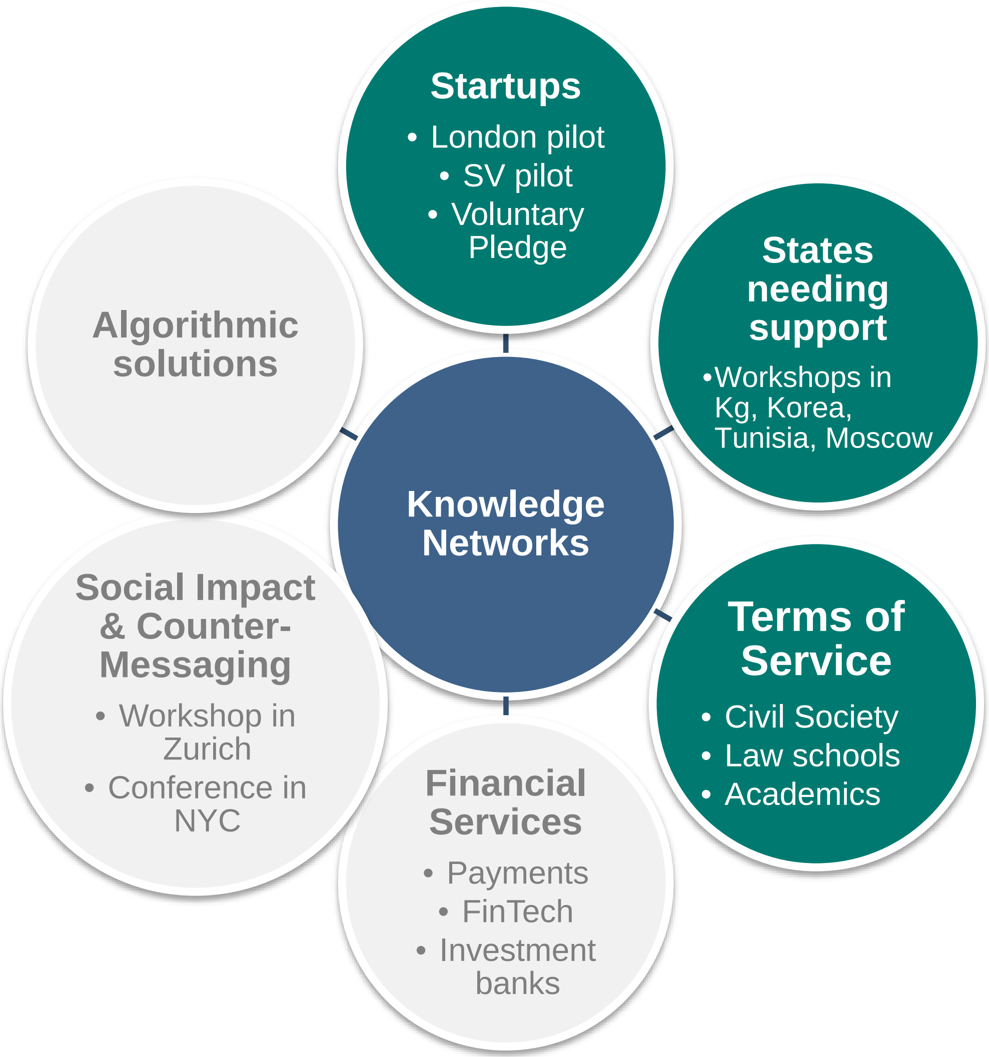
- **The KSP will have thematic focus** based on the Knowledge Networks and stakeholders
- **Content / functionality for the KSP:**
  - Norms, standards, principles (Sample Terms of Service, sample government legislation)
  - Examples of similar initiatives & research

tech
against
terrorism

techagainst**terrorism**.org

In Phase II we will focus on the Startup, State, and ToS workstreams however we will also support additional activities

Main focus for Phase II



Startups
- London pilot
- SV pilot
- Voluntary Pledge

States needing support
- Workshops in Kg, Korea, Tunisia, Moscow

Terms of Service
- Civil Society
- Law schools
- Academics

Financial Services
- Payments
- FinTech
- Investment banks

Social Impact & Counter-Messaging
- Workshop in Zurich
- Conference in NYC

Algorithmic solutions

Knowledge Networks

ICT for peace foundation

UN CTED
Counter-Terrorism Committee Executive Directorate

Thank You !

Please email:
Adam Hadley ICT4Peace
adamhadley@ict4peace.org