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

Strengthening Dialogue and Building Trust

31 Jan, 2017

Presentation by Adam Hadley
adamhadley@ict4peace.org
Objectives of the joint ICT4Peace and UN CTED project (Phase 1)

• 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
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 intergovernmental 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
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
Findings of our consultations: The nature of the threat

Current threat assessment

- Current threat remains anchored in **communications and propaganda**, **radicalisation** and **recruitment of potential fighters** and followers, **transferring and raising funds** and transferring or **sharing knowledge** - helpful to distinguish between **content** and **operations**
- Internet is dual-use technology as is encryption and related technologies
- Use of internet by terrorists will remain until OFFLINE drivers resolved

Emerging or potential threats

- Need to stay on top of the threat – shifting as we speak.
- Limited evidence that terrorist groups have the capabilities to conduct cyber-enable attacks against critical infrastructures – however potential to develop or procure the capabilities and cause significant harm.

Responses

- “Urgent action” increasingly called for by governments (e.g. regarding content restrictions (blocking, filtering, removal requests))
- Increased focus on tech “intermediaries” (ISPs) by governments
- Volume of data leads to over-reliance on technological solutionism to solve complex problems (ref: algorithmic responses, Napalm case)
- Emerging tension between approaches w. imp. human rights implications
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 apply equally online; no. of companies use international, regional or national sanctions lists.

• Microsoft has announced it is using the consolidated UN sanctions list to inform its decisions; Facebook, Google use US lists.

**Terms of Service and emerging policy**

• Some companies are adapting terms of service (TOS) and using community guidelines to prohibit certain content and activity and shape norms of behaviour.

• Companies generally have a zero-tolerance policy for terrorist content and activity on their platforms and have committed to ensuring user 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.
Based on the principle of openness and NGO advocacy, major technology companies now regularly produce Transparency Reports; some limitations/ challenges.
In 2015 the top three tech companies took down over 160,000 items of concern for governments and this is increasing annually.

Content takedowns requested by governments (2011-2015)
Industry responses: Other than developing policy, industry is taking proactive steps to counter the terrorist use of their platforms

- Developing **guidance and systems** (human and automated) for content flagging, referral and content/account removal and for remedial action

- **Training** programmes for employees and users
- **Employ specialist legal teams**
- **Content policy teams** now play critical roles

- Cooperating with **government** or **regional internet referral units** (IRUs), e.g. UK CTIRU, Netherlands, EU IRU based in the Hague (number of challenges)

- Developing tools and mechanisms to **counter the narratives of terrorist** and **violent extremist groups** and their followers
- Carried out **in conjunction with government agencies** and/or **civil society** and **community organizations** (number of challenges)
**Industry responses:** In summary, industry actors are already developing a voluntary framework but there are some persisting tensions

- The gradual **emergence of a voluntary policy framework guiding corporate action** in this area.
- Recognizes the importance of **enhancing public safety and ensuring that** actions remain anchored in the rule of law,
- While also protecting and **respecting human rights** and **fundamental freedoms** and upholding core principles such as **transparency, accountability, predictability and remedy**

- Notably evident in some of the measures govts. are taking in response to public security concerns, such as:
  - **Content restrictions** (removal, blocking or filtering)
  - **Lawful/ unlawful orders** compelling companies to provide access to user data
  - Steps to increase **greater state involvement** in **internet governance.**
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

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

**Disconnect between ONLINE and OFFLINE** PVE efforts

**Limited investment** in long-term education and critical thinking
International Framework for Action:

- **UN** Security Council Resolutions – significant activity
- **UN** Security Council Presidential Statement - plan for “comprehensive international framework” for counter-narratives (S/PRST/2016/6 of 11 May 2016)
- **UN** Secretary-General Action Plan for Preventing Violent Extremism
- **UN** General Assembly Counter-Terrorism Strategy

**United Nations**

**Others**

- EU
- Council of Europe
- OSCE, OAS, AU, SCO
- G7, G20
### International Framework for Action: Norms & principles alongside growing body of expert reports and consultations guiding action in this area

<table>
<thead>
<tr>
<th>Examples of Norms / Principles</th>
<th>Reports from international organisations</th>
</tr>
</thead>
</table>
| • UNDHR; UN ICCPR; UN Human Rights Council Resolutions; UN Guiding Principles on Business and Human Rights | • UN Special Rapporteur on Freedom of Opinion and Expression  
- The Use of Encryption and Anonymity in Digital Communications  
- The Role of the Private Sector in the Digital Age |
| • European Commission’s ICT Sector Guide on Implementing the UN Business and HR Principles | • Reports of the Council of Europe on:  
- The Rule of Law on the Internet and in the Wider Digital World  
- Filtering, Blocking and Take-Down of Illegal Content on the Internet |
| | • UNCTED-ICT4Peace report ‘Private Sector Engagement’ |
What is the cyber dimension?

The nature of the threat

- Cyber / protecting CI and essential services is a different issue from terrorist use of the internet.
- Threat comes and goes in policy circles - no indication that capacity of groups has moved beyond social media/ propaganda / financing
- Actions underway in different fora to protect CI and essential services from ICT/cyber-enabled attacks - apply equally to potential terrorist attacks
- Considered through lens of this project with our industry partners
- ICT4Peace other work relating to international security and cyber/ICT, esp. vis international law, norms of state behaviour, and confidence and capacity building measures

Cyber security and PVE efforts

- What analogies can be drawn between PVE efforts and securing cyberspace in general?
  - Capacity building; critical thinking; dialogue between actors and engagement of private sector, civil social and academia - these require more than just technological solutions
Recommendations from our report:

1. Build on existing policy initiatives and avoid duplication of effort

2. Strengthen dialogue on the emerging normative framework through multi-stakeholder engagement

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
     3. Promote coordination of effort across organisations

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 ToS, sample gov. legislation
     - examples of public-private/multi-stakeholder initiatives
     - policy-relevant research on changing nature of the threat
     - tool-kits for capacity building