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

A project sponsored by
the Governments of Spain and Switzerland,
ICT4Peace Foundation
&
Facebook, Microsoft and Kaspersky Lab

The views expressed herein are those of the author(s) and do not necessarily reflect the views of the United Nations or the ICT4Peace Foundation.

Credits:
Front page image Grandjean, Martin (2014), Wikipedia Commons.

Background

Since the late 1990s, as global connectivity has increased, terrorist and violent extremist groups have become more sophisticated in their use of information and communications technologies (ICT), in particular the internet and social media, to radicalise and recruit terrorist fighters and supporters, spread propaganda and transfer knowledge and funds or to generate funds in support of their ideas and operations. These developments have important implications for the private sector, in particular those technologies and social media companies whose products and services are used by millions, if not billions of people across the globe.

On the one hand, the companies in question feel a business incentive to create a digital environment where their users feel safe, and are increasingly compelled by governments to cooperate in blocking, filtering, countering or removing content or accounts on the grounds of public safety or national security concerns. In addition, users expect the companies to be transparent, accountable, respect privacy and freedom of opinion and expression and guarantee remedy, while also ensuring an open, free and secure internet. This reality has led to greater voluntary engagement of the private sector in efforts to respond to terrorist use of the internet and ICT. This engagement includes industry-driven initiatives and participation in multi-stakeholder and public-private fora focusing on normative, technical and organizational issues, as well as engagement with academia.

Together, these efforts are resulting in the gradual emergence of a normative framework shaping private and public action in this area, as well as growing awareness of the scope of the problem. However, important challenges remain, including the reality that many industry actors are yet to engage and the risk that some government actions can undermine this progress.

1. Project Objectives

The key objectives of the project were to identify the emergence of norms of voluntary self-regulation amongst the private sector in their responses to terrorist use of their products and services, highlight multi-stakeholder and public-private initiatives aimed at supporting efforts in this area, identify persisting challenges, and recommend further areas for engagement. To this end, the project conducted an initial series of consultations with multiple stakeholders on the following:

- Existing and emerging threats relating to the use of the internet and ICT for terrorist purposes.
- Industry approaches to responding to terrorist use of the internet and ICT and emerging principles, standards and practices shaping that response.
- Trends in multi stakeholder and public-private engagement in responding to terrorist use of ICT.
- Mechanisms/ platforms for information exchange and sharing of lessons/ practice on the industry response to terrorist use of the internet and ICT.

The consultations were carried out largely through three workshops held in:

- Geneva (inception meeting), 8 April, 2016, hosted by OHCHR
- Zurich, Switzerland on 25 August 2016, hosted by ETH Zurich

- California (Silicon Valley), USA on 12 September 2016, hosted by Microsoft
- Kuala Lumpur, Malaysia on 03 November 2016, hosted by the Institute of Strategic and International Studies (ISIS), Malaysia

Some 45 participants from the private sector, civil society and academia and regional organizations attended each workshop (Annex 1). An Advisory Group involving UN representatives, senior policy representatives from global technology companies, academic and civil society experts and regional organizations accompanied implementation of the project and the workshops (Annex 2).

2. Key findings

2.1 An Emerging Policy Framework

Unlike other sectors such as the financial services and the telecommunications sectors, which are highly regulated and in which formal requirements and obligations have already been established, regulation vis-à-vis the internet and the services and products that operate through it remains largely voluntary, due in large part to the trans-border complexities of the domain itself. This poses challenges on a number of fronts, particularly when dealing with online terrorist or violent extremist content and activity.

There is a growing trend, however, of self-regulation efforts among by industry actors in response to online terrorist content and activity. Indeed, in some regions, technology and social media companies are sharing experiences, policy and practice on content management-related issues and participating in multi-stakeholder or public-private initiatives such as the Global Network Initiative dialogue or the EU Internet Forum.[1] The combined results of these efforts, which in some instances combine with stepped-up efforts of the telecommunications sector to respond to important normative concerns, suggest the emergence of a voluntary policy framework guiding both private and public sector action in this area.[2] While still at an early stage, this emerging policy framework recognizes the importance of enhancing public safety with actions that remain anchored in the rule of law, protecting and respecting human rights and fundamental freedoms consistent with international law, including international human rights law, and upholding core principles such as transparency, accountability, predictability and remedy.[3]

At the same time, there is a risk that emerging policy framework may be undermined by some of the measures governments are taking in response to public security concerns

[1] In 2015, GNI launched a policy dialogue to explore key questions and considerations concerning government efforts to restrict online content with the aim of protecting public safety, and to discuss the human rights implications of such government actions. To this end it has convened a series of roundtable discussions with academic, civil society, investor, and company participants with other experts and representatives from governments and international organizations. The consultations and extensive deliberations have resulted in a set of recommendations for governments and companies. See 'Extremist Content and the ICT Sector: A Global Initiative Policy Brief', forthcoming, November 2016. Available at: Available at: https://www.globalnetworkinitiative.org/sites/default/files/Extremist-Content-and-ICT-Sector.pdf The EU Internet Forum was established in December 2015. It brings together EU Interior Ministers, high-level representatives of major internet companies, Europol, the EU Counter Terrorism Co-ordinator and the European Parliament. The goal is to reach a joint, voluntary approach based on a public-private partnership to detect and address harmful material online by protecting the public from the spread of terrorist material and terrorist exploitation of communication channels to facilitate and direct their activities and making better use of the Internet to challenge terrorist narratives and online hate speech. See: http://europa.eu/rapid/press-release_IP-15-6243_en.htm

[2] On the telecommunications industry and key normative issues such as freedom of expression and privacy, see the Telecommunications Industry Dialogue as well as the growing participation of telecommunications companies in the GNI's work, including its policy dialogues: http://www.telecomindustrydialogue.org and https://www.globalnetworkinitiative.org/news/global-network-initiative-and-telecommunications-industry-dialogue-join-forces-advance-freedom

[3] Ibid. See also the UN Business and Human Rights Principles in Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy Framework" (A/HRC/17/4 and A/HRC/17/31); the European Commission's *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*; the Manila Principles of Intermediary Liability; and the African Declaration on Internet Rights and Freedoms and the GNI Principles on Freedom of Expression and Privacy.

posed by the growing incidence of terrorist use of the internet. These measures include restrictions, lawful or unlawful orders compelling companies to provide access to user data and steps to increase greater state involvement in internet governance.

2.2 Existing and Emerging Threats

The project consultative process confirmed that the principal uses of the internet and ICT for terrorist purposes remain anchored in communications and propaganda, radicalisation and recruitment of potential fighters and followers, transferring and raising funds and transferring or sharing knowledge. These uses evidently change in accordance with context and the degree of internet penetration in a given location, among other factors. They are viewed as posing serious risks to public safety and, increasingly, to international peace and security. Beyond these uses, there is growing concern that terrorist groups *may* eventually develop the capacities and capabilities to use the internet and broader cyberspace to conduct disruptive and destructive attacks against critical infrastructure, with the potential to cause significant harm.

Some uses of the internet and ICT for terrorist purposes are often indistinguishable from regular use of the internet by other users or groups, making it very difficult to address the issue. Calls by governments at the international, regional and national levels to take ‘urgent action’ against online extremism or terrorist use of the internet are growing, notably in terms of restricting online content with the aim of protecting public safety. Such calls to action tend to be directed against intermediaries (i.e. internet service providers (ISPs), technology and social media companies) rather than the actual creators of the content, often due to the fact that creators of terrorist content operate out of extremely dangerous territories, where a law enforcement approach is simply not feasible. There are competing arguments as to the merits of these approaches. On the one hand, they are often perceived as enhancing public safety and protecting the vulnerable. On the other, they are held to violate the human rights of users, and undermine trust in companies as well as in government.

Moreover, the use of the internet and ICT for terrorist purposes will likely remain a problem as long as the off-line real-world issues driving such activity are not resolved. Since understanding and adapting to the dynamics of context is key to any solution, it remains unclear how policies focused principally on or over-weighted toward short-term technological solutions, such as algorithmic content removal, or solutions centred on restricting content or bulk data collection will yield long-term results. Similar appreciations are applicable to current approaches to countering the narratives of terrorist or violent extremist groups. In short, much needs to be done by all parties to ensure a more appropriate balance between *offline* prevention and online *countering* measures and in demonstrating what yields effective results.

2.3 Current Industry Approaches

Driven by business, user and government prerogatives, major technology and social media companies are investing significant resources in developing voluntary measures to respond to terrorist use of their products and services. These efforts are largely approached from a <u>content management perspective</u> and involve:

- Adapting terms of service (TOS) and community guidelines to prohibit certain content, activity and shape norms of behaviour. In general, companies have a zero-tolerance policy for terrorist content and activity on their platforms and have committed to ensuring the safety of their users. In light of the challenges in determining *who* terrorist actors actually are, some companies use international, regional or national sanctions lists to guide their decision-making on this issue.[4]

- Developing guidance and systems (human and automated) for content flagging, referral and content/ account removal and for remedial action.
- Establishing guidance and systems for responding to law enforcement and government content/ account removal or data access requests.
- Establishing transparency measures for government requests.
- Establishing, training and sustaining content policy and legal teams.
- Cooperating with government or regional internet referral units (IRUs), when required.
- Developing tools and mechanisms (both human and automated) 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.

The technology sector sometimes refers to the importance of failing fast – learning from real world experience and adapting in near real-time. There will clearly be situations where errors are made, especially given the complexity of implementing policy in this area, and the sheer scale of data involved on a daily basis. In the same way, there will be takedown requests that are impractical, inappropriate, or politically partisan.

Undoubtedly, some practices - notably restricting content, account removal, providing access to user data, or engaging in online social engineering practices - continue to raise important normative, ethical and legal questions and, in some instances, implicate the legitimacy, transparency and accountability of those same private actors that are key to building and consolidating trust online.

Hard data in the battle against terrorist use of the internet are elusive. Hence, measuring overall impact of private sector (and often also public sector) efforts to counter-terrorism efforts remains challenging since the evidentiary basis linking such actions to broader prevention strategies remains weak. This is also the case with online counter-speech or counter-narrative efforts.[5]

Start-ups and smaller technology and social media companies face challenges developing and implementing many of these measures due in large part to the resources (human, financial, management) required to develop and sustain them.

[4] For instance, Microsoft recently announced that it "will consider terrorist content to be material posted by or in support of organizations included on the Consolidated United Nations Security Council Sanctions List that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups". See 'Microsoft's approach to terrorist content online'. http://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.00008cf0g1gyufreset139jj0nsg1. For the UN SC Consolidated Sanctions List, see: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

[5] See, for example, the work of the Global Forum for Media Development on this subject. Available at: http://gfmd.info/en/site/news/957/GFMD-Workshop-"Mediadev-CVE--counter-propaganda-Where-is-the-problem"-Brussels- Press-Club-26-April-2016.htm. See also: Radsch, C (2016), Media Development and Countering Violent Extremism: *An Uneasy Relationship, a Need for Dialogue.* Cima/ NED publication. http://www.cima.ned.org/wp-content/uploads/2016/10/CIMA-CVE-Paper_web-150ppi.pdf; Ferguson, Kate (2016) Countering violent extremism through media and communication strategies: A review of the evidence http://www.paccsresearch.org.uk/wp-content/uploads/2016/03/Countering-Violent-Extremism-Through-Media-and-Communication-Strategies-.pdf; SDI (2016) Impact of Counter Narratives Online, ISD http://www.strategicdialogue.org/wp-content/uploads/2016/08/Impact-of-Counter-Narratives_ONLINE.pdf

Technology can be used for good or for malicious purposes. That said, awareness among companies and developers of terrorist use of internet products and services often varies, largely due to the absence of tools or mechanisms to share such information between or with industry actors.

In some cases, companies have been criticized for their collaboration with internet referral units (IRUs) on the grounds that such mechanisms allow law enforcement to rely on company terms of service to inform content-removal related decisions. Some criticism has touched upon perceived lack of transparency and accountability in this type of collaboration.

In the EU context, and given mounting public security concerns surrounding terrorist activity, an internet referral unit was established within EUROPOL in 2015. It is a voluntary arrangement stemming from the European Agenda for Security and is accountable to the European Parliament.[6] In addition to support provided to EU Member States, the EU IRU cooperates with third party partners within the framework of the EU Internet Forum, engaging with online service companies to promote 'self-regulation' activities by the online industry. The overall objective of the EU IRU is to reduce accessibility to terrorist and violent extremist propaganda on the internet by identifying and referring relevant online content to the hosting internet service provider, with a clear assessment of how terrorist material it has identified might be in breach of their terms of service. It uses the Consolidated UN Security Council Sanctions List as a basis for deciding what content to refer.[7]

According to its first annual report of activities, the EU IRU has proven to show effectiveness in the sense that since its inception, companies have removed a significant percentage of content referred to them.[8] It has also committed to transparency through the publication of said annual activity reports, for which both companies and civil society actors have commended it.[9] There are concerns, however, about promoting such mechanisms globally as a good practice, in particular in those jurisdictions where principles such as transparency, accountability and remedy cannot be guaranteed. [10]

2.4 Mechanisms for Information Exchange/ Sharing of Standards and Practices and Capacity Building

In the United States, a number of voluntary initiatives have been established to support information/ practice sharing among technology and social media companies, sometimes involving companies from other regions and representatives from other sectors (e.g. financial services) as well as researchers or civil society actors.[11] These include participation by some of the global technology and social media companies in the EU Internet Forum as well as participation of both global and smaller companies in a voluntary round table forum used to discuss trends in both the use of their products and services as well as tools and mechanisms to respond.

[6] Zurich workshop, 25 August, 2016. See: http://ict4peace.org/wp-content/uploads/2016/10/Summary-Report-Zurich-Workshop-FINAL.pdf
[7] See: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list
[8] See: EU Internet Referral Unit: Year One Report – Highlights. Available at: https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights
[9] Zurich workshop, 25 August, 2016.
[10] GNI (2016), Extremist Content and the ICT Sector: A Global Network Initiative Policy Brief.
[11] In the banking sector there are already quite well established information sharing groups at international/ regional/local level, often with established government communication channels. These are more focused on misuse of banking services in general rather than specific use of ICT. Efforts to create information exchange links between the financial services sector and ICT and social media companies are increasing.

A more recent industry initiative involves a joint effort by Facebook, Microsoft, Twitter and YouTube aimed at removing 'terrorist content' from their services via image hashing or finger-printing. The companies involved will share hashes "of the most extreme and egregious terrorist images and videos [the companies] have removed from [their] services — content most likely to violate all of our respective companies' content policies".[12] The images will be processed through a form of clearing-house or "shared industry database". While only just taking off, the announcement of the initiative has attracted significant media and civil society attention.[13]

Other more normative-focused initiatives include the voluntary Global Network Initiative (GNI), an organisation involving industry (technology, social media and telecommunications companies), investors, civil society and academic experts, mainly from North America and Europe but increasingly from Latin America and Asia. The GNI focuses on ensuring exchange between these actors, developing trust and international standards and has played an important role in ensuring that a focus on core principles, including the UN Principles on Business and Human Rights, are sustained in industry content management efforts.[14] The outcome of its recent industry policy dialogue on Responding to Online Extremism is especially important for those content management issues relating directly to the subject of this report.[15]

Nothing similar to this initiatives exists in other regions but is arguably needed. As noted, resource constraints or competing priorities often limit the engagement of smaller companies and other actors in these efforts.

International, regional and specialised inter-governmental agencies (the UN, the EU, OSCE, Council of Europe, the OAS, the FATF where online transfers and FinTech are concerned, EUROPOL and INTERPOL) are also establishing fora for exchange of information and experiences with technology and social media companies or to build capacity. In addition, a number of governments are supporting the establishment of regional counter-narrative hubs to share information and exchange practices. A number of UN Security Council and Human Rights Council Resolutions and Statements, the UN General Assembly's Counter-Terrorism Strategy and the more recent Secretary-General Plan of Action provide an over-arching policy framework for work in this area.

Across regions, there is an important knowledge/ awareness gap within the start-up community and among investors, law enforcement and national security agencies, regulators and the legal community on issues relating to terrorist use of the internet, including on the emerging policy framework referenced above and how to access or even follow policy guidance.

3. Recommendations

A growing number of private sector actors are engaged in efforts to respond to the use of the internet and ICT for terrorist purposes. The findings of this project shed light on an emerging content policy framework anchored in ensuring public safety while also respecting

[12] 'Facebook, Microsoft, Twitter and YouTube collaborate to remove 'terrorist content' from their services'. TechCrunch. December 5, 2016. See also 'Partnering to Help Curb Spread of Online Terrorist Content'. Facebook News. December 5, 2016.

[13] For a critique on the initiative, see: 'Companies that partner to counter "violent extremism" online must also collaborate to respect rights'. Access Now, December 8, 2016.

[14]

[15] See: Extremist Content and the ICT Sector. GNI, November 2016. Available at: https://www.globalnetworkinitiative.org/news/responding-online-extremism-without-harming-free-speech-and-privacy

the rule of law and universal human rights and principles. At the same time, the findings highlight some of the normative, technical, informational and organisational challenges persisting in current responses to the issue. To this end, the project makes a number of interdependent recommendations for further work. They are largely centred on trust-building within and among sectors, consolidating the emerging normative base for public and private action, establishing mechanisms and platforms for sharing knowledge and information, exchanging practices, capacity building and awareness raising.

3.1 Dialogue Facilitation

Scale up and strengthen existing mechanisms for relationship brokering/ dialogue facilitation and knowledge sharing across regions on existing and emerging challenges among private sector actors and between private sectors and non-private sectors, such as regional inter-governmental organisations, government representatives, academia, and civil society, including affected communities.

3.2 Strengthen the Emerging Normative/Policy Framework

Build on/ strengthen existing initiatives to help consolidate the emerging global normative/policy framework anchored in ensuring public safety and the security of civilians, while also respecting the rule of law and core universal human rights and principles, particularly transparency, accountability and remedy to guide both public and private responses to the use of the internet and ICT for terrorist purposes. The recommendations stemming from the GNI policy dialogue can serve as an important normative basis for this process.

For instance, efforts should be made to ensure that transparency, accountability and remedy underpin any government-backed mechanisms and structures to use technology and social media companies own mechanisms (e.g. terms of service) for reporting violations of companies' terms of service to request the removal of content. To this end, efforts should be made to ensure that:

- Companies are transparent with their users, to the extent permitted by law, about government orders to remove or restrict content.

- Governments do not pressure companies to change their terms of service. Terms of service are developed in order to deliver user experiences that are appropriate for the nature or type of service, and the user community of the service.

- When governments refer content to companies for removal under companies' terms of service, they guard against the risks that such referrals may set precedents for extra-judicial government censorship without adequate access to remedy, accountability, or transparency for users and the public. If governments make such referrals, they should be transparent about, and accountable for, such referrals.

Other actions could include:

- Facilitating understanding of practical interpretations for common definitions of terrorist-related or terrorist-inspired content", or similar.
- Directing resources to public-private pilot initiatives aimed at ensuring public safety and security while also protecting the privacy of users. For instance, in the area of

surveillance, this could include testing the application of public health logic surveillance models for the detection of at-risk factors or dangerous/risky uses of the internet and ICT.

Where counter-narratives/ counter-messaging are concerned, public and private actors should use the opportunity of S/PRST/6 - which tasks the CTC to develop a ‘comprehensive international framework’ - to ensure that said framework is also centred on building trust, is anchored in international norms and standards, and developed with the participation of those most affected by current trends.[16]

Concerning emerging threats relating to potential use by terrorists of the internet or broader cyberspace for disruptive or destructive attacks against, for instance, critical infrastructure, actions should be oriented to promoting awareness and understanding of the policy work already underway by governments and experts regarding the protection of critical infrastructure[17]or on the applicability of existing international law to ‘cyber terrorism’,[18] as well as other initiatives by the OSCE, the Freedom Online Coalition (FOC), and through multi-stakeholder fora.

3.3 Strengthen coordination between different inter-governmental initiatives

Numerous inter-governmental organisations are embarking on initiatives aimed at responding to online terrorist or violent extremist content and activity involving collaboration with technology, social media and telecommunications companies. Some form of informal coordination among these organisations and between them and companies would help avoid overlap, and help ensure more effective use of resources on all sides.

3.4 Strengthen the Links Between Offline Prevention Efforts and Online Content Management and Counter-Narrative Efforts

The UN Secretary-General’s Plan of Action on Preventing Violent Extremism (PVE) strategy – which builds on the earlier UN GA Counter-Terrorism Strategy - provides a strong basis upon which to strengthen these links. Moreover, the Action Plan and subsequent report provide detailed guidance for addressing the connection between the off-line and online worlds, notably through its three pillars which address drivers of violent extremism, shaping policy at international, regional and national levels, and taking action in seven priority areas, many of which this project’s recommendations resonate with.

More specifically, and building in part on the outcome of the GNI policy dialogue, efforts should be stepped up to ensure that:

- Governments protect and respect human rights when developing, implementing, and enforcing laws and policies meant to address terrorist and extremist content online.
- Government legal demands to restrict content for the purpose of protecting public safety are pursuant to the rule of law. They should respect and protect freedom of

[16] Threats to Interational Peace and Security Posed by Terrorist Acts. S/PRST/2016/6 of May 2016. Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=S/PRST/2016/6

[17] See for example, the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications, which includes a number of recommendations relating to protection of critical infrastructure. The Group does not focus on terrorism but rather, state use of ICT. National level efforts to protect critical infrastructure generally apply to protecting CI from all nature of threats. See: https://www.un.org/disarmament/topics/informationsecurity/

[18] Cybersecurity, Terrorism and International Law. Study Group Final Report. July 2016. Available at: http://www.ila-hq.org/en/committees/study_groups.cfm/cid/1050

expression and privacy, and be directed at creators of content, rather than intermediaries, whenever possible.
- Resources are invested in demonstrating how public and private efforts relating to either restricting content or countering narratives contribute to the longer-term prevention of terrorism and violent extremism.

3.5 Establish a Global Mechanism for Knowledge and Information Sharing

Develop a global knowledge portal/repository for sharing and providing access to information on international standards and principles, corporate policy and terms of service, guidelines, good practices, information on existing initiatives (inter-governmental initiatives such as the EU Internet Platform, multi-stakeholder initiatives such as the GNI, initiatives led by international and regional organisations), and sample government policy and legislation.

3.6 Invest in Policy-Relevant Research

Strengthen mechanisms aimed at facilitating reciprocal exchanges between the private sector and academia, particularly on trends and emerging issues.

3.7 Build Capacity and Raise Awareness

Develop tools and mechanisms for capacity building and awareness raising, especially focused on small and medium size technology and social media companies (but also targeting business and law schools, law firms, and civil society groups).

3.8 Invest in Critical Thinking and Media Literacy

Strengthen and promote digital literacy and critical thinking skills to prevent and counter violent extremism leading to terrorism, including by building the technical capability of civil society and media development organizations, religious and community leaders, women, youth, and other credible voices to promote alternative messages and to challenge terrorist propaganda online.

4. Next Steps

This project has demonstrated the willingness and openness of private companies to engage in discussions with the UN and other stakeholders on the steps they are taking to respond to terrorist use of their products and services and the numerous challenges they face in seeking to respond to oft-competing business, user and government interests, which also differ across regions.

It will be important to leverage this opportunity to deepen dialogue between these actors, build trust and raise awareness around current progress and the challenges that remain. To this end, this project will seek to establish a second phase covering a two-year period and centred on supporting the implementation of the recommendations listed above and reporting on progress to the United Nations and other international and regional stakeholders.

ANNEX 1

Participants in Workshops/ Consultations

Private Sector

- Affinis Labs
- Altel Communications Sdn Bhd
- Axial Group Berhad
- Cloudflare
- CryptTalk
- DiGi
- Digital Shadows
- Dropbox
- Facebook
- Google
- iKeepSafe.org
- JMS Public Relations
- Kaspersky Lab
- KPMG
- Kudelski Group
- LaQuadratureduNet
- Microsoft
- Mozilla
- Open Systems AG
- Orange
- PatternEx
- Phandeeyar
- Pretty Easy Privacy
- Rappler Inc.
- SentinelOne
- Sidley Austin LLP
- SITE Intelligence Group
- Soufan Group
- Snapchat
- SSP Blue
- Standard Chartered Bank
- Telefonica
- Telekom Malaysia
- Treasure My Text
- Trust & Safety Group
- Tune Talk
- Twitter
- Twoo / Massive Media
- UBS
- Vimeo
- Wickr
- Yahoo!
- YTL Communications
- ZeroFOX

Trade associations

- Electronic Money Association

Civil society

- Access Now
- Anti-Defamation League
- Center for Democracy and Technology
- Committee to Protect Journalists
- Electronic Frontier Foundation
- Electronic Frontier Foundation Finland
- FSM
- Global Network Initaitive (GNI)
- Institute for Policy Analysis of Conflict
- International Centre for Counter-terrorism
- Moonshot CVE
- Open Net Initiative
- Samir Kassir Foundation
- SECDEV Foundation
- Southern Poverty Law Center
- Tech4GS (Technology for Global Security)
- VoxPol

Academia/ Think-Tanks

- Brennan Center for Justice, NYU School of Law
- Centre of Excellence for National Security (RSIS)
- Dublin City University/VoxPol
- ETH
- Institute for Strategic and International Studies (ISIS), Malaysia
- King’s College London
- Martin School/University of Oxford
- National Law University Delhi
- Nanyang Technological University
- University of California, Irvine (International Justice Clinic)

Government and Inter-Governmental Organisations

- Council of Europe
- European Commission
- EUROPOL IRU
- GCTF
- Government of Spain (via Embassy in Switzerland)
- Government of Switzerland (MOFA/ CT)
- Government of Canada (which branch)
- Government of Kyrgyzstan (CT structure)
- Government of United Kingdom (Home Office)
- Government of the United States (US Department of State and US Naval Criminal Investigative Service)
- INTERPOL
- OAS
- OSCE
- RATS-SCO
- UN CTED
- UNICRI
- UN ISIL/ AQ Monitoring Team
- UN OHCHR
- UN OICT
- WEF

Multi-Stakeholder and Public-Private Initiatives

- GCERF
- Global Network Initiative (GNI)

ANNEX 2

Project Core/ Advisory Group

- Microsoft
- Facebook
- Google
- Kaspersky Lab
- AskFM
- Dublin City University/ VoxPol
- ETH
- The Global Network Initiative (GNI)
- The Global Cyber Security Capacity Centre (GCSCC), Oxford Martin School
- ICT4Peace
- UNCTED
- UN Special Rapporteur on Freedom of Opinion and Expression
- UN ISIL/AQ Monitoring Team
- EU Home & Migration Affairs

Project Team

Joint project directors: Marc Porret (UNCTED), Dr. Camino Kavanagh (ICT4Peace), Adam Hadley (ICT4Peace)
Project researchers/ associates: Sophia Khan, Diana Ruiz (ICT4Peace), Matteo Sestito and Katie Wilson (UNCTED).

Contact: info@ict4peace.org

ICT for peace foundation

CTED
Counter-Terrorism Committee
Executive Directorate