Countering Violent Extremism (CVE) Working Group
Strategic Communications Initiative

Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online

Introduction

Since its inception, the Internet has offered innumerable opportunities for society, facilitating economic development, communication, participation and access to information. An open, secure, stable, accessible, and peaceful ICT environment is essential for all and requires effective cooperation among States to reduce risks to international peace and security.[1] However, the Internet is also often misused by violent extremists and terrorists. Violent extremist and terrorist groups are increasingly using communication technologies to fundraise, intimidate, train, radicalize, recruit and incite others to commit violent extremist and terrorist acts. Governments should take appropriate steps to prevent and counter the use of the Internet for violent extremist and terrorist purposes (including through social media), while respecting privacy and freedoms of expression, association, peaceful assembly, and religion or belief, as well as the need to preserve global connectivity and the free and secure flow of information. These responses can be divided into two main categories:

1. **Content-based responses**: Government efforts to address the availability and accessibility of violent extremist and terrorist propaganda through international cooperation and to engage with private companies to counter terrorism and violent extremism online on a collaborative basis, including content reporting, removal, filtering and appropriate regulation/legislation.
2. **Communications-based responses**: Government efforts to support or assist in challenging the appeal of violent extremist and terrorist propaganda through strategic communications, including supporting civil society organizations to use counter- and alternative narratives both online and offline.

The UN General Assembly noted in its fifth review of the *United Nations Global Counter-Terrorism Strategy* the importance of cooperation among stakeholders in the implementation of the Strategy, including among Member States, international, regional and subregional organizations, the private sector and civil society, to address the increasing use of the Information and Communication Technologies (ICT) by terrorists and their supporters, while respecting human rights, fundamental freedoms and complying with international law and the purposes and principles of the Charter. The General Assembly stressed that it is essential to develop the most effective means to counter terrorist propaganda, incitement and recruitment, including through the Internet, in compliance with international law, including international human rights law. Furthermore, The General Assembly recommends that Member States consider the implementation of relevant recommendations of the UN Secretary-General's *Plan of Action to Prevent Violent Extremism,* as applicable to the national context, which identifies strategic communications, the Internet and social media as key action areas in preventing and countering violent extremism and terrorism.[2]

---

[1] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174), 22 July 2015, para. 2.

[2] UN Global Counter-Terrorism Strategy Review (A/RES/70/291), 19 July 2016, operative paras. 42f. and 40. For the UN Secretary-General's Plan of Action to Prevent Violent Extremism, cf. A/70/674, 24 December 2015, here para. 55.

The UN Security Council issued a Presidential Statement in May 2016 (S/PRST/2016/6) recognizing that the international community should consider developing effective means to counter terrorist propaganda, incitement and recruitment, including through the Internet, in compliance with international law, including international human rights law.[3] As requested by the Security Council, the Counter-Terrorism Committee submitted to the Security Council on 28 April 2017 a proposal for a comprehensive international framework to counter-terrorist narratives.[4] Based upon this submission, the Security Council adopted resolution 2354 (2017), which notes the urgent need to globally counter the activities of certain violent extremist and terrorist groups to incite and recruit to commit terrorist acts and further notes that terrorists use ICT services, such as the Internet and social media, to help craft and spread distorted narratives as well as to mobilize resources and garner support from sympathisers.

At the Seventh Ministerial Plenary Meeting in New York on 21 September 2016, Global Counterterrorism Forum (GCTF) Ministers endorsed the launch of a review and assessment of existing governmental best practices and lessons learned in online prevention and counter-measures to address violent extremism online as part of the GCTF's *Initiative to Address the Life Cycle of Radicalization to Violence* (Life Cycle Initiative).

Accordingly, the non-binding recommendations below compile a non-exhaustive list of governmental good practices regarding strategic communications and social media aspects in preventing and countering violent extremism and terrorism online for GCTF Members – as well as any other interested Government. The good practices expressed in this document were identified in meetings and subsequent discussions with GCTF Members, reflecting their experience in this regard. Moreover, with these recommendations, the GCTF aims to support and complement existing work and initiatives by other international and regional organizations, namely the UN and other relevant stakeholders involved in this context.[5]

The good practices are divided into three sections:

- Section I addresses overarching good practices for preventing and countering violent extremism and terrorism online;
- Section II addresses good practices for content-based responses; and
- Section III addresses good practices for communications-based responses.

In this respect, Sections I, II and III are considered complementary to pursuing a comprehensive approach to preventing and countering violent extremism and terrorism on the Internet and social media platforms.

---

[3] UN Security Council, Statement by the President of the Security Council (S/PRST/2016/6), 11 May 2016.

[4] Comprehensive International Framework to Counter-Terrorist Narratives (S/2017/375), 28 April 2017.

[5] This includes the UN-CTED/ICT4Peace-initiative focused on deepening the understanding of private industries' responses to the terrorist use of their products and services and related challenges and to promote self-regulation and sharing good practices across the ICT industry, www.techagainstterrorism.org; the EU Internet Forum, on terrorist material, the EU Internet Forum's Civil Society Empowerment Programme (launched in 2016 at the second EU Forum to support civil society efforts to develop effective counter-narratives online in partnership with the private sector), the European Commission's code of conduct that includes a series of commitments to combat the spread of illegal hate speech online in Europe; the EU Clean IT Project, a public-private dialogue around the terrorist use of the Internet; the EU Radicalization Awareness Network (RAN) Working Group on Communications and Narratives (RAN C&N), which looks at best practices and lessons learned in the delivery of counter-narrative communications between civil society practitioners; the European Strategic Communications Network (ESCN) tasked with establishing and organizing a network of EU Member States, using a communications approach to understand and address the emerging communications challenges including ISIL/Da'esh's divisive discourse and violent right wing extremism; or the Global Coalition Communications Cell, which runs campaigns and builds capacity to counter ISIL/Da'esh's communications.

These recommended good practices are intended to address violent extremism that is conducive to terrorism in all its forms and manifestations. It should be underlined that violent extremism and terrorism are not exclusive to any region, nationality, or belief. GCTF Members and other interested Governments are encouraged to consider the implementation of these good practices in their respective national contexts while tailoring them to local conditions and cultures, and ensure that measures taken to counter terrorism and violent extremism, including to counter those narratives, comply with Member States' obligations under international law, including international human rights law, and respect the rule of law.

These recommendations stress the importance of firmly embedding content- and communications-based responses within a comprehensive online and offline approach to preventing and countering violent extremism and terrorism involving the active participation and collaboration of all States and international and regional organizations while respecting privacy and freedoms of expression, association, peaceful assembly, and religion or belief, as well as mentioned in the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 22 July 2015 the need to preserve global connectivity and the free and secure flow of information[6]. Such a comprehensive approach should encompass preventive as well as security and criminal justice measures, pursuant to international law and while ensuring national ownership, to address all drivers of violent extremism conducive to terrorism, both internal and external, in a balanced manner,[7] as well as manifestations of violent extremism and terrorism on the Internet and social media platforms. It is important for effectively addressing the availability, accessibility and influence of violent extremist and terrorist content online to provide for appropriate/effective investigation and prosecution, by the appropriate national authorities, of persons who engage in violent extremist and terrorist acts, such as the criminal facilitation of violent extremism and terrorism online, including recruitment, terrorist financing, attack planning and coordination, threat communications, and other crimes. In addition, such a comprehensive approach entails acknowledging the important role of the media in "enhance[ing] dialogue and broaden[ing] understanding, and in promoting tolerance and coexistence, and in fostering an environment which is not conducive to incitement to terrorism, as well as in countering terrorist narratives".[8] In its "Declaration on freedom of expression and information in the media in the context of the fight against terrorism", the Council of Europe had invited the media and journalists to consider namely bearing in mind their particular responsibilities in order not to contribute to the aims of terrorists, in particular by taking care not to add to the feeling of fear that terrorist acts can create, and not to offer a platform to terrorists by giving them disproportionate attention, and to consider adopting self-regulatory measures, where they do not exist, or adapt existing measures so that they can effectively respond to ethical issues raised by media reporting on violent extremism and terrorism, and implement them.[9]
The good practices included in this document do not endorse any specific approach but acknowledge the diverse approaches States take with regards to addressing violent extremism and terrorism and its narratives on the Internet and social media platforms.

---

[6] Cf. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174), 22 July 2015, para. 30. In his foreword, the UN Secretary-General refers to the need to «uphold the global commitment to foster an open, safe and peaceful Internet».

[7] UN Global Counter-Terrorism Strategy Review (A/RES/70/291), operative para. 39.

[8] UN Security Council Resolution 2354 (2017), preambular para. 13.

[9] Cf. Declaration on freedom of expression and information in the media in the context of the fight against terrorism, adopted by the Committee of Ministers on 2 March 2005 at the 917th meeting of the Ministers' Deputies (https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Decl-02.03.2005&Sector=secCM&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75&direct=true)

It is noted that States have the primary responsibility in countering violent extremism and terrorism. It is a State's prerogative to decide which approach is most effective, in compliance with its obligations under international law as well as in accordance with its national law.

Good Practices

I. General Good Practices for Preventing and Countering Violent Extremism and Terrorism Online

Good Practice 1: To adopt and implement law and policy frameworks at the national level to prevent and counter violent extremism and terrorism online.

Governments are encouraged to adopt and implement measures to prevent and counter violent extremism and terrorism online that are in compliance with States' obligations under international law and respect the principle of rule of law. These measures can range from developing and implementing national communications strategies to challenging violent extremist narratives,[10] to repudiating attempts at the justification or glorification *(apologie)* of terrorist acts, to prohibiting by law, as may be necessary and appropriate and in accordance with their obligations under international law, the incitement to commit terrorist acts.[11]

As affirmed in UN Security Council Resolutions 2354 (2017), 2178 (2014) and 1624 (2005), any law and policy measure taken on the national level to prevent and counter violent extremism and terrorism including online, has to comply with States' obligations under international law, in particular international human rights law, refugee law, and humanitarian law. This includes any obligations a State has undertaken under relevant international agreements, covenants and conventions such as the International Covenant on Civil and Political Rights (ICCPR), International Covenant on Economic, Social and Cultural Rights (ICESCR), and the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD). Importantly, it is noted that in the context of preventing and countering violent extremism, effective measures and the protection of human rights are not conflicting goals, but complementary and mutually reinforcing.

Furthermore, it is recommended that law and policy makers provide definitions and/or understandings of pertinent terms such as "(countering) violent extremism" and "terrorism" in their national laws and action plans.[12] The existence of such definitions can shape States' understanding of the problem, delimit their responses to it, and help to distinguish lawful from unlawful responses. Moreover, it avoids arbitrary interpretation and implementation of provisions which can undermine legal certainty and eventually the principle of the rule of law.

---

[10] UN General Assembly, Plan of Action to Prevent Violent Extremism, Report of the Secretary-General (A/70/674), 24 December 2015, para. 55 (a).

[11] UN Security Council Resolution 2354 (2017), preambular para. 12, and UN Security Council Resolution 1624 (2005), preambular para. 4 and operative para. 1 (a).

[12] Without precluding other definitions or terms found elsewhere, including in national law, a reference point which may be considered for what could be commonly understood as "terrorist acts" is provided by UN Security Council Resolution 1566 (2004), para. 3: "[…] criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature […]."

Good Practice 2: To maintain a comprehensive understanding of the current and likely future online threats presented by violent extremism and terrorism in each national and local context.

One of the intrinsic characteristics of the Internet is its technical complexity. Continuously evolving technology offers tremendous new opportunities, but also vulnerabilities that can be exploited by violent extremists and terrorists. Therefore, it is recommended that Governments maintain a comprehensive understanding of technological trends and the associated challenges they may present. This can be achieved by the analysis of relevant online audiences; their platforms of choice and the emergence of popular content. This will also provide an understanding of the impact of online "echo chambers" and algorithmic "filter bubbles" where applicable.[13]

Governments are also encouraged to invest in research and analytical tools to advance understanding of the online and offline impacts of violent extremist online communications to radicalize and recruit individuals to violence, and polarize communities. Such tools can also improve our understanding of broad trends in online conversations and of online audiences and influencers beyond terrorist communications

Good Practice 3: To develop a clear strategy to tackle violent extremism and terrorism online based on a whole-of-government and a whole-of-society approach, which coordinates both content- and communications-based responses, as well as offline activities, including education and engagement of civil society organizations where appropriate.

In order to ensure a comprehensive, scaled approach it is vital that efforts to tackle violent extremism online are aligned with a clear and overarching online strategy, which includes specific, measurable, and achievable goals and objectives.

The Government-led strategy should be underpinned by a well-defined "theory of change" that explains how (and why) both content- and communications-based responses employed contribute to the objectives and goals of the overall strategy, as well as safeguards put in place to ensure these responses are proportionate or generate unintended consequences. Governments are encouraged to ensure these responses are thoroughly monitored and evaluated against overall strategic goals and objectives using consistent and comparable indicators and methodologies.

This online strategy developed by Governments should promote a "whole-of-society" approach to promote synergies among all relevant stakeholders and should be incorporated into broader national strategies to prevent and counter violent extremism and terrorism and policy frameworks to ensure that online and offline efforts to tackle the threat are coordinated. This could include efforts to foster critical thinking, digital literacy and resilience through education, local community engagement activities, and other measures to address the social and individual factors that can lead individuals to support violent extremism and terrorism.

The efficacy of such a comprehensive strategy could be increased by the formation of a national Interagency Task Force which synchronises and integrates "whole-of-government" programmes and activities to prevent and counter violent extremism and terrorism, conducts strategic planning, and evaluates ongoing efforts in preventing and countering violent extremism and terrorism both online and offline.

[13] Online "echo chambers" describe the phenomenon where individuals are exposed to conforming ideas and opinions at the expense of alternative or dissenting views. "Filter bubbles" are likely to occur where search engines or social networks personalise search results or newsfeed content through machine-learning models and algorithms that recommend content based on an individuals' location, demographic information or past online behaviour, and is therefore more likely to agree with.

Good Practice 4: To develop, in collaboration with other relevant stakeholders, a common monitoring and evaluation framework that promotes transparency and facilitates greater understanding of the impact of responses.

Monitoring and evaluating programmes and policies regarding violent extremism is crucial to the development of realistic objectives and indicators of success, and to help ensure that measures adopted are impactful and sustainable. At the same time, such frameworks strengthen transparency and engender greater understanding of programmes and policies. The development of a common and comprehensive monitoring and evaluation framework that provides clear indicators is vital to measure success.

Such a framework is further considered crucial to ensure the legitimacy and efficacy of actions taken to prevent and counter violent extremism and terrorism online. Continuous monitoring and evaluation of both content- and communications-based policies and collaborative programmes further allows for ongoing refinements, eventually increasing the impact of those measures.

However, research has shown that monitoring and evaluation of these programmes and policies is complex. Therefore, Governments are encouraged to draw analogies, where possible and appropriate, to existing monitoring and evaluation frameworks from other sectors, such as gang prevention, local community engagement, or limiting child sexual exploitation online.

In general, Governments are encouraged to develop – in cooperation with the ICT industry, civil society organizations, and academic institutions – indicators that are realistic and feasible to measure the success of a certain policy or programme aimed at preventing and countering violent extremism, while protecting human rights, such as the right to freedom of expression, as enshrined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[14] Those indicators should contribute to the evaluation of the goals and objectives set out in the relevant strategy. Governments are also encouraged to continually share best practices and information about national evaluation programmes and policies to facilitate sustainable cooperation.

Good Practice 5: To strengthen international cooperation as a key component to effectively preventing and countering violent extremism and terrorism online.

International cooperation is indispensable to preventing and countering violent extremism and terrorism online, as the Internet is inherently transnational. Concerted and coordinated efforts between Governments expand knowledge and understanding of the challenges posed by violent extremism and terrorism on the Internet and social media platforms.[15]

[14] As UN Security Council Resolution 2354 (2017) notes, the right to freedom of expression is reflected in Article 19 of the Universal Declaration of Human Rights adopted by the General Assembly in 1948 (UDHR), and in Article 19 of the International Covenant on Civil and Political Rights adopted by the General Assembly in 1966 (ICCPR) and stresses that any restrictions thereon shall only be such as are provided by law and are necessary on the grounds set out in paragraph 3 of Article 19 of the ICCPR.

[15] Examples of such an exchange and deepening of the collective understanding of the challenges posed by violent extremism on the Internet were the Special Meeting of the UN Counter-Terrorism Committee (CTC) with Member States and relevant international and regional organizations, civil society organizations, and the private sector on "Preventing the Exploitation of Information and Communications Technologies for Terrorist purposes, while Respecting Human Rights and Fundamental Freedoms" in New York in 2016 and the GCTF Second Symposium on Preventing and Countering Terrorists' Use of the Internet in Beijing in 2016.

International cooperation facilitates capacity building through the sharing of good practices which contributes to ensuring that national responses to limit the impact of and counter violent extremist and terrorist propaganda – both online and offline – are complementary and sustainable. International forums can facilitate in-depth discussions on creating synergies within the international community to maximise collective efforts and to pool expertise on preventing and countering violent extremism and terrorism on the Internet and social media platforms. Additionally, such forums can create an environment of mutual trust, contribute to the building of platforms for enhanced communication, and ensure the efficient and effective application of resources.

Furthermore, Governments are encouraged to strengthen mutual legal assistance, to participate in regional cooperation platforms and to develop and enhance arrangements for prompt cross-regional cooperation.[16] In particular, international and regional organizations can play an important role in capacity building efforts in digital evidence exploitation to enhance investigations.[17] INTERPOL's I-24/7 secure global police communications system, e.g., enables the exchange of operational information in support of criminal investigations.

Good Practice 6: To adopt a multi-stakeholder approach between Governments, the ICT industry and civil society organizations in preventing and countering violent extremism and terrorism online.

Given the transnational characteristics of the Internet, preventing and countering violent extremism and terrorism online can only be achieved through effective collaboration between Governments, the ICT industry, and relevant civil society organizations. Such a multi-stakeholder approach that combines political, technical, and contextual expertise is beneficial for both content- and communications-based responses.[18] An open dialogue among the respective stakeholders is crucial to pursue efficient and sustainable cooperation based on shared responsibilities between States, ICT industry and civil society organizations to prevent and counter violent extremism and terrorism

A multi-stakeholder approach is most likely to be effective when relevant stakeholders have a common understanding regarding each other's roles and responsibilities, as well as each other's strengths and limitations in responding to violent extremism online. In that respect, Governments can play an important role in engaging with ICT industry to counter violent extremism and terrorism online on a voluntary and collaborative basis, and in assisting relevant stakeholders, including by creating online and offline platforms for collaboration. Those platforms can foster a more inclusive process, open communication channels, build capacity, defuse conflicts of interest and identify critical gaps. Such coordinated efforts further prevent duplications, ensure complementary actions, and streamline multi-stakeholder initiatives, for instance in the form of public-private partnerships. Governments are also encouraged to support and take part in industry-led efforts.[19]

---

[16] UN Security Council Resolution 2322 (2016), para. 13 (h).

[17] UN Security Council, Letter dated 26 April 2017 from the Chair of the Security Council Committee established pursuant to Resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council (S/2017/375), para. 5.

[18] An example is the UN-CTED/ICT4Peace-initiative that focuses on deepening the understanding of private industries' responses to the terrorist use of their products and services and related challenges and to promote self-regulation and sharing good practices across the ICT industry, www.techagainstterrorism.org.

[19] A good example of such an effort is the *Global Internet Forum to Counter Terrorism,* an industry-led forum announced in June 2017 by Microsoft, Twitter, Facebook and Google, which has been designed to accelerate and strengthen collaboration on issues around content- and communications-based responses and collaborate with civil society organizations, governments, and regional and international organizations https://newsroom.fb.com/news/2017/06/global-internet-forum-to-counter-terrorism.

The ICT industry has technical expertise, access, and resources that could be leveraged to successfully implement measures aimed at preventing and countering violent extremism online. For instance, ICT companies have the technical expertise to develop tools and mechanisms (both human and automated) to counter the narratives of violent extremist and terrorist groups and to find solutions to rapidly identify and remove violent extremist and terrorist content from the Internet. Civil society organizations, which are often deeply rooted within local communities and therefore more likely to be credible among key audiences, are well-placed to support building effective and sustainable local community-level responses.

II. Good Practices for Content-based Responses

Good Practice 7: To adopt laws, regulations, and policies that address the availability and accessibility of violent extremist and terrorist content on the Internet.

The right to freedom of expression is a pillar of the international human rights law framework. At the same time, it may be limited under the specific circumstances outlined in Article 19 (3) of the ICCPR.[20] The exceptions may include the case of incitement to commit a terrorist act or acts.[21] Importantly, any restriction on the right to freedom of expression must be consistent with States' obligations under international law, including human rights law, and relevant national law.

Governments can legitimately limit the right to freedom of expression in the specific circumstances that a restriction is provided by law and necessary for respect of the rights or reputations of others or the protection of national security or of public order *(ordre public),* and proportionate.[22] Violent extremism and terrorism online can pose a threat to national security and/or public order, and in some cases may be restricted, provided that it is proscribed by law and necessary on the grounds set out in Article 19 (3) ICCPR. In that respect, Governments are encouraged to clearly define relevant offences in their respective national legislation, allowing individuals to foresee and anticipate the consequences arising out of their actions.

At the same time, communications that are morally repugnant, shock, disturb, or offend generally do not rise to a criminal level. One of the most effective means to address such expression is through open and pluralistic debate that engages with these ideas and opinions in a respectful manner and promotes intercultural understanding. Challenging these ideas through more debate that gives a voice to members of all communities contributes to revealing the falsehood and fallacies attached to them.

[20] Also relevant in this context is Article 20 ICCPR which addresses propaganda for war and any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. In that regard, Human Rights Committee General Comment No. 34 notes that Articles 19 and 20 ICCPR are compatible with and complement each other. The acts that are addressed in Article 20 ICCPR are all subject to restriction pursuant to Article 19 (3) ICCPR. In every case in which a State restricts freedom of expression it is necessary to justify the prohibitions and their provisions in strict conformity with Article 19 (CCPR/HRC/GC/34, 12 September 2011, paras 50f.).

[21] Cf. also UN Security Council Resolutions 2354 (2017) and 1624 (2005) which condemn the incitement of terrorist acts and repudiate attempts at the justification or glorification (*apologie*) of terrorist acts that may incite further terrorist acts. UN Security Council Resolution 1624 (2005) operative para. 1 (a) calls upon all States to adopt such measures as may be necessary and appropriate and in accordance with their obligations under international law to prohibit by law incitement to commit a terrorist act or acts.

[22] Article 19 (3) ICCPR; Article 19 UDHR; see Human Rights Committee, General Comment No. 34 on the Freedom of opinion and expression, CCPR/C/GC/34, 12 September 2011, paras. 21-36.

A further right which must be carefully balanced in addressing violent extremist and terrorist content on the Internet, is the right to not be subjected to arbitrary or unlawful interference with one's privacy, as enshrined in Article 12 UDHR and Article 17 ICCPR. It is recalled that an individual's privacy must be protected against unlawful or arbitrary interference.[23]

Good Practice 8: To take into account any applicable existing international standards and/or principles when addressing the availability and accessibility of violent extremist and terrorist content on the Internet and social media platforms.

There are a number of existing documents recommending international standards and/or principles for complying with obligations under international law that may be taken into account by Governments – and/or by the ICT industry – when addressing violent extremist and terrorist content on the Internet.
These documents may include, but are not limited to, the UN Human Rights Council Resolution 16/18 (Combating intolerance, negative stereotyping and stigmatization of, and discrimination, incitement to violence and violence against, persons based on religion or belief),[24] the Rabat Plan of Action on the prohibition of advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility or violence,[25] the Article 19 Camden Principles on Freedom of Expression and Equality,[26] or the Global Network Initiative policy brief on extremist content and the ICT sector,[27] and may offer, as appropriate and necessary, practical guidance. The Camden Principles offer general guidance on how to implement the right to freedom of expression in compliance with States' obligations under international human rights law; and the Global Network Initiative policy brief provides a set of practical recommendations for Governments and the ICT industry in respect to preventing violent extremism and terrorism on the Internet.

Good Practice 9: To develop effective collaboration, where appropriate, and promote stronger engagement by the ICT industry as well as cooperation with civil society organizations when addressing violent extremist and terrorist content on the Internet and social media platforms.

Taking into account the important role of the ICT industry in providing tools, services and infrastructure necessary for online communications, continued engagement between Governments and the ICT industry is crucial to effectively and efficiently address the availability and accessibility of violent extremist and terrorist content on the Internet and social media platforms. Such collaboration can take various forms and its implementation depends upon the national context. In some jurisdictions, mechanisms have been introduced that bring public and private sector actors together

---

[23] UN General Assembly, OHCHR, Report on best practices and lessons learned on how protecting and promoting human rights can contribute to preventing and countering violent extremism (A/HRC/33/29), 21 July 2016, pp. 15f., available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/162/55/PDF/G1616255.pdf?OpenElement.

[24] UN Human Rights Council, Combating intolerance, negative stereotyping and stigmatization of, and discrimination, incitement to violence and violence against, persons based on religion or belief (A/HRC/RES/16/18), 12 April 2011, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/16session/A.HRC.RES.16.18_en.pdf.

[25] UN General Assembly, Annual report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of incitement to national, racial or religious hatred (A/HRC/22/7/Add.4), 11 January 2013, available at http://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf.

[26] Article 19, The Camden Principles on Freedom of Expression and Equality, April 2009, available at http://www.refworld.org/docid/4b5826fd2.html.

[27] Global Network Initiative Policy Brief, Extremist Content and the ICT Sector, November 2016, available at https://www.globalnetworkinitiative.org/sites/default/files/Extremist-Content-and-ICT-Sector.pdf.

to reduce the accessibility of violent extremist and terrorist content online, including by blocking, filtering or removing such content. In some countries, relevant authorities identify online terrorist content and inform companies of the potential abuse of their platforms. In some countries, national authorities cannot require the removal of content, on the basis that doing so would constitute a violation of their obligations under international law, including international human rights law, and national law.

It is recommended that Governments take into account existing multi-stakeholder initiatives and learn from those experiences when framing the specific terms of collaboration. To strengthen collaboration between Governments and the ICT industry, so-called Internet Referral Units (IRUs) that serve as a focal point for voluntary coordination and collaboration between different governmental agencies and the ICT industry are one possible approach for pursuing this good practice.[28] One of the main tasks of such a unit is to identify violent extremist and terrorist content on the Internet, which is undertaken in compliance with States' obligations under international and national law, and subsequently refer the respective content to the relevant ICT company to assess it in accordance with its own terms of service. Importantly, such a referral activity does not constitute an enforceable act. The decision regarding the removal of referred online content remains with the private ICT company and in accordance with the company's terms and conditions, unless otherwise decided under national law. Such a unit may further serve as a platform that facilitates information exchange through ensuring regular meetings amongst national partners and the relevant ICT company. This can be particularly important in preventing compromising or interfering with ongoing intelligence investigations or criminal investigations/prosecution of individuals or groups.

Collaboration with civil society organizations is encouraged in order to assist in the identification and flagging process of violent extremist and terrorism content on the Internet akin to the approach taken in combating child sexual abuse material online.[29] Such collaboration may involve law enforcement agencies, the ICT industry and a civil society organization with expertise in preventing and countering violent extremism and terrorism. Civil society organizations, if so inclined, could voluntarily and proactively search for violent extremist and terrorist content and could provide a platform for the public to report such content anonymously. Civil society organizations could choose to include and/or work with teams of specifically trained personnel to assess reported online content and work closely with public and private stakeholders, as appropriate, to flag relevant content to ICT companies for review of violations of their terms of service and/or follow procedures to report content, as appropriate, to law enforcement agencies. Civil society organizations, if so inclined, could further track whether referred content remains online or not.

Good Practice 10: To provide reference to the pertinent laws and regulations that motivate such referrals of relevant content to the ICT industry.

Governments are encouraged to provide reference to the pertinent laws and regulations that motivate such referrals of relevant content to the respective ICT company when referring violent extremist and terrorist content or when requesting the removal, filtering or blocking of such content. This openness in decision-making and execution processes would strengthen trust in and between the respective stakeholders, and consequently, would also promote greater transparency. In that respect, Governments are encouraged to make pertinent laws and regulations that constitute the national legal basis for addressing violent extremist content accessible to the public and inform the ICT industry of the competent authorities that are authorised to address violent extremist content and to make such referrals.

[28] Such so-called Internet Referral Units (IRUs) exist, for instance, in the European Union, the Netherlands and the United Kingdom.

[29] In that regard, an analogy is drawn with the detection of child sexual abuse material online and the work of the Internet Watch Foundation.

In order to strengthen openness and consequently oversight, it is further recommended that Internet referrals units and the ICT industry continue to publish periodic reports, indicating the number of total referrals and removals made.

Good Practice 11: To acknowledge the role of the ICT industry in effectively addressing the availability and accessibility of violent extremist and terrorist content on the Internet and social media platforms.

With regards to addressing the availability and accessibility of violent extremist and terrorist content online, the important role of the ICT industry could be understood as deriving from their control over the actual online communication platforms. The ICT industry should be mindful of its users' reasonable expectations regarding the treatment of online content. As such, terms of service are well-suited to reflect those expectations.

However, not all online communication service providers follow the same standards and guidelines with regards to the formulation and enforcement of their terms of service, though generally terrorism, violent extremism and incitement to violence, are all banned from these platforms.[30] Therefore, the ICT industry should be encouraged to collaboratively and voluntarily develop consistent community guidelines with regard to preventing and countering violent extremism and terrorism online.[31] In this context, the ICT industry is further encouraged to review and adapt their terms of service to reflect relevant legislation and regulation, as and where appropriate. In that respect, the ICT industry's responsibility to respect human rights, as set out in the UN Guiding Principles on Business and Human Rights, is recalled and it is recommended that terms of service are developed with a view to respecting human rights, which may include avoiding overly restrictive community guidelines that could have a chilling-effect on the full enjoyment of users' human rights, in particular the right to freedom of expression and the right to hold opinions without interference.[32]

In order to implement the terms of service with regard to addressing online content, the ICT industry, and in particular online communication service providers should enforce their terms of service effectively. The ICT companies should ensure their terms of service cover terrorist content and remove, block, filter, or otherwise address any content that violates their terms of service within a reasonable timeframe. In that respect, many ICT companies allow their users to flag content that violates their terms of service. The ICT industry thus has to be mindful of possible unintended consequences the application of the respective terms of service could carry, e.g. on the potential impact on human rights of its users, the possibility of compromising ongoing criminal investigations, as well as reinforcing perceived grievances and the conception of a exclusionary "us versus them" world-view that may indirectly serve violent extremists' and terrorists' purposes.

---

[30] In that regard, it is considered problematic that certain ICT companies refer to different sanctions lists. E.g., some refer to the UN Security Council Consolidated Sanction List, whereas others refer only to a State's list of terrorist organizations and/or groups. Therefore, Governments are encouraged to raise awareness regarding internationally considered terrorist organizations and/or groups among the relevant stakeholders, in particular among the ICT industry.

[31] The Knowledge Sharing Platform developed by the UN-CTED/ICT4Peace project will collect existing and model terms of service that could be used by companies, available at http:///www.techagainstterrorism.org.

[32] E.g., see European Commission, ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, available at https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf.

Good Practice 12: To monitor and evaluate the application of automated processes that are employed to limit the re-dissemination of existing and/or already identified violent extremist and terrorist content Online.

Automated processes can be an effective and efficient means to address the vast scale of the online environment and the speed at which content can be disseminated. A number of automated processes are employed commercially, as well as in other areas of online criminality or harms, including child sexual abuse imagery and copyright infringement, to augment human review processes and accelerate the identification of online content.

Automation can be employed in a number of areas to assist in addressing the re-dissemination of existing and/or already identified violent extremist or terrorist content online by accelerating its removal. E.g., efforts such as the "hash-sharing" database launched by the ICT industry to help identify duplicates of human-reviewed and removed content and prevent its reappearance on other online platforms, can contribute to preventing the further dissemination of existing and already identified violent extremist content.[33]

Governments are encouraged to support the voluntary efforts of private companies to carefully and continuously monitor and evaluate their use of automated processes to assess effectiveness and accuracy thereof, including ensuring that they do not generate misleading or inaccurate results. Given the rapid technological advances in this area, the introduction of new automated processes should be carefully scrutinised to ensure that they do not cause unintended consequences or contravene the right to freedom of expression. To this end, exchanges between ICT industry and Governments on the issue of compatibility between automated removal and right to freedom of expression should be encouraged.

III. Good Practices for Communications-based Responses

Good Practice 13: To address all aspects of violent extremism and terrorism by tailoring online interventions to take into account a spectrum of communications responses, including preventative programmes and counter-narrative campaigns.

In order to fully address the range of violent extremist and terrorist content available online, a wide array of communications responses are needed, including preventative educational or positive narrative campaigns aimed at broad audiences, counter-narrative campaigns targeted at more specific at-risk audiences, and online individualised interventions for those participating in violent extremist and terrorist communities online. The safety of the individuals carrying out these activities should be of paramount importance to Government efforts. It is also crucial that Governments effectively communicate their national security policies in the sphere of preventing and countering violent extremism and terrorism and that online communications supplement offline messaging and activities in these areas.

Governments could consider developing their own proactive and positive narratives that not only aim to directly combat or refute violent extremist and terrorist narratives, but also serve to build a strong sense of identity and belonging and encourage civic engagement, inclusiveness and responsibility, and therefore engender resilience within their societies. Such campaigns should strive to provide credible alternatives and address issues of concern to vulnerable audiences who are subject to violent extremist and terrorist narratives. Digital literacy and digital citizenship classes can be integrated into education programmes to address either identified or underlying vulnerabilities in this context. These

[33] European Commission – Press release, EU Internet Forum: a major step forward in curbing terrorist content on the internet, 8 December 2016, available at http://europa.eu/rapid/press-release_IP-16-4328_en.htm.

programmes are often most effective when developed and delivered in partnership with civil society organizations. It is important that these types of campaigns are transparent with regard to their origin or funding and realistic in order to avoid exacerbating grievances that violent extremist and terrorist groups often exploit, and that online and offline messaging campaigns are complementary.

However, for a variety of reasons there can be limits to the effectiveness of Governments directly delivering campaigns to counter online violent extremist and terrorist content. Governments are encouraged to also work alongside the ICT industry and relevant civil society organizations, on a voluntary basis, to support and empower credible voices to ensure they are heard online, and provide both positive alternative messages and online engagement with individuals expressing violent extremist views online. Finally, civil society organizations can contribute research and analysis on both the threat and the impact of responses.

Good Practice 14: To encourage voluntary collaboration to produce authentic and innovative communications-based approaches to the challenge of violent extremist and terrorist content online by convening the ICT industry, civil society organizations and other actors.

Governments could encourage the ICT industry, to be as proactive as possible in countering violent extremism and terrorism on their platforms in order to better protect their users by supporting innovative communications-based approaches on a voluntary basis. Voluntary collaboration with major ICT industry companies can help to achieve the reach and impact required to effectively and sustainably counter the threat posed by violent extremist and terrorist communications online.

A multi-stakeholder approach presupposes a wider range of actors from the ICT industry, civil society organizations and other areas acting in accordance with their respective roles in these efforts. From the ICT industry, smaller platforms have an important role to play, alongside experts in analytics, communications, advertising, marketing and content production. Researchers, academics and practitioners can provide insights into violent extremist and terrorist communications and inform potential responses, while a range of civil society organizations can provide authentic, credible voices (including youth, women, community and faith groups, former (violent) extremists and terrorists or survivors of extremist and terrorist violence, or popular public figures) and ensure communications-based responses take into account the gender dimension and address specific concerns and vulnerabilities of both men and women.

These collaborations serve to pool creativity, expertise and resources and encourage the development of sustainable campaigns and effective means of delivery and evaluation. Some examples of these innovative approaches have been digital literacy workshops, content creation labs for youth, interactive ‘hackathons’ and the production of dedicated media platforms for civil society groups.

Good Practice 15: To ensure campaigns have a distinct target audience (or audiences), a specific goal (e.g., to decrease the risk of radicalization to violence or promote peaceful alternatives to violent narratives) and provide tightly focused, distinct, and context-specific messages. Analysis of specific audience(s) can enable the identification of suitable messengers that are credible to the relevant target audience(s).

Campaign success often relies upon an understanding of the best platforms and tactics with which to reach the target audience. This can be achieved with a range of social listening and social media analysis software, which are designed to help communications teams identify messengers and produce content relevant for specific target audiences. These activities should be undertaken with consideration for the legal context in which a campaign takes place, including data protection laws.

These tools are particularly useful for undertaking an audience segmentation exercise as part of the initial scoping phase of the campaign. This is often informative regarding the type of content and narratives that will likely resonate, and it can help to identify both the messengers and platforms that would be most effective for delivery. Where possible, a cross-section of the target audience should also be consulted during this stage to review and provide feedback on the proposed content. Depending on the focus of the campaign, this could include, e.g., youth, women, faith leaders or former (violent) extremists and terrorists.

Once the campaign strategy has been established and content has begun to be disseminated, the performance of the campaign can also be tracked using social media analysis software. This can provide insight into how the content is being received across different geographies and demographics. This begins an iterative process throughout which the campaign can be optimised and re-deployed.

Good Practice 16: To ensure all campaigns are centred on an overall goal, which may be as simple as promoting dialogue and engagement; a realistic set of measurable objectives; and a robust evaluation methodology to determine impact on target audiences.

Setting an overall long-term goal and a related series of more immediate objectives, before both the design and the dissemination stages of a campaign, provides a series of benchmarks against which to measure its impact on the intended target audience. Objectives should therefore be clearly defined, quantifiable measures of a desired effect. They should be measurable, allowing campaigners to discern from available metrics and indicators whether or not they were achieved, and realistic with respect to the resources available, as well as the performance of previous campaigns.

As well as setting clear goals and objectives, all campaigns should be developed based on a definitive "theory of change" that outlines: how the campaign will meet the objectives set; how the desired impact on the intended target audience will be achieved; and provides indicators to evaluate whether the overall long-term goals were accomplished. The development of goals, objectives and the theory of change should, where possible, be informed by a data-driven approach.

The continuous monitoring and evaluation of communications-based campaigns enables an iterative process of optimizing the content or channels and increasing the reach, engagement and impact of those measures. Governments can assist in funding innovative data gathering, analysis and research methods, and invest in building a common monitoring and evaluation framework. This will improve understandings of the long-term impact of communications responses online and allow future responses to be adapted accordingly.

Good Practice 17: To be aware of and take steps to mitigate against the possible risks involved in the strategy and delivery of communications campaigns.

Communications-based responses inevitably deal with sensitive subject matter and can put audiences and campaigners at-risk, potentially exposing participants to online abuse or physical harm. The specific security risks a campaign must consider vary depending on the type of campaign, as well as factors such as the contexts in which it is delivered. This includes the security risk that may be posed to civil society organizations and the ICT industry involved in the delivery of campaigns. However, these risks can be effectively mitigated through careful planning and implementation.

Beyond the security challenges related to communications-based responses, there are other types of risk that should be considered. Campaigns can have a range of complex impacts, not all of which will necessarily be positive. E.g., serving unintended audiences with a message designed for another specific group could cause offense, generate feelings of alienation or even confirm existing negative

views. Monitoring and evaluation activities may also carry potential risks to a campaign, e.g. through the inadvertent publication of identifiable user data. It is therefore important to give consideration to the legal context in which a campaign takes place, including data protection laws. Finally, although many communications-based responses do not seek engagements with individuals who are at-risk of falling into violent extremism and terrorism, or who are currently members of violent extremist and terrorist groups, all campaigns should have pre-determined guidelines in place for interactions with such individuals.