SEPTEMBER 2022

TOOLKIT ON RACIALLY OR ETHNICALLY MOTIVATED VIOLENT EXTREMISM (REMVE)[1]

GCTF "RACIALLY OR ETHNICALLY MOTIVATED VIOLENT EXTREMISM" TOOLKIT INITIATIVE

GCTF
GLOBAL COUNTERTERRORISM FORUM

Table of Contents

Section I: Introduction

Racially or ethnically motivated violent extremism (REMVE)[1] and its actors, groups, and movements pose a multilayered and transnational threat, constantly evolving and transcending borders. In recent years, REMVE actors have carried out widely publicized violent attacks motivated by a broad variety of social, economic, and/or political grievances, or in the name of defending against perceived threats to their racial or ethnic identity.[2] REMVE networks, operations, and ideologies have become increasingly transnational, and increasingly concerning at international, regional, and national levels. Actors and groups form connections, both online and offline, where they share tactics, membership, propaganda, and ideology, and engage in cross-border fundraising and other financial transactions. Preventing, deterring, disrupting, counteracting, and prosecuting REMVE threats pose unique challenges for States, some of which may lack the legal, operational, and policy frameworks or have not comprehensively prioritized addressing REMVE threats.[3]

As a response to the complex challenges posed by REMVE, the United States and Norway partnered under the auspices of the Global Counterterrorism Forum (GCTF) to launch the "Racially or Ethnically Motivated Violent Extremism" Toolkit Initiative. This Initiative aims to strengthen the abilities of GCTF Members and additional stakeholders, including GCTF non-member States, civil society organizations, and the private sector, to develop and implement counter-REMVE strategies, policies, and programs that reflect relevant GCTF good practices and respect relevant domestic and international law. The REMVE Initiative Toolkit (hereinafter referred to as *the Toolkit*) aims to provide practical guidance and strategies to prevent, deter, disrupt, counteract, respond to, and prosecute REMVE threats. This Toolkit builds upon existing GCTF Framework Documents, such as:

- *Ankara Memorandum on Good Practices for a Multi-Sectoral Approach to Countering Violent Extremism;*
- *Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online;*
- *Rome Memorandum on Good Practices for Rehabilitation and Reintegration of Violent Extremist Offenders; and*

[1] GCTF Members and experts use a number of different expressions to describe REMVE and interrelated threats. These include "racially or ethnically motivated terrorism," "ideologically motivated violent extremism," "right-wing terrorism," "far-right terrorism," "extreme-right terrorism," "violent right-wing extremism," and "white supremacist terrorism," "terrorism on the basis of xenophobia," and "terrorism in the name of religion or belief," among others. At the international level, "violent incidents often underpinned by racial, ethnic, political, and ideological motivations" have been expressly outlined as aspects of "terrorist attacks on the basis of xenophobia, racism and other forms of intolerance, or in the name of religion or belief" (XRIRB). Despite differences in terminology, each of these expressions describes attacks perpetrated by individuals or groups in the name of defending against perceived threats to their racial or ethnic identity or ensuring the superiority/supremacy thereof.

[2] Examples of such REMVE attacks include the 2019 Christchurch shootings perpetrated by Brenton Tarrant and the 2011 attacks in Oslo and Utøya island committed by Anders Breivik. Both attacks resulted in a significant number of casualties and fatalities.

[3] See for example the GCTF's *Memorandum on Good Practices on Strengthening National-Local Cooperation in Preventing and Countering Violent Extremism Conducive to Terrorism,* full text available at https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2020/GCTF%20Memorandum%20on%20Good%20Practices%20on%20Strengthening%20NLC%20in%20PCVE.pdf?ver=2020-09-29-100315-357 *Memorandum on Good Practices on Strengthening National-Local Cooperation in Preventing and Countering Violent Extremism Conducive to Terrorism* on "uneven political will" as a policy challenge to national-local cooperation on P/CVE.

- *Addendum to the Rome Memorandum on Good Practices for Rehabilitation and Reintegration of Violent Extremist Offenders;*
- *Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context;*
- *Rabat – Washington Good Practices on the Prevention, Detection, Intervention and Response to Homegrown Terrorism;*
- *Good Practices on Women and Countering Violent Extremism; and*
- *Addendum to the GCTF Good Practices on Women and Countering Violent Extremism with a Focus on Mainstreaming Gender*.[4]

The Toolkit also builds upon the April 2021 GCTF REMVE-focused exploratory dialogues, and utilizes the International Institute for Justice and the Rule of Law (IIJ) Criminal Justice Practitioner's Guide on Addressing Racially or Ethnically Motivated Violent Extremism.

The United States and Norway presented the REMVE Initiative for endorsement at the Nineteenth GCTF Coordinating Committee Meeting held virtually on 6 October 2021 and held two virtual exploratory preparatory meetings in November and December 2021, followed by a formal digital launch in February 2022. The Initiative virtually convened two iterations of its workshop in March 2022, drawing wide representation from GCTF Members, non-member States, academia, civil society, policymakers and practitioners, information and communications technology (ICT) companies, and international and regional organizations. The workshop featured a tabletop exercise with fictional scenarios designed to facilitate REMVE-specific discussions on prevention, criminal prosecution, terrorist financing, and resilience building. The structure and focus of the tabletop exercise enabled inclusive and democratic engagement, with all participants having the opportunity to contribute to and shape the discussions around the fictional scenarios. The workshop generated and facilitated the elaboration of good practices and recommendations related to preventing, deterring, disrupting, counteracting, and prosecuting REMVE actors and groups with reference to the legal, policy, and operational challenges posed by the REMVE threat.

The Toolkit is the culmination of this consultation process. This Toolkit is a non-binding document intended as a resource for policymakers and practitioners, civil society, and other subject matter experts (SMEs) and stakeholders confronting the policy, operational, and legal challenges of designing, implementing, communicating, and managing measures to prevent and respond to the threat of REMVE. The good practices and recommendations put forth by the workshop participants, in addition to the themes identified at the launch event and the preparatory meetings, comprise the substance of this Toolkit. These non-binding recommendations should be considered and implemented in line with each State's specific circumstances, including resources and capabilities, existing domestic laws and policies, and their international legal obligations and commitments, including international and regional human rights obligations. The purpose of the Toolkit is to provide stakeholders with concrete

[4] On the topic of women and gender in violent extremism, see also United Nations Security Council Resolution (UNSCR) 2178 (2014), UNSCR 2242 (2015), the 2016 UN Secretary-General's Plan of Action to Prevent Violent Extremism, UNSCR 2395 (2017), UNSCR 2395 (2017), and the UN Global Counter-Terrorism Strategy (2018).

recommendations toward the development and operationalization of whole-of-government and whole-of-society strategies and programs to counter REMVE as well as to enhance appropriate international cooperation on REMVE issues. This Toolkit is also intended to address gaps in the international community's understanding of REMVE threats, including targeted recommendations and practical guidance to complement existing resources.

The Toolkit is thus designed to be a resource both for States without REMVE-specific legislative provisions and/or policies as well as for States which may already have explicitly REMVE-focused or REMVE-applicable statutes, strategies, and programs. This Toolkit is organized as follows: Section II provides an overview of the REMVE landscape, including defining the concepts, challenges, and the terrain, as well as situating the REMVE challenge within the broader framework of international legal norms and applicable human rights obligations. Section III examines the effective development, implementation, and coordination of strategies to counter REMVE. Section IV reflects on how to foster multi-stakeholder cooperation and resilience and capacity building. Section V focuses on the importance of international cooperation and multi-stakeholder coordination and integrating regional and local counter-REMVE programs into national strategies.

Section II: REMVE Overview

A. Defining the concepts, challenges, and the terrain/gaps

The definition of REMVE varies among States and international entities, with many States using different terminology to define this form of violent extremism conducive to terrorism. While some countries use the term "racially or ethnically motivated violent extremism," others use terminologies that may have political connotations, such as "far-right extremism," "violent right-wing extremism," or "ideologically-motivated violent extremism." In sum, the existing terminology is meant to describe violent extremism conducive to terrorism or terrorism perpetrated by individuals or groups who promote and/or conduct violence in the name of defending against perceived threats to their racial, ethnic, and national identities, and/or ensuring the superiority/supremacy of their racial, ethnic, or national identities. REMVE actors and groups derive their agendas from the perception of bias related to race or ethnic superiority against specific, minority populations and with various motivating factors as discussed in further sections. For the purposes of this Toolkit, REMVE will be approached with reference to this synthesized understanding.

1. Distinguishing REMVE

The existing definitional divergences – both in respect of REMVE and terrorism[5] – compound the challenge of distinguishing REMVE from other violent extremist conducive to terrorism or terrorist threats. A good starting point in addressing the REMVE definitional conundrum, and identifying where the boundaries of REMVE lie, is to concentrate on the beliefs and ideologies commonly understood to fit under the broad REMVE umbrella. One approach is to focus on the overlaps with categories of violence, the criteria for inclusion and exclusion in this categorization, and the definitions of violent extremist conducive to terrorism behavior that different countries have adopted. An alternative

[5] Although there are a number of internationally and regionally adopted Conventions aiming to address terrorism and terrorism-related activities, there is no universally agreed definition of "terrorism." A list of terrorism-related United Nations Conventions as well as relevant regional Conventions is available at: https://treaties.un.org/Pages/DB.aspx?path=DB/studies/page2_en.xml

approach is a thorough, critical assessment of the components of various extreme ideologies that radicalize to violence (e.g., racism, anti-Semitism, xenophobia,[6] etc.), and conspiracy theories (such as Eurabia and the "great replacement theory"[7]) and how these components both partially overlap and diverge in a REMVE context. Furthermore, the radicalization to violence modeling used with regard to other violent extremists might also require significant rethinking when applied to REMVE actors, as these models may not appropriately capture the process of REMVE radicalization to violence, due to the fluidity of REMVE ideologies and movements online and offline making it difficult to distinguish and identify individual REMVE actors.[8] The use of multi-stakeholder scenario-based discussions, tabletop exercises, and/or realistic simulations while assessing the threat of REMVE and how best to counter it could be a helpful tool for knowledge and skills exchange as well as in enhancing the design, development, monitoring, evaluation, and implementation of REMVE-specific radicalization-to-violence modeling and de-radicalization programming. Organizational structures could also differ in important ways when comparing REMVE with other violent extremists.

Due to the extensive range of motivating factors, disengaging a radicalized individual from violent extremist ideologies requires tailored solutions. At present, REMVE actors often operate with minimal top-down guidance from a group's leadership and without many formalized group affiliations. The result is more individualized activities or loosely organized associations among REMVE actors.[9] This individualization of solutions, coupled with the loose, amorphous nature of REMVE group leadership, can result in an overfocus on, or inaccurate application of theories related to leaderless resistance, or "lone actors" when trying to understand REMVE. For example, when assessing whether an individual is a "lone actor," it is important to consider the broader ecosystem that cultivated, encouraged, and/or supported them.[10] Such an examination can help identify underlying motivations and improve understanding of the mechanics of radicalization to REMVE violence online and/or offline.

The spread of information and ideologies—and the channels utilized to do so—have further impacts on distinguishing the nature of REMVE threats and movements. The use of technology, including online platforms, message boards, gaming platforms, and other online spaces and forums by violent extremist and terrorist actors has introduced a novel component to these existing definitional challenges. A good illustration is the increasing production and dissemination of a broad range of online content in the form of memeification, satire, irony, and other formats, which has blurred the distinction between content that complies and content that *does not* comply with the relevant

[6] Following the significant rise of violent incidents often underpinned by racial, ethnic, political, and ideological motivations, the UNODC has recently launched a manual to facilitate international legal cooperation on xenophobia, racism and other forms of intolerance, or in the name of religion or belief (XRIRB).

[7] Eurabia is a conspiracy theory based on the assumption that Europe will be completely taken over by Islamic and Middle Eastern forces. The "great replacement theory" suggests that over-welcoming immigration policies are intended to bring large influxes of non-white immigrants to dilute the political power of white people in Western countries.

[8] See further the GCTF "Racially or Ethnically Motivated Violent Extremism" (REMVE) Toolkit Initiative Exploratory Preparatory Deep-Dives with Subject Matter Experts, available at: https://www.thegctf.org/Portals/1/Documents/Links/Meetings/2022/REMVE%201-2%20and%209-10%20March/Deep%20Dives/DeepDiveSummariesGCTFREMVEInitiative.pdf?ver=05cqxSVJA_xqUcyNgPS8AA%3d%3d.

[9] This is in contrast to the 1990s and earlier decades during which REMVE activities were driven by more strictly organized groups such as skinhead street gangs. See further Jacob Aasland Ravndal et al, "RTV Trend Report 2021," *Center for Research on Extremism*, page 7, https://www.sv.uio.no/c-rex/english/publications/c-rex-reports/2021/rtv-trend-report/c-rex-rtv-trend-report-2021.pdf.

[10] Recent statistics indicate that while lone actors were responsible for most of the fatal violence committed in Western Europe, they are typically part of the extremist sub-cultures on the internet, or they are at the fringes of organized groups. While these individuals may act alone in respect of the planning or carrying out attacks, they are typically not isolated or without a loose support network. See further the GCTF "Racially or Ethnically Motivated Violent Extremism" (REMVE) Toolkit Initiative Exploratory Preparatory Deep-Dives with Subject Matter Experts, available at: https://www.thegctf.org/Portals/1/Documents/Links/Meetings/2022/REMVE%201-2%20and%209-10%20March/Deep%20Dives/DeepDiveSummariesGCTFREMVEInitiative.pdf?ver=05cqxSVJA_xqUcyNgPS8AA%3d%3d.

domestic, regional, and international legal provisions.[11] This blurring, in addition to the existing definitional divergences, can impact the efficiency of States' efforts to identify and counter REMVE within and across borders. For example, significant differences in or lack of domestic legal regimes applicable to REMVE materials and activities can cause delays in cross-border coordination of counter-REMVE messaging and measures both offline and online. The complex and distinct nature of the REMVE threat means that both national and cross-border preparedness are essential, responses should be tailored, and resources used judiciously. The lack of consensus terminology on REMVE as evidenced by the range of existing definitions at international and domestic levels can have severe consequences for the victims of REMVE as part of their efforts to seek compensation through the relevant civil and criminal justice processes.[12] It is thus important to establish and/or enhance national and international guidelines and mechanisms to assist and support victims of REMVE.[13]

2. Delineating the Challenges

The differences in definitions pose some challenges in distinguishing REMVE from other forms of violent extremism conducive to terrorism. Developing a shared understanding of what REMVE is and refining relevant legislative provisions and policies to keep pace with the rapidly evolving nature of REMVE are good starting points to prevent, deter, disrupt, counteract, and prosecute REMVE activities. Regular review of relevant laws, regulations, and policies will help support a more comprehensive understanding of the current REMVE threat landscape across legislative, policy, and operational responses. For example, many high-profile REMVE groups[14] are more focused on building out their international networks than committing mass-casualty attacks which would lead to their interdiction by police, intelligence, and security agencies. Such REMVE groups often serve as inspiration for unaffiliated lone actors who are willing to carry out one-off attacks or perpetrating attacks that are not explicitly directed by group leadership to accelerate chaos and political tension.[15] Enhanced designation, proscription, or banning legal and regulatory frameworks which take into

[11] The EU's Radicalization Awareness Network defines memes as: "Internet memes are graphics of visual and textual remixes shared and widely distributed online. They depict everyday situations and often express slapstick, which is difficult to express in words. With a general turn towards visual elements in communication, it is becoming increasingly impossible to ignore memes — especially in political contexts. As with every new technology, the far right has been quick to adapt to the new requirements of seizing the attention of broader audiences and to tailor white supremacism to the jargon of online communities…As inane as these pictures may seem, they are important as they offer a low threshold to interact with extremist ideas." See further "It's not funny anymore. Far-right extremists' use of humour," *Radicalization Awareness Network*, https://ec.europa.eu/home-affairs/system/files/2021-03/ran_ad-hoc_pap_fre_humor_20210215_en.pdf.

[12] For example, see the case of Tanya Gersh, a Montana real estate agent. Gersh secured a $14 million judgment against neo-Nazi website publisher Andrew Anglin, following an anti-Semitic campaign that Anglin whipped up against Gersh's family. However, Anglin has been able to successfully evade requests to disclose information about his assets and finances post-judgment and is now reportedly living outside of the United States, further complicating Gersh's efforts to obtain compensation. For more information, see Michael Kunzelman, " Neo-Nazi website founder accused of ignoring $14M judgment" *AP News*, https://apnews.com/article/technology-race-and-ethnicity-montana-courts-1554c9a9254449b75018cee56317c557. See also GCTF "Racially or Ethnically Motivated Violent Extremism" (REMVE) Launch Event Speakers List, available at: https://www.thegctf.org/Portals/1/Documents/Links/Meetings/2022/REMVE%203%20Feb/Speakers%20List/REMVE_Launch_SpeakersList_FIN.pdf?ver=8C-uBZigG_pbnfHb1Jk22w%3d%3d.

[13] See further the range of GCTF Initiatives on supporting victims of terrorism and in particular, the GCTF's *Madrid Memorandum on Good Practices for Assistance to Victims of Terrorism Immediately after the Attack and in Criminal Proceedings*, *Madrid Declaration on Victims of Terrorism* and *Plan of Action on Victims of Terrorism*. Other relevant GCTF Initiatives include the GCTF *Good Practices on Women and Countering Violent Extremism, the Addendum to the GCTF Good Practices on Women and Countering Violent Extremism, with a Focus on Mainstreaming Gender, the Hague Memorandum on Good Practices for the Judiciary in Adjudicating Terrorism Offenses* and the *Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector.*

[14] For example, the Atomwaffen Division and the Nordic Resistance Movement.

[15] For example, Conor Climo, a Las Vegas, Nevada resident, was found with bombmaking materials in his residence and was in communication with "individuals who identified with" Feuerkrieg Division (FKD), an Atomwaffen Division-inspired accelerationist white supremacist group. Climo was communicating with individuals who identified with FKD in relation to carrying out surveillance for potential plots and discussing attacks on Jewish and LGBTQ+ targets. For further information, see Daveed Gartenstein-Ross and Samuel Hodgson, "Skinheads, Saints, and (National) Socialists: An Overview of the Transnational White Supremacist Movement," *Foundation for the Defense of Democracies,* https://www.fdd.org/analysis/2021/06/14/skinheads-saints-and-national-socialists/.

consideration this particular *modus operandi* could be quite helpful in preventing, deterring, disrupting, counteracting, and prosecuting REMVE groups and not only individual actors. All such regimes need to be consistent with national and international law, while respecting international human rights and the rule of law.

There is dynamic fluidity among the narratives, causes, and drivers fueling REMVE. Broadly, these could be broken down into four broad groupings to allow for critical reflection and to permit the categorization of motivating behaviors and factors: xenophobic narratives, anti-government and anti-authority narratives, gender/gender identity and sexuality-based narratives, and other narratives (to include left-wing, climate change, and anti-technology narratives among others). At present, the xenophobia narrative can explain extensive elements about the motivations of various violent extremist movements. In the longer run, there is a need to better understand the intersections of anti-government sentiments, nationalism/xenophobia, discrimination,[16] and REMVE. With respect to the latter, gender and sexuality are already being manipulated in narratives for recruitment, radicalization to violence, and propaganda by REMVE actors.[17]

REMVE is also increasingly a cross-border or transnational phenomenon with an attack in one country sometimes inspiring a copycat attack in another country. In some cases, high-profile events can resonate across borders, having a significant transnational impact on REMVE actors.[18] With the broad range of online platforms and expanding possibilities to switch from one platform to another to avoid bans/blocks/sanctions, REMVE actors can more easily form and sustain cross-border and international networks through both virtual networks and international travel. As REMVE actors online use meme culture, irony and satire, or video games to spread their ideology[19] and radicalize to violence individuals of various ages, including children and youth,[20] there has been an increase in transnational digital subcultures, a challenge that should be taken into consideration when designing and implementing domestic and international counter-REMVE strategies and policies. REMVE actors have also exploited online platforms to fundraise for their activities, increasingly relying on crowdfunding and cryptocurrency. While online platforms pose novel challenges and exacerbate existing ones, it is

[16] Discrimination can occur on several grounds, including gender, class, disability, age, and sexual orientation, among others. It is important to note that not all of these discrimination characteristics are relevant to REMVE. While sexual orientation as a basis for discrimination tends to be prominent in REMVE ideologies, age and disability are less so. The United Nations defines discrimination as "any unfair treatment or arbitrary distinction based on a person's race, sex, religion, nationality, ethnic origin, sexual orientation, disability, age, language, social origin, or other status." See further "Prohibition of discrimination, harassment, including sexual harassment, and abuse of authority," available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N08/238/36/PDF/N0823836.pdf?OpenElement.

[17] For example, it was often assumed that women recruit other women and men recruit other men, yet research suggests that women disproportionately recruit men into these movements. Thus, further critical examination of the types of influence and impact that gender narratives can have upon potential recruits is needed. See further the GCTF "Racially or Ethnically Motivated Violent Extremism" (REMVE) Toolkit Initiative Exploratory Preparatory Deep-Dives with Subject Matter Experts, available at: https://www.thegctf.org/Portals/1/Documents/Links/Meetings/2022/REMVE%201-2%20and%209-10%20March/Deep%20Dives/DeepDiveSummariesGCTFREMVEInitiative.pdf?ver=05cqxSVJA_xqUcyNgPS8AA%3d%3d.

[18] "A Perfect Storm: Insurrection, Incitement, and The Violent Far-Right Movement," The Soufan Center,4 October, 2021 https://thesoufancenter.org/research/a-perfect-storm-insurrection-incitement-and-the-violent-far-right-movement/

[19] For examples, see Cathrine Thorleifsson, "Trends in international right-wing terrorism and tools for prevention," delivered at the GCTF "REMVE Toolkit Initiative Launch Event, available at: https://www.thegctf.org/Portals/1/Documents/Links/Meetings/2022/REMVE%203%20Feb/Presentations/GCTFREMVELaunch_Thorleifsson.pdf?ver=oqNASaXwnOOhyxEs4yGnGA%3d%3d. See also "It's not funny anymore. Far-right extremists' use of humour," *Radicalization Awareness Network*, https://ec.europa.eu/home-affairs/system/files/2021-03/ran_ad-hoc_pap_fre_humor_20210215_en.pdf.

[20] While there is no single, universal, standard definition for what constitutes "youth", the existing definitions make a distinction between children and youth. The United Nations Convention on the Rights of the Child defines a child as a person under the age of 18, whereas UN Security Council Resolution 2250 defines youth as people between 18 to 29 years of age. The UN itself defines youth as people aged 15 to 24 years. Thus, while there may be some age overlap based on the various definitions, these are two separate categories in principle. See further: *Youth, Peace and Security: A Programming Handbook*, https://www.un.org/peacebuilding/sites/www.un.org.peacebuilding/files/documents/yps_programming_handbook.pdf.

important that States include both online and offline components in counter-REMVE strategies and policies.

Addressing such a multi-layered and cross-border threat, especially given its evolving nature, requires a comprehensive, multi-stakeholder, and agile approach – or what can be described as a REMVE response cycle. Counter-REMVE policies and strategies should be rooted and operationalized as part of a whole-of-government and whole-of-society approach, and respect relevant domestic and international legal obligations, including applicable international human rights obligations. REMVE response cycles tend to have several common components: early prevention and detection bolster local and community resilience, timely response, and enhanced information sharing. Structured in these phases is the need for understanding of local and national conditions, and how communities can be empowered to help rehabilitate and reintegrate REMVE actors that disengage from a violent extremist path. The REMVE response cycle, as such, needs to integrate each of these components to create a true whole-of-government and whole-of-society approach to countering the threat and addressing relevant challenges.

B. International law including the human rights framework

Any legal and policy measures adopted domestically to prevent, deter, disrupt, and counteract REMVE, both online and offline, should comply with States' obligations under international law, including their obligations under international human rights law.[21] Efforts to address the threat of REMVE, including through the use of REMVE data in watchlists,[22] where appropriate, need to be consistent with the rights to freedom of expression and freedom of peaceful assembly and association, and the right to privacy among other domestic and international legal and human rights obligations, including non-discrimination. This may arise particularly in the context of online REMVE content and/or activity that might not always meet the thresholds required to constitute a criminal offense or to trigger an action such as removal or suspension by the relevant online platform. States may therefore need to consider the need to criminalize a broader range of REMVE activities online, and also provide clear guidelines/policies for the takedown of REMVE content, which incites or extols violence, with the requirement to appropriately respect an individual's right to freedom of expression and privacy.[23] Establishing, strengthening, and regularly updating the designation or proscription legal and regulatory frameworks that target the full spectra of online and offline REMVE actors and groups is important in this context. In turn, private actors may need to realign or adjust their platforms' terms of service to reflect both the need to remove REMVE content that could be instigating violence and to respect individual rights. In addition to the right to freedom of expression, consideration should also be given to the right to privacy as a whole and, in particular, not to be subjected to arbitrary or

[21] See further the International Covenant on Civil and Political Rights, the UN Global Counter-Terrorism Strategy Review (A/RES/70/291), para 42, 19 July 2016 as well as UN Security Council Resolutions 2354 (2017), 2178 (2014) and 1624 (2005).

[22] See further the UN Security Council Resolution Resolution 2396 (S/RES/2396 (2017), the *GCTF New York Memorandum on Good Practices for Interdicting Terrorist Travel*, the *GCTF Watchlisting Guidance Manual Initiative and the GCTF Counterterrorism Watchlisting Toolkit.*

[23] The *Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence* annexed to the Report of the United Nations High Commissioner for Human Rights on the respective expert workshops, sets out six factors which should be considered in determining when expression should be considered criminal and could be helpful in this context. UN Human Rights Council, *Annual report of the United Nations High Commissioner for Human Rights – Report on the expert workshops on the prohibition of incitement to national, racial or religious hatred* (A/HRC/22/17/Add.4), 11 January 2013. See further, the European Court of Human Rights, Factsheet – *Hate speech*, February 2022, pp. 20 – 25 in particular, and the Research Report by the Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, July 2020.

unlawful interference with one's privacy while addressing REMVE threats and challenges.[24] Thus, respect for States' international legal obligations should be integral to the design and implementation of counter-REMVE policies and programs and should shape the adoption of new, or the adjustment of existing, legislative provisions. The adoption of effective counter-REMVE measures and the protection of human rights should be seen as complementary and mutually reinforcing goals.[25]

As the following recommendations in this Toolkit suggest, policies and measures for the early prevention and countering of REMVE activities as well as building resilience to REMVE challenges may be implemented not only at State and local community levels, but also by private actors, such as ICT or technology companies and social media companies.[26] While States have the primary duty to protect against breaches of human rights in their territories or jurisdictions, many international instruments governing corporate responsibility now also recognize the role of third parties in promoting and respecting human rights.[27] For example, ICT companies including social media platforms have an increasingly important responsibility to ensure respect and protection for human rights and fundamental freedoms within their respective platforms and through their terms of use. The cooperation among States, international, regional, and sub-regional organizations, the private sector, and civil society, with respect to the increasing use of ICTs by REMVE actors and their supporters, should respect human rights and fundamental freedoms.[28]

Section III: Effective Development, Implementation, and Coordination of REMVE Strategies

Recommendation 1: Understanding the REMVE phenomenon.

The REMVE phenomenon poses a multi-layered set of challenges. To effectively counter REMVE, it is important for governments, policymakers, practitioners, and other stakeholders to gain a comprehensive understanding of the REMVE phenomenon in its various manifestations. As a starting point, the appropriate stakeholders should examine the impact that political polarization has on violent extremist milieus. For instance, divisive rhetoric used within the political sphere, especially relating to race, ethnicity, religion, gender identity, sexual orientation,[29] and/or immigration status

[24] 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.

[25] See further the *GCTF Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online* .

[26] It is relevant to note that the Global Network Initiative's *Policy Brief on Extremist Content and the ICT Sector* has made recommendations to governments as well as ICT companies that the reporting or commentary by journalists and media outlets on terrorist groups or acts of terrorism should not be restricted, and consequently, policies and legislation should make a distinction between speech intended to incite terrorist acts and speech which debates, discusses or reports on such acts. See also the Global Network Initiative, *Extremist Content and the ICT Sector, A Global Network Initiative Policy Brief*, 4 November 2016, and The Camden Principles on Freedom of Expression and Equality (Article 19 in particular).

[27] See further the *GCTF Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online* Annual Report of the Special Rapporteur to the Human Rights Council on online content regulation (A/HRC/38/35), 6 April 2018; UN Global Counter-Terrorism Strategy Review (A/RES/70/291), para 42, 19 July 2016.

[28] See further both the perambulatory clauses and core Pillars of The United Nations Global Counter-Terrorism Strategy: Seventh Review (A/RES/75/291), 2 July 2021.

[29] It is important to note that sexual orientation is a core element of REMVE ideology. In Norway, for example, for several years, the Police Security Services have highlighted that hatred of the LGBTQ+ community is central to REMVE groups' ideology. In addition, in June 2016 with Resolution 32/2, the UN Human Rights Council created the mandate of Independent Expert on protection against violence and discrimination based on sexual orientation and gender identity due to increasing acts of violence and discrimination against individuals because of their sexual orientation and gender identity. The mandate was renewed with Resolution 41/18. Further details on the mandate are available at https://www.ohchr.org/en/special-procedures/ie-sexual-orientation-and-gender-identity.

can be perceived as legitimizing REMVE ideologies and potentially driving the radicalization of some individuals to violence.[30] Many REMVE groups target government institutions and support instances of civil unrest.[31] A multi-stakeholder examination of how REMVE ideologies are fostered by divisions within domestic society, as well as how the restoration of trust in governmental institutions can support local to global efforts to prevent radicalization to REMVE, is needed. Furthermore, prevention and disengagement programs should be designed in a manner that facilitates a comprehensive understanding of the motivations of individuals radicalized to REMVE, and their potential connections to violent extremist groups. Finally, governments and civil society organizations need to liaise with victim communities that have been targeted by REMVE actors to better understand REMVE. These communities may have a more nuanced grasp of the particular threats facing them and, as such, this information can provide police, intelligence, security agencies, and institutions with a better insight into the REMVE landscape.

Recommendation 2: Understanding REMVE-motivated actors' coded language and other particular uses of information and communications technology (ICT) to advance their violent objectives.

In ways similar toother violent extremists or terrorists, REMVE actors use ICTs, such as internet products, including social media platforms/applications and cryptocurrencies, to further their violent objectives. Due to the constantly evolving ways in which existing ICTs are used, it is essential to have a holistic and forward-looking understanding of these technologies and how they are used for REMVE-related activities and messaging. This understanding is particularly important with respect to social media platforms with extensive public reach, which serve as sites of recruitment and radicalization to REMVE and facilitate the dissemination of REMVE materials that may be amplified and furthered by moving to other specialized and/or encrypted platforms. In addition, video games and gaming-adjacent platforms or functions, such as unmoderated chatrooms and live streaming services, can also be utilized by REMVE actors and groups. Video games and social media networks that utilize virtual reality may also pose novel challenges. It is very important to understand the constantly evolving language and imagery used to communicate REMVE ideology online, as codes, irony, humor, and "doublespeak" are often used, which allow such actors to avoid detection.[32] It is also important to recognize that while de-platforming or removing REMVE actors from online platforms may temporarily erect barriers to online recruitment, radicalization to violence, and mobilization to REMVE, this approach may feed into a recurrent REMVE censorship narrative of government overreach, which alleges that only certain voices are silenced by authorities.[33] As such, de-platforming

[30] For example, freedom of expression debates are ongoing regarding the rhetoric used by some anti-Islam groups in Europe and particularly Scandinavia, in relation to the latest Koran burnings of Rasmus Paludan in Sweden, and attempts by Sian (Stop the Islamification of Norway) in Norway.

[31] There is a crossover between REMVE groups and anti-government activities. Political assassinations and harassment of politicians and government officials as well as riots and insurgencies against governmental institutions, such as on the U.S. Capitol or the Reichstag in Berlin, have occurred with greater frequency. See: Tore Bjørgo, "Changes in Extreme Right Violence, Victims and Perpetrators: European Trends," available at: https://www.thegctf.org/Portals/1/Documents/Links/Meetings/2022/REMVE%201-2%20and%209-10%20March/PPTs/T.Bjorgo%20-%20GCTF%20REMVE%20WorkshopB.pdf?ver=2EgHvLeeSiEYHsOj7VlO1w%3d%3d.

[32] For example, white supremacists have used words that sound similar to "boogaloo" (a term for a civil war) but not exactly 'boogaloo' to avoid detection as follows: "'Boogaloo' has been morphed to sound-alikes like Big Luau (hence the Hawaiian shirts clothing) and Big Igloo (hence the patches) in an explicit effort to throw would-be censors off the scent." Source: Emma Grey Ellis, "The Meme-Fueled Rise of a Dangerous, Far-Right Militia," https://www.wired.com/story/boogaloo-movement-protests/.

[33] See the GCTF "Racially or Ethnically Motivated Violent Extremism" (REMVE) Toolkit Initiative Exploratory Preparatory Deep-Dives with Subject Matter Experts, available at: https://www.thegctf.org/Portals/1/Documents/Links/Meetings/2022/REMVE%201-2%20and%209-10%20March/Deep%20Dives/DeepDiveSummariesGCTFREMVEInitiative.pdf?ver=05cqxSVJA_xqUcyNgPS8AA%3d%3d.

or other content removal should only occur when and as consistent with domestic and international law. Furthermore, legislation should be able to rapidly adapt to changes in technology to effectively respond to swift ICT evolution and the new ways REMVE actors choose to utilize ICTs for nefarious activities. Many laws are limited to outdated responses (e.g., phone taps) when the threat is far advanced in its operations and platform use. Public-private partnerships (PPPs) between private actors and relevant public institutions (e.g., criminal justice actors) can be key in detecting and deterring REMVE by enhancing the knowledge of current threats and trends, thereby facilitating more effective legal, policy, and operational responses.

Recommendation 3: Examining the nexus between criminal organizations and violent extremist groups/individuals.

Active and latent nexuses between criminal organizations and REMVE groups should be examined by the relevant police, security, and intelligence services. Such a nexus has already been detected amongst some known REMVE actors[34] who have relied on drugs, firearms, and other illicit goods to traffic as a source of funding. Early detection and disruption of such relationships is crucial as many of the skills that can be obtained through membership in and/or collaboration with criminal organizations, such as money laundering, identity fraud, or weapons proficiency, can make REMVE actors more dangerous and harder to counter.[35] REMVE actors have also been known to monetize hate speech[36] by receiving payments for advertising on websites that host their content; these payments are then used to fund wider ideological goals. As the particular use of these payments is not necessarily an activity that the relevant institutions can easily investigate or have the remit to investigate, such monetization poses substantial challenges. Being aware of this monetization is nevertheless important in the broader context of the nexus between criminal organizations and REMVE actors. Understanding the relationship among criminal organizations and REMVE actors should therefore be a key priority. To disrupt and counter this nexus, international and domestic cooperation in confronting REMVE could be expanded. Facilitating international and multi-stakeholder cooperation, for instance, among policymakers, practitioners, civil servants, and private partners (e.g., financial institutions) could be an important first step in fostering a better understanding of the sensitivities and complexities of REMVE.

[34] In one example, 64 members of various white supremacist groups including the Aryan Nation, Aryan Circle, Aryan Brotherhood, the Peckerwoods, Dirty White Boys, and Soldiers of Aryan Culture, were arrested and sentenced to a combined 820 years in prison. The majority of the defendants relied heavily on profits from methamphetamine sales to fund their activities. See: U.S. Department of Justice, "64 White Supremacists Sentenced to a Combined 820 Years in Federal Prison" 14 February, 2020, https://www.justice.gov/usao-ndtx/pr/64-white-supremacists-sentenced-combined-820-years-federal-prison. It is important to emphasize that while other forms of organized crime have been used for financing violent extremist and terrorist groups – e.g., firearms trading and/or human trafficking among others – drugs and firearms trafficking were relied upon in this particular case.

[35] See also the GCTF's *The Hague Good Practices on the Nexus between Transnational Organized Crime and Terrorism*.

[36] For the purposes of this Toolkit, the definition relied on is the one used by the UN which is as follows: "any kind of communication in speech, writing or behavior, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, color, descent, gender or other identity factor." Full text at https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf.

Recommendation 4: Reflecting the complexities of REMVE in all aspects of preventing/countering violent extremism (P/CVE) strategies, policies, and legal provisions.

States' P/CVE strategies, policy responses, and legal provisions should be nuanced enough to consider the complex and multilayered set of challenges that REMVE poses. Building from a comprehensive understanding of the REMVE phenomenon, the complexity of REMVE should be reflected at all stages of the REMVE response cycle, from early prevention to resilience building, intervention, criminal prosecution, and rehabilitation and reintegration. Efforts aimed at discouraging and prosecuting violent extremists should be complemented by efforts to protect soft targets[37], such as public places, schools, houses of worship, and other similar targets, and to support their response and recovery in the event of an attack. Additionally, the response cycle itself should respect relevant international and domestic law obligations. Implementing a comprehensive understanding of REMVE threats into P/CVE strategies and related policy and legal responses will likely help reduce further radicalization and promote trust in intervening parties, such as governmental institutions or civil society organizations. In addition, engaging in a whole-of-society consultation process at every level of government and society while designing detection and prevention measures, as well as rehabilitation and reintegration programs, can ensure the longevity and effectiveness of such measures and programs. Lastly, a flexible and agile approach is advisable. REMVE is an evolving challenge, and its complexities should be reflected in all counter-REMVE methods to ensure that changes in REMVE actors, the nature of the threat, and fundraising or violent recruitment trends are accounted for.

Recommendation 5: Regular monitoring and (re-)evaluation of legislative and policy measures.

The operation and implementation of national legislation applicable to REMVE should be regularly reviewed and re-evaluated by the relevant domestic institutions. Legislation may need to be updated or amended as the nature of the REMVE threat changes and/or REMVE actors evolve and multiply, to ensure that the applicable laws remain appropriate to the threat.[38] For example, such regular (re)evaluation of the relevant legislation can ensure that the list of designated, proscribed, or banned groups or actors captures the most recent REMVE developments and alterations to their *modus operandi*. Changes or variations in regional and/or international definitions of REMVE, REMVE actors, or related criminal thresholds may also challenge a collective or coordinated response.[39] States should aim to integrate existing good practices in their legislation.[40]

[37] The GCTF Soft Target Protection Initiative defines soft targets as, "places which support community and economic prosperity, where people congregate to study, shop, conduct business, be entertained, worship, or travel." Moreover, these places are "inherently vulnerable to a terrorist attack." For more information see *The GCTF Soft Target Protection Initiative*, *Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context,* https://www.thegctf.org/Portals/1/Documents/Links/Meetings/2017/Twelfth%20GCTF%20Coordinating%20Committee%20Meeting/GCTF%20-%20Antalya%20Memorandum%20on%20the%20Protection%20of%20Soft%20Targets%20in%20a%20Counterterrorism%20Context.pdf?ver=2017-09-17-010844-720

[38] This includes ensuring that the applicable criminal thresholds regarding offences that may include incitement, of violent extremism and/or terrorism, or preparation or possession of materials (online and offline) as such reflect these changes and developments.

[39] Domestic legislation may require amending as to ensure the efficacy of its intended purpose. There should also be regular implementation of international and regional instruments addressing REMVE.

[40] For example, States should harmonize their legislation with that of other countries and in a manner consistent with international legal obligations, including those on human rights where applicable.

In essence, national legislatures should respond promptly to changes in the REMVE threat and seek to enhance domestic, regional, and international legislative frameworks. This is particularly important regarding REMVE online content, as ICTs and social media companies' operations are cross-border and terms of service may vary across jurisdictions, thus making it challenging for social media companies to respond efficiently or consistently. The emphasis of legislative efforts should not only be on regulation of online platforms or online financial transactions, but rather also on targeting the tactics and operations of REMVE actors that can be identified in those spaces. Further, it is crucial that any legislative and policy measures aimed at limiting the impact of and countering REMVE – both online and offline – are complementary and sustainable. Coordinating the designation, proscription, or banning of REMVE actors or groups, in a manner consistent with domestic and international law, could enhance the efficiency, complementarity, and sustainability of such legislative and policy measures.

Example of National Legislation Evaluation

In the aftermath of the terrorist attack in Oslo and Utøya in 2011, the Norwegian Criminal Code was amended to further prevent acts of terrorism, including so-called "solo terrorism". An important measure in this regard was to broaden the criminalization of preparatory terrorist acts. Section 131 third paragraph states that any person who intends to carry out an offence as specified in section 131 first paragraph (terrorist acts) or section 132 (aggravated terrorist acts), and who commits acts that facilitate and point towards carrying out the offence, shall be subject to punishment for attempt. This provision, which criminalizes preparatory terrorist acts in general, made it easier to investigate and prevent terrorism at an early stage.

Furthermore, participation in a terrorist organization and receipt of terrorist training was made a criminal offence (section 136 a and 136 letter d), and a new criminal provision on involvement with firearms or explosives with the intent to commit a criminal act was passed (section 191 a). In addition, the maximum prison sentence for aggravated terrorist acts in the Criminal Code of 1902 was changed from 21 to 30 years. According to the Criminal Code of 2005, which at the time had not yet entered into force, the maximum prison sentence for aggravated terrorist acts was already 30 years (section 132). However, it was deemed necessary to increase the maximum prison sentence before the new Criminal Code entered into force.

Recommendation 6: Regular (re-)evaluation of national P/CVE strategies.

Online and offline strategies to prevent, detect, and disrupt REMVE as well as to rehabilitate and reintegrate REMVE actors and to support their victims continue to develop. Monitoring and evaluation (M&E) mechanisms are also necessary to ensure the efficiency of such P/CVE strategies in accordance with this development. Effective M&E needs to be comprehensive and consistently applied and should include all the relevant stakeholders who were involved in the creation and implementation of P/CVE strategies. Successful assessment strategies are those developed in the earliest stages of an evaluation. The M&E process could involve a multi-stakeholder feedback loop involving criminal justice, intelligence, social and welfare services, educational and private bodies, as well as local community leaders and civil society actors, which facilitates systematic whole-of-society substantive contributions. The feedback loop could focus on assessing the efficacy and sustainability of all strategies for the prevention of REMVE, intervention, rehabilitation, and reintegration of REMVE actors, including legislative and policy measures, online or offline financial measures, and local or community-led measures, with a view to identifying gaps. Aside from assisting in revising or refining existing strategies, the feedback loop could also assist in determining future areas where novel national strategies for the prevention and countering of violent extremism could be created. Regular (re-)evaluation of national strategies for the prevention and countering of violent extremism could also assist States in ensuring compliance with international and domestic law.

Recommendation 7: Facilitating and strengthening intra- and interagency cooperation and integration of national strategies and good practices across the relevant domestic actors countering REMVE.

Intra- and inter-agency coordination and collaboration is critical to ensure the consistent and thorough implementation of counter-REMVE strategies, to build a shared understanding of REMVE among the agencies involved, and to promote a unified response to REMVE. Many different agencies and sections within them will be involved in the various components of a counter-REMVE strategy, from prevention to protection, intervention, and disruption, as well as rehabilitation and reintegration of REMVE actors, and support for their victims. Collaboration and cooperation among the criminal justice, governmental, and local authorities involved through appropriate information sharing, as well as the development and maintenance of public-private partnerships (PPPs), will be essential in adopting a whole-of-society approach to preventing and countering REMVE. The public, governmental institutions, and the private sector should all increase their awareness of REMVE threats and challenges. Governments and local law enforcement should establish partnerships with civil society and the private sector to promote situational awareness, joint planning, training, and two-way communication and information sharing on REMVE threats and tactics. Consistently sharing knowledge and expertise through PPPs can help achieve that. National legislation, policies, or strategies that provide clarity on the definitions of REMVE and measures to counteract REMVE should also facilitate better and stronger intra- and inter- agency cooperation. Agreements on the modalities of intra- and inter- agency cooperation, including information-sharing guidelines and appropriate limitations on sharing information, inclusion of REMVE-related information on a centralized whole-of-government watchlist, or a centralized interagency working group, may assist in facilitating and strengthening intra- and inter- agency coordination. Inter- and intra-agency cooperation and PPPs can also be critical in exchanging information about countering REMVE threat groups engaging in unlawful behavior.

Recommendation 8: Facilitating and strengthening regional and international cooperation and sharing of good practices related to REMVE.

Due to the transnational nature of the REMVE threat and the cross-border operation of REMVE actors, facilitating and strengthening regional and international cooperation and the sharing of REMVE-related good practices and threat information is vital. It is important to underscore the primary role of States and their competent agencies in preventing and countering violent extremism conducive to terrorism and terrorism at the national and international levels. Additionally, States and their agencies should conduct international cooperation in accordance with the principles of the United Nations Charter and relevant UN Security Council Resolutions.

States should also aim to harmonize their national legislation with that of other countries to integrate existing good practices and align their legislation, where applicable, in a manner consistent with international law obligations, including on human rights. Regional and international cooperation is essential to all components of a counter-REMVE strategy and to foster productive capacity-building exchanges and coordination. The sharing of good practices, lessons learned, and threat information is therefore key for States to address the transnational activities, operating methods, and loose organizational structures of REMVE actors and movements. Strong cross-jurisdictional relationships among relevant intelligence, police and security services, criminal justice personnel, and private sector organizations such as ICT companies and banks are very important to facilitate this cooperation. Informal channels for information sharing, such as through points of contact in inter- or non-governmental bodies or in other States, could facilitate more direct information exchange. Structured mechanisms, whereby shared information can be used in another country's domestic prosecutions or used by partner States to detect or prevent cross-border travel by REMVE actors, would also be beneficial.[41] Moreover, States should share information on REMVE actors via bilateral and multilateral (including using INTERPOL databases and the I-24/7 network) mechanisms to help travel by REMVE actors and to add REMVE terrorists to domestic and international watchlists. In this context, it is important to ensure that the applicable designated, proscribed, or banned groups databases are up to date and reflective of the most recent developments in REMVE activities and groupings both online and offline. All of the relevant designation, proscription, or banning mechanisms, and watchlisting databases should be consistent with domestic and international law.

This type of cooperation is also important when addressing REMVE online content, as ICTs, including social media companies, provide crucial communications platforms for REMVE actors across borders. Technology companies' terms of service may vary across jurisdictions, thus making it challenging for technology companies to respond efficiently or consistently when they identify REMVE threats or exchange of information in online forums. However, with regional and international cooperation and a harmonization of good practices, States, State-level entities, and companies can collectively better address REMVE.

Section IV: Capacity Building and Fostering Multi-Stakeholder Cooperation

Recommendation 9: Strengthening relationships among State and non-State actors in multi-stakeholder responses.

Fostering partnerships between State and non-State actors, especially in the context of early prevention, is very important in countering REMVE effectively. State and non-State actors should consider regular exchanges of information and, when appropriate, collaboration, to better understand the evolution(s) of the REMVE threat, to promptly identify new or resurgent REMVE threats, to develop effective countermeasures, and to implement prevention and resilience-building programs. Such partnerships can be formalized through a memorandum of understanding (MoU) or other similar

[41] Eurojust, the European Union Agency for Criminal Justice Cooperation, is an example of such a structured mechanism through which national judicial authorities work closely together to fight serious organized cross-border crime. Eurojust coordinates the work of national authorities – from EU Member States as well as third party States – in investigating and prosecuting transnational crime.

arrangements or agreements, or they can take the form of informal cooperation built on personal relationships. It is important to bring together a wide range of national and local stakeholders, such as criminal justice institutions, intelligence, security and police agencies, social and welfare services, health services, educational bodies, financial service providers, and online service providers, among others, as multi-stakeholder and evidence-based policymaking are key tools in preventing, countering, and building resilience against REMVE. Voluntary and cooperative engagement is key to information sharing, which in turn is essential to improving and sustaining capacity in terms of preventing, countering, and building resilience against REMVE, building trust, and promoting awareness of the REMVE threat. State and non-State actors should consider jointly facilitating and supporting multi-stakeholder international and national research and the strengthening of training program capabilities. Through cutting-edge research and knowledge exchange, society's overall knowledge and understanding of REMVE, particularly of the relevant actors or groups in the REMVE movement and the evolution of the REMVE movement, can be enhanced. States can also consider the employment of multi-stakeholder scenario-based discussions, tabletop exercises, and/or realistic simulations in developing and testing REMVE strategies and policies as well as in designing and implementing REMVE programming as these inclusive formats can facilitate cutting-edge research, policy development, and knowledge exchange.

Examples of Existing Multi-Stakeholder Programs

In implementing programmatic activities, the Organization for Security and Co-operation in Europe (OSCE) provides a good model for whole-of-society approaches to addressing P/CVE and counterterrorism issues. The OSCE takes a holistic approach in integrating human rights and civil society components as well as internal monitoring and evaluation mechanisms based on international best practices and OECD standards in its multi-stakeholder programming efforts.

Canada's Community Resilience Fund funds research, evaluation, and networking opportunities that are focused on countering violent extremism. A very broad range of organizations that are working to build partnerships among communities and enhance knowledge about the threat of violent extremism of all types can apply for funding: anything from regional governments, provincial territorial police forces, not-for-profit organizations, universities, individual researchers, international NGOs, and more. The Fund has been quite successful in funding several projects that contributed to enhanced knowledge of extremism and brought communities together.

In the United States, the Department of Homeland Security's Center for Prevention Programs and Partnership (CP3) enables local communities to prevent targeted violence and terrorism, with the goal of helping individuals

Recommendation 10: Building local and community-level capacities in reporting and disengaging radicalism to extremist violence.

Prevention begins with an understanding of local contexts and grievances that make individuals more susceptible to radicalization to violent extremism conducive to terrorism. Local community leaders and grassroots organizations can play an important role in identifying early signs of violent extremism and radicalization to violence, reporting suspicious behavior, and raising concerns with relevant governmental bodies. It is thus crucial to involve local community institutions and leaders as part of multi-stakeholder collaboration efforts. Communities can be integrated as a core part of broader counter-REMVE efforts, rather than as a single component of disengagement and de-radicalization programs. Further, facilitating open communication and constructive synergy among social welfare, intelligence and police services, schools and educational training institutions, and local community and religious leaders can help strengthen counter-REMVE resilience-building efforts and whole-of-society intervention mechanisms. Community policing strategies and approaches can be very useful in furthering education and information campaigns and in fortifying trust among local communities and police services and other governmental bodies. While police services and other security bodies can be very useful implementers for locally based prevention and resilience strategies, it is important to provide appropriate and tailored training and assistance reflective of the needs, contexts, and challenges of the particular community they are assigned to, including training and assistance focused on the community's own security concerns.

Recommendation 11: Prioritizing alternative measures within REMVE prevention efforts.

Appropriate alternative measures, such as psychosocial services and other alternatives to pre-trial detention and post-conviction incarceration, should be part of States' counter-REMVE prevention toolkit.[42] Psychosocial and other similar services can be an important component in early prevention, resilience-building, disengagement, and de-radicalization efforts. To be successful, an early prevention model should actively involve social welfare, education, and mental health professionals, such as psychologists and psychiatrists, and leverage relevant stakeholders and experts to support the design and implementation of prevention and disengagement programs. It is important to note that individuals susceptible to grooming and radicalizing to REMVE or other forms of violent extremism and/or terrorism tend to seek a community. Providing "off-ramps" with appropriate support mechanisms in place should form part of any considerations on designing alternative measures.

When designing and implementing alternative measures domestically, States should take into account the relevant political, economic, social, and cultural circumstances, as well as the applicable national and international legal and policy frameworks.[43] At the international level, a key theme regarding the development and implementation of alternative measures is ensuring "a proper balance among the rights of individual offenders, the rights of victims, and the concern of society for public safety and crime prevention"[44], as well as ensuring that the human rights of the individuals suspected of engaging in criminality are respected and protected. Finally, local community leaders and civil society organizations should be involved in all stages of designing and implementing alternative measures. Such involvement can repair the relationship between the radicalized individual and the community and bolster/re-introduce the individual's sense of belonging and responsibility to the community, thus increasing the likelihood of successful rehabilitation and reintegration.

[42] See also the GCTF's *Recommendations on the Effective Use of Appropriate Alternative Measures for Terrorism-Related Offenses*.

[43] The relevant international standards include the International Covenant on Civil and Political Rights (Articles 9 and 14 in particular), General Assembly Resolution 2200 A (XXI), Annex (16 December 1966); United Nations Standard Minimum Rules for Non-Custodial Measures (the Tokyo Rules), General Assembly Resolution A/RES/ 45/110, Annex (14 December 1990); Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, General Assembly Resolution A/RES/40/34 (29 November 1985); UN Economic and Social Council Resolution: Basic Principles on the Use of Restorative Justice Programmes in Criminal Matters, E/RES/2002/12 (24 July 2002); Arts. 37 and 40, United Nations Convention on the Rights of the Child (CRC) (A/RES/44/25, 20 November 1989).

[44] The Tokyo Rules, Rule 1.4.

Recommendation 12: Integrating schools and other educational institutions.

Educational institutions can be indispensable partners in the early prevention of REMVE and in community resilience-building.[45] Training educators, parents, and school administrators to engage with students at the first sign of radicalization can assist with early detection and mitigation efforts. The engagement may be as simple as, for example, a school hosting informational programs or providing resources to educate parents and community members about how youths could be exposed to REMVE messaging in a variety of fora, including through social media and certain violent or ideological video games. There are also local community groups that may benefit from the same training to complement school resources, including but not limited to sports and academic coaches, club leaders, youth group leaders and others, noting that many of these private entities are not included in government-funded trainings.[46] It is important that the integration of schools and educational institutions is not limited to those only operating within school buildings. It is also vital that individuals engaging with children and youth outside of an academic or curricular setting receive tailored and comprehensive training with respect to the relevant legal, policy, and operational guidelines, as well as avoiding bias.[47] Such training can take the more interactive form of age-appropriate scenario-based discussions, tabletop exercises, and/or realistic simulations as these formats enable the involvement and participation of a broad range of voices as well as collaborative knowledge exchange.

Moreover, it is important to avoid the perception that, by integrating educational bodies into counter-REMVE efforts, teachers have de-radicalization responsibilities, as such a perception may have second-order consequences on freedom of expression and thought in the classroom.[48] Further, clear, centralized guidelines and appropriate resourcing are crucial, as educators may have to address mandates from national, regional, and local governments, but without sufficient resources to do so. Finally, while schools can be powerful actors, they may not adequately capture the breadth of the youth population that is vulnerable to REMVE. Peer-to-peer, after-school, or extracurricular programs can be important additional components of early prevention strategies, as such programs might have a wider reach across generations and ages than schools.[49] Young people can sometimes feel excluded or disconnected from peace and security programming. Young people can serve an integral role in preventing and resolving conflict and building sustainable peace efforts in their communities (as affirmed in United Nations Security Council Resolution 2250 on Youth, Peace, and Security (YPS) – adopted on 9 December 2015.) This resolution "marked a fundamental shift in acknowledging the positive role young women and young men play in the maintenance of peace and security, and the importance of enabling their meaningful participation in decision-making at all levels."[50] Further,

[45] The United Kingdom's PREVENT program, which requires teachers and other educators to report signs of radicalization, is an example. Though controversial, it is nevertheless very useful for spotting signs of radicalization early on. Another example is the Norwegian Dembra program, developed for schools for the prevention of racism, group-based hostility, and antidemocratic attitudes. The program offers professional development for teachers, school leaders, and other school staff. Based on the school's own circumstances, Dembra helps strengthen the school's work on participation and critical thinking. See further https://dembra.no/en/.

[46] See further the GCTF's *Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online*, full text available at https://www.thegctf.org*Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online*, which provides a number of examples as to how sports programs, cultural and youth groups can be embedded in a whole-of-society P/CVE policies and strategies.

[47] See further the GCTF's *Abu Dhabi Memorandum on Good Practices for Education and Countering Violent Extremism* (CVE):

[48] It is important that the education sector is not securitized, or that schools become information-collecting institutions, as this may undermine the teacher's standing and relationship with students, genuine efforts to protect students, and broader community trust.

[49] The "Invent2Prevent" program provides seed money to university student teams to enable them to design their own CVE and sometimes REMVE online campaigns, often linked to offline activities, as part of their college course. Some of these campaigns have become NGOs.

[50] See further the United Nations' *Youth, Peace and Security* Handbook which highlights the exclusion of youth, women and other vulnerable groups in peacebuilding and security efforts, and the impact of this exclusion on the effectiveness of the efforts (pp. 21 and 28 offer good

youth and, in particular young men, tend to be viewed as a monolithic potential threat, based on their age and gender.[51] However, young people should not be viewed purely as vulnerable to violent extremism, but rather as key stakeholders in designing and supporting educational and community-based responses. Young people are often more aware of the conditions and drivers that lead their peers to radicalize toward violence; they also tend to be more effective at communicating and influencing their peers and younger age groups.[52] Youth peers should thus be approached as essential partners in REMVE prevention efforts to be integrated into the entire lifecycle of counter-REMVE programs.

Recommendation 13: Enhancing public-private cooperation to counter REMVE online.

Countering REMVE online is extremely challenging. Both public and private bodies should consider how to moderate content on online platforms, including social media platforms and online gaming platforms, and tailor their responses to respecting human rights while ensuring the effectiveness of these measures. As a starting point, governments, policymakers, and national- and local-level authorities, as well as civil society organizations, local community leaders and institutions, and the private sector should aim to design and develop online tools and strategies to counter REMVE content that respect human rights. For example, ICT and social media companies should draft and enforce their terms of use in a manner consistent with human rights.[53]

Monitoring and assessment of REMVE content shared and REMVE activities via gaming platforms should also be part of the efforts to disrupt and counter REMVE. However, such monitoring should be done in a way that does not alienate individuals for whom gaming provides an important sense of community and belonging. Moreover, it is important to distinguish between terrorist and violent extremist content and content that may be legal but is still harmful. Platforms should also ensure that their algorithms — intentionally or accidentally — do not push forward extremist content. Lastly, as REMVE actors evolve and learn to adapt their tactics, techniques, and procedures (TTPs), police, security, and intelligence services, as well as ICT companies, should regularly review and enhance their responses and capabilities.

Recommendation 14: Understanding the complexities of REMVE communications online.

To enhance the capabilities of ICT companies to counteract and disrupt REMVE activities and content circulation online, States should develop clear and comprehensive international and regional guidelines on how to counter online REMVE communication.[54] Currently, the differences across

examples): "Whether because of mere oversight or because of a presumption that youth voices are not important enough to include in data collection, these omissions constitute a serious gap in the conflict analysis methodology." https://www.un.org/peacebuilding/sites/www.un.org.peacebuilding/files/documents/yps_programming_handbook.pdf.

[51] Ibid.

[52] See further GCTF's *Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online*, full text available at https://www.thegctf.org*Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online*, which provides a number of examples on how sports programs, cultural and youth groups can be embedded in a whole-of-society P/CVE policies and strategies.

[53] See for example Regulation EU 2021/784, which addresses the dissemination of terrorist content online. A core aim of the Regulation is to improve the functioning of the digital single market by reinforcing legal certainty for hosting service providers and users' trust in the online environment, as well as by strengthening safeguards to the freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society and the freedom and pluralism of the media. https://eur-lex.europa.eu/eli/reg/2021/784/oj

[54] States should also consider the role of the Global Internet Forum to Counter Terrorism (GIFCT), which brings together the technology industry, government, civil society, and academia to foster collaboration and information-sharing to counter terrorist and violent extremist activity online. https://gifct.org

domestic legislation on violent extremist online communication and materials pose a significant barrier to efficient cross-border efforts to counter REMVE; an additional complicating factor is that often the ICT companies providing the online service or platform misused by REMVE actors can be based in a third country. As a result, ICT companies frequently find themselves in a position of having to develop their own guidelines and terms of service in the absence of clear and consistent international, regional, and/or domestic guidelines, resulting in a fragmented and piecemeal approach when ICT companies engage in content removal, for example.[55]

Content removal, account suspension, and de-platforming by ICT companies are the most common methods to disrupt the spread of REMVE materials in various formats. The availability of clear and appropriate international and regional guidelines, in addition to domestic provisions on content that violates criminal law provisions, is of vital importance, as State-directed content removal triggers questions relating to freedom of expression and the legality of the companies' actions, such as what threshold the content should meet to be removed. Takedowns may not, however, be the most efficient tool that social media companies can use in countering REMVE online. In some cases, content removed on one account can be reposted by another, or a user might move from mainstream platforms to less monitored and possibly more malevolent platforms. In addition, some REMVE actors have learned how to operate around the boundaries of relevant legal provisions as well as ICT companies' terms of service without breaching the applicable thresholds to trigger company actions and/or criminal responsibility.[56] The description of "awful but lawful" could be applied to some REMVE content and activities online, exemplifying the fine line between criminality and freedom of expression[57] that ICTs should navigate. As a final point, ICT companies such as social media companies, also need to contend with whether to preserve removed content for criminal justice purposes and if so, for how long, while at the same time fulfilling their duty to protect users' privacy. When coordinating with ICT companies on content preservation requests, the relevant authorities should ensure that such requests follow clear judicial authorization and formalized processes for content preservation.

Recommendation 15: Supporting ICT companies' counter-REMVE capabilities by developing and coordinating whole-of-society counternarratives.

The public and private bodies involved in the development and/or enhancement of online tools should consider devoting resources to developing REMVE counternarratives.[58] Providing such alternative narratives can be more efficient than content removal or de-platforming and avoids the perception of

[55] At EU level, the European Commission has proposed two legislative initiatives to upgrade rules governing digital services in the EU: the Digital Services Act (DSA) and the Digital Markets Act (DMA) as part of developing a consistent approach across the EU. See also EU Regulation 2021/784 full text available at https://eur-lex.europa.eu/eli/reg/2021/784/oj.

[56] An illustrative example is the so-called 'hate preacher' Anjem Choudary who avoided criminal prosecution for a number of years but was subsequently convicted of the offence of inviting support for a proscribed organization (*R v Anjem Choudary and Mohammed Rahman* [2016] EWCA Crim 61). The proscribed organization in question was ISIL/Da'esh.

[57] For example, different domestic and regional approaches to the scope and reach of the right to freedom of expression can make it very challenging for ICT companies to respond efficiently and consistently, as online REMVE activities and networks cross jurisdictional borders.

[58] These measures should be aimed at the protection of freedom of expression online by ensuring fairness and diversity, as well as a level playing field in the competition for recommendations on major social media platforms.

targeted censorship. As a result, alternative or counternarratives[59] should be a key component of counter-REMVE strategies. To be effective, alternative or counternarratives need to be cognizant of and appropriately tailored to the local context, while also reflecting national contexts. In essence, counternarratives should have a distinct target audience, a specific goal, a clear, focused, context-specific message, and trained, credible messengers to deliver them. Locally led efforts are vital to improving resilience to and the effective countering of REMVE, as such efforts are more likely to appreciate and factor in the particular drivers and vulnerabilities that have made individuals more susceptible to REMVE. Alternative or counternarrative development should also reflect a whole-of-society effort, including perspectives from various public entities, the private sector, civil society, academia, local community leaders, and civic institutions, such as schools and places of worship. This is crucial in the context of youth and children, who often develop their own exclusive slang, colloquialisms, or terminology. Lack of awareness or inclusion of such slang can hamper the development of effective counternarratives, as government-led development of alternative narratives may not reach the right audiences or resonate in the intended or the most effective manner. It is thus crucial that the relevant public and private entities involved in designing and promoting counternarratives have open dialogue so as to include credible and resonant voices that understand and connect with the target group.

Developing and executing successful counternarratives does not, however, negate the need for actions regarding other strategies to counter REMVE content and activities. To that end, the relevant public and private bodies should invest in improving the tools and capabilities they have for understanding REMVE content and activities on all types of online platforms (e.g., “audio-first” platforms), most notably open-source intelligence dark web investigations, and undercover work. It is important that police and intelligence and security agencies are equipped to conduct investigations on the entirety of the internet, including the deep web and especially the dark web, as REMVE actors are known to use the dark web for their communications and operations. Open-source intelligence can also complement intelligence gathered through more formal channels to provide a fuller picture of REMVE actors and their operations.[60] A multi-stakeholder approach is also key when drafting and implementing counternarrative policies. Governments should work together with ICT companies, as well as local communities to provide alternative messaging.

Recommendation 16: Raising awareness and disrupting the use of online gaming as a vector for REMVE grooming and radicalization to violence.

The role of online gaming as a potential vector for radicalization to violence across all age groups has grown in recent years. A sizeable proportion of the radicalization to violence occurs on gaming-adjacent platforms, such as private chat rooms, which are not monitored or moderated in compliance

[59] There is no standard definition for counternarratives, but the UN Counter-Terrorism Committee Executive Directorate defines them as messages that provide a positive alternative to “terrorist or violent extremist messages” and “aim to deconstruct, discredit, and demystify violent extremist messaging, whether through ideology, logic, fact, or humour.” See: *CTED Analytical Brief: Countering terrorist narratives online and offline*, UN CTED, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_analytical_brief_countering_terrorist_narratives_online_and_offline.pdf.

[60] Open-source intelligence can be especially useful in cryptocurrency/blockchain forensic analysis, for example. “Off-chain,” or non-blockchain analyses, especially open-source investigations, can greatly complement “on-chain” information discovered via forensic analyses of the blockchain, thus producing a fuller picture of the actor’s illicit activities.

with terms of service, and less so within the main components of the video game itself.[61] It is important to emphasize that this phenomenon is observable across all age groups and is not gender specific.

There are three distinct ways in which REMVE actors and other violent extremists can exploit video games to spread their message and increase recruitment. First, although rare, games could be used as a training ground for violent attacks.[62] Second, REMVE and other violent extremist actors have begun utilizing gaming culture terms, video game aesthetics, iconography, and slogans to resonate and appeal to young people, in particular.[63] And third, by exploiting the difficulties associated with moderating online gaming platforms, such as unmoderated private chat rooms within or adjacent to gaming platforms, REMVE and other violent extremist actors can more easily spread propaganda and expand recruitment. Violent extremists' usage of signs, symbols, and slang might not be easily recognizable to platform moderators if they have not been specifically trained on how to spot them. Moreover, many gaming companies are small and may not have the personnel needed to provide enough local and specialized moderation throughout the jurisdictions in which they operate, with the result that companies need to rely on users to flag REMVE content and activities. User-driven content moderation is only effective if users are proficient in the relevant platform's terms of service and if the users themselves are aware of the violent extremist language or rhetoric being used.

While disrupting the use of online gaming as a vector for radicalization to REMVE violence can be a complex challenge, it is important to note that online gaming should not be viewed only from a threat perspective. Gaming can be a source of community for many people, and draconian moderation measures may worsen the challenges by driving individuals into more isolation, thus increasing their vulnerability to radicalization to violence. For example, heavy regulation of online gaming spaces may heighten the appeal of these games to young people by making them appear "cool" and "edgy" to play. Counter-REMVE measures focused on online gaming should be carefully leveraged against the possibility of depriving individuals of a community that can, in some ways, serve as a buffer against radicalization to violence. To ensure a tailored and comprehensive response to the challenges of online gaming as vectors for radicalization to REMVE violence, engaging a broad range of public and private bodies as well as local and youth leaders would provide a more holistic approach.[64]

Recommendation 17: Designing and developing a whole-of-government and whole-of-society response to REMVE online.

As part of a whole-of-society response to REMVE online, governments should consider enhancing their relationships with gaming and ICT companies to improve information sharing and help strengthen their capabilities to counter REMVE content and activities. Likewise, the gaming industry should consider partnering with national and regional governments and local municipalities to develop and implement a plan of action for safeguarding their platforms from REMVE content and activities. As children and youth are increasingly at risk of online and offline exposure to radicalization and/or recruitment to extremism/REMVE, the age of radicalization to extremist violence is lowering. Thus,

[61] The EU's Radicalization Awareness Network has called gaming-adjacent platforms "hotbeds" of radicalization. See further "*Extremists*' use of gaming (adjacent) platforms: Insights regarding primary and secondary prevention measures," *Radicalization Awareness Network*, https://ec.europa.eu/home-affairs/system/files/2021-08/ran_extremists_use_gaming_platforms_082021_en.pdf.

[62] There have been some neo-Nazi video games where the targets for in-game violence were members of the LGBTQ+ or Jewish communities.

[63] The Christchurch attack was a prominent example, where the attacker livestreamed the attack in a manner similar to first-person shooting games.

[64] See, for example, Wicked Saints Studios, which makes text-based adventure activism games using behavioral technology: https://www.wickedsaints.studio/. In their approach to gaming, Wicked Saints Studios show how companies can use gamification and games to build prevention skills.

integrating educational bodies such as primary and secondary schools as well as universities within offline and online counter-REMVE strategies is crucial. In this context, it is important to provide those working in educational bodies with appropriate training, including workshops to enhance digital literacy, promote critical thinking skills, and develop clear lines of communication with social and welfare services and other resources with police, intelligence, and security services.

Whole-of-society counter-REMVE strategies should support and facilitate regular collaboration among research institutions and online gaming and ICT companies to enhance knowledge and capabilities. Closing knowledge and capability gaps is important as the work that the relevant sectors of academia and/or civil society may be conducting might not necessarily address the information gap that ICT companies are facing in countering REMVE content and activities. For example, there can be a disconnect between how researchers discuss their findings and how designers and engineers in the online gaming industry can implement these findings in algorithms or virtual components of a game. Research institutions, online gaming platforms, and other technology companies should encourage and/or enhance already existing collaborations among, for example, ICT and online gaming companies, outlining specific knowledge gap(s) that they need to address. Meanwhile, research institutions should provide the requested information in a format/language that is more accessible to ICT and gaming companies. Lastly, as REMVE actors evolve and learn to adapt their TTPs, public and private partners should continue to enhance their responses and capabilities.

Recommendation 18: Developing sustainable and useful REMVE programming to help communities build resilience.

Offline programming can play an important role in helping individuals within local communities build resilience to REMVE. Local programs that are tailored to local contexts, challenges, and vulnerabilities should be essential components to any strategies to prevent, deter, disrupt, and counter REMVE. Further, robust M&E processes of such programs are an important tool for developing counter-REMVE programming that is sustainable and useful to individual communities. M&E mechanisms should be integrated into the initial design and implementation phases of any new REMVE program or effort and should involve a whole-of-society consultation process. Frequent and structured interaction among relevant security, police, and intelligence personnel, local community and religious leaders, civil society organizations, and other front-line workers and subject matter experts can help to assess the implementation and operation of locally based prevention or resilience building programs. Such M&E collaboration should be a key component of supporting the sustainability and effectiveness of counter-REMVE strategies and policies to promote effective programming that can help communities build internal resilience to REMVE challenges.[65] Additionally, facilitating and supporting cutting-edge research and interdisciplinary information exchange and cooperation is key to enhancing knowledge, strengthening M&E efforts, building trust and resilience, and bringing communities together.

Recommendation 19: Local engagement and exchange of local REMVE initiatives/good practices.

Due to a more nuanced grasp of the unique REMVE threats they face, local communities, institutions, victims of REMVE, and civil society organizations can be vital partners in the design, development, and implementation of counter-REMVE initiatives. Local communities can play an important role in

[65] An example is the holistic M&E approach adopted by the OSCE, which integrates human rights and civil society components as well as internal monitoring system based on Organization for Economic Co-operation and Development (OECD) standards.

developing counternarratives. Local counternarrative programs can benefit specific audiences, such as teachers or parents, who interact with individuals most vulnerable to REMVE ideologies.[66] Counternarratives, however, should respect the freedom of expression of those targeted and consider the possible risk of further radicalization to violence of certain vulnerable groups. A cooperative relationship among local communities, civil society organizations, and governments can allow government agencies and local leaders to refine and expand their understanding of REMVE threats and how best to address, prevent, and counter relevant security challenges.

Moreover, local counter-REMVE initiatives and good practices should be integrated into, or at a minimum referenced by, national strategies. It is key that national strategies complement local efforts rather than attempt to supplant them. Governments should ensure meaningful local and community participation throughout the process of designing, developing, and implementing these initiatives to effectively operationalize community resources. This can be achieved by fostering effective dialogue and cooperation among State and non-State actors that is based on mutual trust and understanding. Further, it is important that REMVE strategies make clear the distinction between prevention, resilience building, and countering REMVE so the right audience is targeted. As with recommendation 9, States and local communities can also consider the employment of multi-stakeholder scenario-based discussions, tabletop exercises, and/or realistic simulations in developing and testing REMVE strategies and policies as well as in designing and implementing REMVE programming as these inclusive formats can facilitate cutting-edge research, policy development, and knowledge exchange.

Section V: International Cooperation and Multi-Stakeholder Coordination

Recommendation 20: Coordinating information exchange across national and global stakeholders.

Coordination among State agencies is one of the key challenges in countering REMVE. Improving interagency information sharing, collaboration, and coordination will strengthen States' capacity to respond to REMVE. Due to the cross-border and evolving nature of REMVE, security and intelligence agencies can find it difficult to obtain the necessary information promptly and efficiently share that information across all agencies involved and other relevant stakeholders. For example, when requesting data and information from ICT companies, it is not uncommon for multiple government agencies, ministries, or offices to reach out asking for the same information at different times. Domestically, States should consider identifying a single point of coordination among police and security agencies, prosecutors, and other relevant stakeholders for requesting evidence from social media and other ICT companies. Further, at the national level, there should be interagency permissions and standard operating procedures, as well as clearly defined limits with respect to information sharing among State agencies, including appropriate use of this information for watchlisting and screening purposes.[67] These domestic efforts should be complemented by international and regional information-sharing resources and mechanisms.

[66] Studies have shown that, when equipped with the right training, parents and educators prove to be effective in reaching vulnerable youths and intervening in the process of their radicalization.

[67] See relevant GCTF documents on watchlisting, such as the GCTF's *Counterterrorism Watchlisting Toolkit* and *the New York Memorandum on Good Practices for Interdicting Terrorist Travel*.

Strong cross-jurisdictional coordination and collaboration among the relevant intelligence, police and security services, and criminal justice personnel are crucial.[68] State agencies involved in countering REMVE should have awareness of how REMVE conduct is criminalized in neighboring countries to best facilitate efficient and appropriate information sharing, and to prevent REMVE actors from exploiting seams that result from a patchwork of laws, policies, and authorities. Formal and informal channels for information sharing, including through the establishment of memoranda of understanding, could be a good means of facilitating more direct information exchange. Any such exchanges should be operationalized in a manner that aligns with international and domestic legal protections while also respecting international human rights. Additionally, States should support evolving methods of information collection, such as open-source information and prison and financial intelligence.

Recommendation 21: Strengthening Public-Private Partnerships' cooperation and coordination on financial tools to counter REMVE.

PPPs are a vital tool for countering the financing of REMVE. Financial institutions have unique access to information, data, and financial records that could be useful to police, intelligence, and security agencies and countering the financing of terrorism (CFT) efforts. When governments and the private sector enter into PPPs, and the appropriate legal and regulatory frameworks to do so are in place, then detecting and countering the financing and prohibited REMVE-related transactions can be more efficient. Aside from strengthening public-private cooperation and coordination on assessing how REMVE actors finance their criminal activities, the relevant stakeholders should also strengthen, regularly evaluate, and update the financial tools needed to disrupt and prevent REMVE actors' funding flows, thus denying or at least curtailing these actors' abilities to raise, move, store, and use financial resources.[69] The public and private bodies involved should aim to share knowledge and information on the evolving means through which REMVE actors fundraise in a manner that is respectful of applicable legal and policy obligations. Raising awareness of how REMVE actors financially sustain their activities and closing knowledge gaps in this respect should be an important component of counter-REMVE strategies. Private sector companies — such as financial institutions, blockchain analysis companies, or cryptocurrency exchanges — can have granular data in their systems or platforms that can shed light on how REMVE groups and actors use financial products and services, sometimes to evade sanctions or other legal mechanisms. By entering into established PPPs, authorities could increase the understanding of how REMVE actors fund their activities and/or lead to more actionable intelligence.

Further, States could consider formalizing partnerships with private sector actors to support and strengthen multi-stakeholder financial investigative tools, where financial regulations permit. A more formalized basis for information sharing and coordination could allow for improved efficiency of public and private counter-REMVE efforts, as smaller companies might not have the necessary internal knowledge or capacity to recognize or investigate REMVE fundraising efforts on their platforms or in their systems. To support and enhance such partnerships, governmental bodies can initiate and foster interdisciplinary research to identify and flag the latest REMVE threats and fundraising trends. Information sharing, whether among agencies or between public and private bodies, should be carried

[68] Norway has devoted significant efforts to the prevention of REMVE, with a focus on the pre-criminal space, i.e., before criminal activity has occurred. Norway's model brings together the security police with the regular local police force and other parts of government to build understanding of the different types of information agencies possess, and how these can be cross-shared and utilized. This model helps security and law enforcement agencies at all levels keep pace with the evolving threat landscape. The partnership also extends to civil society and assesses both the online and offline activities of threat actors, understanding that this holistic approach is necessary.

[69] For the purposes of the Toolkit, fund or funding is defined broadly to include both traditional (fiat) currency and emerging forms of payments, such as cryptocurrency.

out in line with safeguarding non-discrimination, privacy, and freedom of expression rights, as well as with respect to the rule of law and relevant international obligations.

Recommendation 22: Enhancing legal and regulatory frameworks to support public-private cooperation in counter REMVE-related financial investigations.

Robust legal and regulatory frameworks complement each other in providing the necessary foundation to operationalize PPPs and to support efforts to counter the financing of REMVE. Most States comply with the Financial Action Task Force's (FATF) Standards or are working to address their deficiencies, regarding their anti-money laundering (AML) and countering the financing of terrorism regimes.[70] As REMVE actors' use of cryptocurrency, digital assets, and other emerging monetary instruments grows, it is important that States have the capacity to address prohibited REMVE-related activities. Given the cross-border nature of some REMVE-related transactions, States with an expertise in AML/CFT, in particular cryptocurrencies and other digital assets, should consider engaging in cross-border training and capacity-building exercises to assist countries that are still developing their AML/CFT regimes, and will be assessed on their compliance with the FATF's CFT and virtual asset standards. Once the regulatory and legal frameworks are established, police, intelligence, and security agencies, financial intelligence units (FIUs), and private industry can use sophisticated financial analysis software and tools to detect suspicious transactions and analyze financial data. Know Your Customer (KYC) requirements can begin the process of detecting suspicious REMVE-related transactions and/or terrorist financing. This process continues with Customer Due Diligence requirements that stipulate that a financial institution should conduct ongoing monitoring and keep up-to-date customer information and should factor into the risk profile for that specific customer and cause certain transactions to be flagged as suspicious. To effectively identify and detect risks and suspicious transactions, States, financial sectors, and other relevant stakeholders should be knowledgeable about emerging technologies and proficient in relevant modern analytical methods.

Recommendation 23: Aligning financial and intelligence data collection and exchange with international and domestic legal obligations.

The collection of financial data and intelligence is a crucial aspect of detecting and interdicting REMVE activity, but it should be conducted in line with States' obligations under international law and domestic legal regimes. Such an alignment can be challenging due to States' differing legal frameworks and different thresholds for what constitutes criminalized financial activities with respect to REMVE.[71] A lack of pre-existing global principles and international agreements could pose legal, operational, and policy challenges to sharing financial information. On the legal side, financial intelligence should be obtained while respecting the applicable privacy and data protection legislation, owing to the nature of the information being collected. Due to KYC obligations and mandatory reporting requirements, many financial institutions can detect and report suspicious transactions and activities, including uncharacteristic purchases or transfers or payments to known REMVE groups or actors. When financial institutions and other covered entities share financial intelligence with the appropriate

[70] See further the Financial Action Task Force (FATF) *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations.*

[71] Any information sharing undertaken via the Egmont Group, for instance, comes with an agreed-upon set of principles and other agreements that States are asked to respect. The Egmont Group also has protective restrictions on what States can use the information for, such as using it for leads but not allowing it in court, and ensuring it is not used for political reasons. The Financial Action Task Force's (FATF) Standards also provide agreed-upon recommendations and principles for States to follow in exchange of financial information. See: the Financial Action Task Force (FATF) *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations.*

authorities, it should be carried out in accordance with domestic legal and regulatory regimes, while respecting data protection regulations.

As such, it is important to implement and/or enact legislation that establishes the regulatory framework regarding the collection, analysis, and response to prohibited REMVE-related financial transactions, supported by a proper legislative framework, in accordance with FATF Standards, to prohibit terrorist financing. The legislation should include provisions for the type of financial institutions, products, and services operating within the jurisdiction. Legislative frameworks should also ensure that there are clear provisions outlining how information can be shared and how that information — especially information obtained from different countries — can be used in court to support prosecutions. States could consider implementing structured cooperation and coordination mechanisms with police, security, and intelligence services in other countries, allowing investigators in one country to potentially share, obtain, and use information from other countries in their own domestic prosecutions.[72]

Recommendation 24: Enhancing the operational capabilities of financial and intelligence data collection and exchange tools.

Operationally, differing regulatory regimes do not necessarily prevent countries from sharing information, but countries may have different requirements or standards that could limit the use of the information. Thus, it is important for relevant agencies to clearly understand what information can be shared between States and, moreover, for what purpose. Policymakers, regulators, police, security, and intelligence agencies could identify pre-existing avenues to share information that can be used to share REMVE-related financial information. Authorities could then establish a clear process, in accordance with the requirements of a specific measure or mechanism, that would allow for bilateral or multilateral State communications, including a dedicated point of contact with responsibility for coordination among countries, guided by pre-existing mechanisms, arrangements, or legal agreements.

States could also examine the sufficiency or effectiveness of existing information-sharing arrangements relevant to REMVE information. If necessary, States can consider formalizing information-sharing processes on REMVE-related activities through an MoU. The MoU will need to ensure it does not impede existing agreements among the States or contradict international or domestic legal obligations. The agreement should also comply with human rights and data protection provisions. Such an MoU could support efficient working relationships among relevant entities and counterparts in each State, so that cross-border information-sharing processes work expeditiously and effectively.

Recommendation 25: Enhancing regional and international alignment of counter-financing REMVE responses.

International and regional responses to REMVE should be aligned for them to work most efficiently. For example, targeted financial sanctions can help counter REMVE groups and individual actors' funding streams by ensuring uniformity of proscription/designation, regulatory and legal regimes, and application. This could be particularly helpful in circumstances where REMVE actors are relying on complex and cross-jurisdictional funding streams. However, any adverse effects of sanctions should be noted: they can contribute to the further radicalization to violence of certain actors and can

[72] Eurojust is an example of such a mechanism.

become less effective over time if REMVE actors develop sanctions-evasion mechanisms, similar to those developed by certain terrorist groups, including non-REMVE groups like al-Qaeda and the so-called ISIL/Da'esh. Cooperation with the private sector, especially ICT companies, can be crucial in addressing the challenges associated with self-financed REMVE actors.

Recommendation 26: Promoting whole-of-society resilience throughout the REMVE life cycle.

Countering REMVE requires a holistic approach with whole-of-society involvement, input, and feedback. Such an approach can serve to build a strong sense of belonging and encourage sustained civic engagement, inclusiveness, and responsibility, and therefore engender whole-of-society resilience. Promoting whole-of-society resilience throughout the entire REMVE life cycle, from early prevention and detection, through to bolstered community resilience, timely response, and enhanced information sharing, will also help to strengthen programs and interventions, empowering actors and sustaining momentum for success. This more expansive approach can be applied across the full life cycle of REMVE, from preventing susceptible individuals from being attracted to REMVE ideologies, to intervening with individuals who are on the path to REMVE radicalization to violence, to the rehabilitation and reintegration back into society of radicalized individuals, where appropriate and feasible. Building whole-of-society resilience is important since many stages of the REMVE life cycle are not necessarily linear and might feature overlaps. Moreover, countering REMVE is an ongoing and iterative process. Integrating whole-of-society resilience throughout the life cycle can thus help with coordination efforts among the various government, non-government, civil society, and community-level actors involved in producing, implementing, and evaluating counter-REMVE programming. To ensure the longevity and effectiveness of such programming, open and honest dialogue among all stakeholders is vital in pursuing efficient and sustainable collaboration to prevent and counter REMVE. Governments should be aware of any existing sensitivities especially in instances where civil society organizations and local community leaders may be concerned about the stigmatization of particular communities.

September 2022

GCTF
GLOBAL COUNTERTERRORISM
FORUM

www.thegctf.org