CEP BRIEFING PAPER

Virtual Event Series 2021: Violent Right-Wing Extremism and Terrorism

Dr. Hans-Jakob Schindler, Alexander Ritzmann and Marco Macori

Counter Extremism Project (CEP) Germany

May 2021

COUNTER EXTREMISM PROJECT

Table of Contents

I. Overview

In an in-depth study in 2020, the Counter Extremism Project (CEP), commissioned by the Federal Foreign Office of Germany, analyzed the transnational connectivity of the violent right-wing extremist (vXRW) and terrorist movement in five European countries and the US.[1] It argued that in particular since 2014 a new leaderless apocalyptic transnational vXRW and terrorist movement emerged, which is responsible for a growing amount of violence in the countries at the center of the study.

The study also outlined that all governments had developed a variety of countermeasures, ranging from prevention and countering violent extremist (P/CVE) approaches, efforts with a focus on executive and intelligence-led measures to mixed strategies which integrated P/CVE with an increase in executive capacities as well as legal and administrative changes.

However, the study argued that due to the growing transnational connectivity of right-wing extremist and terrorist networks, both offline in physical networking hubs as well as online through specific online ecosystems, transnational measures and mechanisms would be an effective, complementary tool to national strategies and tactics.

From the analysis of the study, five main issue areas emerge, in which further transnational cooperation and coordination could be achieved to mitigate the threat emanating from this movement:

(1) The further development of a common understanding and legal concepts, better capturing the terrorist nature of this developing threat.
(2) Development of a deeper and more nuanced understanding of the various online ecosystems that underpin and connect the networks within this transnational movement and the deployment of already existing capacities, which are currently geared to counter Islamist terrorism online.
(3) More in-depth analytics concerning the financial activities and transnational commercial connections of the vXRW and terrorist movement to allow for the potential adjustment of existing global counter terrorism financing mechanisms.
(4) Greater awareness and the development of appropriate countermeasures focusing on the training activities within the vXRW movement, in particular paramilitary training.
(5) The further development of P/CVE approaches and concepts on a local, national and transnational level, based on lessons learned.

Throughout 2021, CEP, in cooperation with the Federal Foreign Office of Germany will address these issues in a series of virtual events, bringing together relevant national and multilateral policy stakeholders. These events will be accompanied by a series of short reports, outlining the main operational and policy issues. Building on the discussions with relevant stakeholders, these papers will contain a range of concrete policy recommendations.

[1] Counter Extremism Project, Violent Right-Wing Extremism and Terrorism – Transnational Connectivity, Definitions, Incidents, Structures and Countermeasures, November 2020, https://www.counterextremism.com/sites/default/files/CEP%20Study_Violent%20Right-Wing%20Extremism%20and%20Terrorism_Nov%202020.pdf. For ease of reference referred to as CEP XRW Report 2020.

This overview paper aims to outline the main aspects of these five issue areas and demonstrate how these relate to each other.

II. Building stronger transnational mechanisms

II.I. Central role of legal concepts

The growing level of violence perpetrated by members of the transnational vXRW and terrorist movement have increased awareness both of the general public as well as among policy stakeholders of this developing threat.

In June 2020, Catherine de Bolle, Executive Director of Europol, highlighted that "a wave of [extreme] right-wing violent incidents that included the terrible attacks in Christchurch (New Zealand) and others in the USA [and ...] also reached Europe."[2] At the same time, German Federal Interior Minister, Horst Seehofer, declared "right-wing extremism [...] the biggest threat to security in Germany,"[3] an assessment he repeated again in October 2020.[4] In the US, the Federal Bureau of Investigations (FBI), assessed that 2019 had been "the deadliest year for domestic violent extremism since [...]1995,"[5] and in early 2020 elevated the threat posed by far-right extremism and "racially motivated violent extremism," placing it at the same threat level as foreign terrorist organizations such as the Islamic State of Iraq and the Levant (ISIL).[6]

However, the CEP study found that on a transnational level a common understanding and shared legal concepts relating to this threat remain underdeveloped.[7] This presents a challenge both for the collection and collation of data describing this threat as well as the development of joint mechanisms tailored to mitigate it. Furthermore, the report highlighted that many of the groups and networks within this transnational movement have not yet been designated as terrorism-related by many governments.[8] This limits the potential applicability of already developed counterterrorism measures, including measures to combat the financing of terrorism.

Therefore, a first crucial step should be a transnational dialogue focused on discussing commonalities and differences in the analysis of this threat that could be captured in shared

[2] Europol, EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT (TE-SAT) 2020, https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020
[3] Deutsche Welle, "Number of right-wing extremists in Germany on rise, security report suggests," 9 July 2020, https://www.dw.com/en/germany-right-wing-extremists/a-54105110
[4] Andre Przybyl, "Bundesinnenminister: Rechtsextremismus ist größte Bedrohung", Neues Ruhr-Wort, 1 October 2020, https://neuesruhrwort.de/2020/10/01/bundesinnenminister-rechtsextremismus-groesste-bedrohung/
[5] Jill Sanborn, "Statement Before the House Committee on Homeland Security, Subcommittee on Intelligence and Counterterrorism. Confronting the Rise in Anti-Semitic Domestic Terrorism. Statement for the Record," 26 February 2020, https://www.fbi.gov/news/testimony/confronting-the-rise-in-anti-semitic-domestic-terrorism.
[6] U.S. Department of Justice, Federal Bureau of Investigation, "FBI Oversight, Statement Before the House Judiciary Committee, by Christopher Wray," Washington, DC, 5 February 2020, https://www.fbi.gov/news/testimony/fbi-oversight-020520/
[7] CEP XRW Report 2020, page 32f.
[8] CEP XRW Report 2020, page 38f.

legal concepts. This would also enable a broadening of the understanding of the threat emanating from the transnational vXRW and terrorist movement, not only as a national domestic extremist issue but also as a transnational terrorism threat.

II.II. Online sphere integral to the movement, but heterogenous

The CEP study also demonstrates that the transnational vXRW and terrorist movement has developed specific online ecosystems which are an integral part of the movement. In addition to meetings and gathering in geographic network hubs,[9] the online sphere plays a crucial role in the transnational functionality of the movement.[10] This is particularly the case during the current COVID-19 crisis.[11]

Within this unorganized collective, individuals and groups feel connected by shared values, actions and perceived enemies. However, due to the fact that this movement is leaderless and characterized by a variety of organizational models and structures as well as networks of loosely connected individuals,[12] the online ecosystem mirrors this variety and is characterized by a variety in online nodes. Different sub-milieus are e.g. the transnational XRW Mixed Martial Arts (MMA) and music scenes, the accelerationists like Atomwaffen Division (AWD)/"lone" actors, the traditional groups/parties like Nordic Resistance Movement (NRM) or the Nationaldemokratische Partei Deutschlands (NPD). They have all developed their own distinct online communities, employing a wide range of strategies and tactics. Therefore, tailored analyses and appropriate counter measures should be deployed.

Building on an analysis of these strategies and tactics, a range of preventative and countermeasures should be employed, starting with effective proactive moderation by platform providers, the deployment of strategic communication also in messenger apps and gaming platforms as well as tailored alternative or counter-narratives. In recent years a range of stakeholders within the tech industry have made efforts to counter the misuse of their services. The Christchurch Call for Action and the development of the Global Internet Forum to Counter Terrorism's (GIFCT) Content Incident Protocol demonstrate this.[13] However, significant failures, such as the failure to quickly contain the spread of the Christchurch attack video[14] or effectively moderate online communities prior to the attack on the US Capitol in January 2021[15] continue to occur regularly.

Therefore, in addition to voluntary industry initiatives, government regulation is playing an indispensable role by requiring greater transparency, setting standards for moderation, creating legal clarity and providing commercial incentives through penalty systems which enable companies to strengthen their defensive mechanisms against abuse by

[9] CEP XRW Report 2020, page 18f.
[10] CEP XRW Report 2020, page 28f.
[11] CEP XRW Report 2020, page 19.
[12] CEP XRW Report 2020, page 11f.
[13] https://gifct.org/crisis-communications/
[14] Lapowsky, Issie, Why Tech Didn't Stop the New Zealand Attack from Going Viral, Wired, 15 March 2019, https://www.wired.com/story/new-zealand-shooting-video-social-media/
[15] McEvoy, Jemima, Capitol Attack Was Planned Openly Online For Weeks—Police Still Weren't Ready, Forbes, 7 January 2021, https://www.forbes.com/sites/jemimamcevoy/2021/01/07/capitol-attack-was-planned-openly-online-for-weeks-police-still-werent-ready/?sh=2cbe57ce76e2

extremist/terrorist actors. In this regard, new legal developments such as the amendments of the German Network Enforcement Act (NetzDG) in 2020 and 2021, the passing of the Terrorism Content Online (TCO) Regulation of the European Union as well as the ongoing negotiations concerning the future Digital Services Act (DSA) of the European Union are crucial developments. In addition to necessary improvements of these new regulatory systems,[16] the effectiveness of these new regulatory frameworks will also depend on a common understanding between governments concerning the legal aspects of the threat and its connection to terrorism. For example, NetzDG and DSA require companies to remove "illegal" content after notification, while the TCO focuses on terrorism-related content.

II.III. Financial activities, transnational commercial connections

The CEP study identified three primary income streams for the transnational vXRW and terrorist movement: a) events, such as festivals and MMA events, b) sale of merchandise and c) donations. In combination, all these income streams generate significant amount of turnover.[17] The sale of merchandise also involves online stores both in Europe as well as the US.[18] Furthermore, as payment service providers have in some cases withdrawn business from these online stores, the use of cryptocurrencies as alternative payment methods have increased.[19]

Unfortunately, the awareness of the tech industry remains low and its defensive mechanisms against the misuse of their services for terrorist financing remain weak.[20] Similarly, regulatory challenges and gaps concerning the misuse of cryptocurrencies also continue to exist.[21]

---

[16] See for example: Ritzmann, Alexander; Schindler, Hans-Jakob, NetzDG 2.0. Recommendations for the amendment of the German Network Enforcement Act (NetzDG), CEP, 2020, https://www.counterextremism.com/sites/default/files/CEP%20NetzDG%202.0%20Policy%20Paper%20April%202020%20ENG.pdf
Ritzmann, Alexander, Farid, Hany, Terrorist Content Online - How to build comprehensible transparency for automated decisionmaking systems (ADM), CEP Policy Brief 2020, https://www.counterextremism.com/sites/default/files/CEP%20TCO%20ADM%20Transparency%202604.pdf
Ritzmann, Alexander; Farid, Hany; Schindler, Hans-Jakob, The EU Digital Services Act (DSA). Recommendations For An Effective Regulation Against. Terrorist Content Online, CEP, 2020, https://www.counterextremism.com/sites/default/files/CEP%20Policy%20Paper_EU%20DSA_Sept%202020.pdf
[17] CEP XRW Report 2020, page 22f.
[18] CEP XRW Report 2020, page 23.
[19] CEP Report 2020, page 23.
[20] Schindler, Hans-Jakob, Financing of Terrorism and Social Media Platforms, CEP Policy Paper, April 2020, https://www.counterextremism.com/sites/default/files/CEP%20Policy%20Paper_Terrorist%20Financing%20und%20Social%20Media_April%202020.pdf
Schindler, Hans-Jakob, Misuse of Online Services for the Financing of Terrorism, Counter IED Report 2021 (forthcoming)
[21] Eisermann, Daniel, Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges, CEP/Berlin Risk, 2020, https://www.counterextremism.com/sites/default/files/Cryptocurrencies%20as%20Threats%20to%20Public%20Security%20and%20Counter-Terrorism_ENG%20Translation_April%202020.pdf
Schindler, Hans-Jakob; Eisermann, Daniel; Hanley-Giersch, Jennifer, Further Development of European Regulatory Framework for Cryptocurrencies necessary to mitigate Risks of Terrorism

Therefore, more effective regulation of the tech industry will also be an important measure to disrupt the financial activities, in particular the transnational financial activities, of the vXRW movement. In addition, media reports indicate that recent arrests in Germany in December 2020[22] and January 2021[23] targeted vXRW networks that financed their activities via the drug trade.

Unfortunately, as the CEP study highlights,[24] currently, raw data and overall analyses concerning the financial activities of vXRW and terrorism networks remain rare.[25] Furthermore, the understanding of this phenomenon among regulators seems generally less developed compared to the financing of Islamist terrorism. Therefore, it is of particular importance that the Financial Action Task Force (FATF) has highlighted the analysis of right-wing extremist financing as one of its current priorities.[26] However, further cooperation concerning these online and offline financial activities would be helpful. Here too, further agreement on legal concepts and the aspects of the transnational vXRW movement that are related to terrorism will enable greater applicability of the already existing legal and administrative mechanisms, developed in the past 20 years to counter the financing of terrorism.

II.IV. Paramilitary training activities: awareness and countermeasures

One of the most concerning offline threats emanating from members of the transnational vXRW and terrorist movement concerns ongoing training, in particular paramilitary training activities. In the past few years, paramilitary training activities of members of the transnational vXRW movement concentrated on locations in the United States, Central and Eastern Europe as well as the Balkans, while South African right-wing extremists have strengthened their connections to networks in the US and Europe and served as an inspiration.[27] Here a

Financing, CEP/Berlin Risk, 2020, https://www.counterextremism.com/sites/default/files/CEP-Berlin%20Risk_Policy%20Paper%20EU%20Crypto%20Currency%20Final.pdf
In 2021 the FATF released new draft guidance, which indicates significant progress. The draft text advises regulators to identify mixers, tumblers and other technologies that obfuscate transparency as high-risk, see: FATF, Draft updated Guidance for a risk-based approach to virtual assets and VASPs, 2021, page 16, https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf

[22] Möseneder, Michael; Schmidt, Colette M., Fünf Festnahmen und spektakulärer Waffenfund in rechtsextremer Szene, Der Standard, 13 December 2020, https://www.derstandard.de/story/2000122445163/fuenf-festnahmen-und-spektakulaerer-waffenfund-in-rechtsextremer-szene

[23] Hemmerling, Axel; Johanna Hemkentokrax, Johanna; Kendzia, Ludwig, Razzien gegen Neonazi-Netzwerk in Thüringen, Sachsen-Anhalt und Hessen, MDR, 26 February 2021, https://www.mdr.de/nachrichten/thueringen/razzia-neonazi-netzwerk-drogenhandel-turonen-garde-bruderschaft-100.html

[24] CEP XRW Report 2020, page 38.

[25] CEP is currently compiling and analyzing data concerning the financial activities of vXRW networks in Germany.

[26] FATF, Priorities for the Financial Action Task Force (FATF) under the German Presidency. Objectives for 2020-2022, page 2, https://www.fatf-gafi.org/media/fatf/documents/German-Presidency-Priorities.pdf

[27] Ware, Jacob, Transnational White Supremacist Militancy Thriving in South Africa, Council on Foreign Relations, 17 September 2020, https://www.cfr.org/blog/transnational-white-supremacist-militancy-thriving-south-africa

commercially driven weapons and paramilitary training infrastructure has developed which does not seem to deploy particular strict know-your-customer protocols when offering sensitive training services to foreigners.[28]

One particular aspect of this issue concern XRW foreign fighters that travelled to and took part in the conflict of Ukraine after 2014.[29] This conflict also increased the role and relevance of Central and Eastern European groups and networks for the transnational movement as a whole.[30] Many of these XRW foreign fighters have since returned home. Their military combat experience, coupled with their extremist ideologies, remain a serious concern.

Furthermore, the close connection of many networks within the movement to the MMA scene in Europe and the US[31] as well as the penetration of vXRW individuals in the professional security industry[32] may aid in the preparation for and perpetration of violence and therefore deserves further analysis.

In order to counter these activities, both common legal concepts as well as the further development of a range of legal and administrative measures is necessary. These could focus on disrupting travel of the respective individuals,[33] as well as increasing controls over access to arms, ammunitions, explosive material and their precursors.[34] Finally, greater clarity over potential financial flows towards these training facilities and the respective online content related to members of vXRW and terrorist networks could serve as an early warning mechanism.

II.V. P/CVE approaches: local, national, transnational

Common legal concepts, better control of the vXRW and terrorist online ecosystems, the disruption of financial, training and paramilitary training activities are important disruptive mechanisms. However, these measures and mechanisms should be integrated into a holistic policy strategy that also focuses on preventative measures. In this regard, many governments have gained considerable experience in measures preventing and countering Islamist extremism and terrorism.

Some states have also developed large scale C/PVE programs focused on vXRW and terrorism. For example, in recent years Germany ramped up its P/CVE effort, as its Ministry for Family Affairs, Senior Citizens, Women and Youth earmarked 460 million euros with the

[28] CEP highlighted this issue during a webinar in April 2021. For the presentations of this event, see: https://www.youtube.com/watch?v=tmocjdq46Z0&list=PLMgGq1NecSpZT08nubo9VaGaIWXGMykkR
[29] Rekawek, Kacper, Career Break or a New Career? Extremist Foreign Fighters in Ukraine, CEP, 2020, https://www.counterextremism.com/sites/default/files/CEP%20Report_Career%20Break%20or%20a%20New%20Career_Extremist%20Foreign%20Fighters%20in%20Ukraine_April%202020.pdf
[30] CEP XRW Report 2020, page 13ff.
[31] CEP XRW Report 2020, page 22.
[32] CEP XRW Report 2020, page 18.
[33] CEP XRW Report 2020, page 38.
[34] In this regard, the new EU regulation focusing on tighter controls of explosive precursors is a significant step. These controls could be brought to bear against this specific threat, see: Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1148&from=DE

priority of tackling right-wing extremism and antisemitism in the funding period 2020 to 2023.[35] On a multilateral level, discussions have also started to discuss this challenge. The Radicalisation Awareness Network (RAN) of the European Commission, a network of more than 6000 P/CVE practitioners,"[36] highlighted in its plenary session in October 2019 that "far-right extremism" was to be the top "cross-cutting issue" to be addressed in 2020.[37]

Therefore, considerable local, national and transnational learnings can be brought to bear on this issue. P/CVE approaches could be structured along the four P/CVE approaches and their combinations:

(1) **Legalistic Approach** (Criminal law/prosecution of specific offences and proscription/banning vXRW groups domestically and potentially multilaterally)
(2) **Community/Multi-Agency Approach** (Municipalities, including police and civil society organizations work together based on a shared understanding of the local phenomenon)
(3) **Administrative Approach** (Cross-agency/coordinated government interventions to disrupt vXRW actors, including their "legal" activities by e.g. investigating tax/building/fire code violations and connections to organized crime, as well as direct involvement in criminal activities such as the drug trade[38])
(4) **Civil Society Approach** (Information campaigns, documentation/analysis and counter-mobilization)

A multilateral discussion that takes stock of the various strategies, tactics and methods used in P/CVE approaches when countering violent Islamist extremism and terrorism and aims to analyze transferable lessons learned (positive as well as negative) seems of particular importance. Such a multilateral dialogue could support the further development of new or the amendment of existing P/CVE approaches to counter the threat posed by the transnational vXRW and terrorist movement and the networks, groups and individuals contained therein.

[35] Demokratie leben!, "Prävention von Rechtsextremismus und Antisemitismus stärken," https://www.demokratie-leben.de/zusatzseiten/praevention-von-rechtsextremismus-und-anti-semitismus-staerken.html
[36] See: Radicalisation Awareness Network (RAN), "About RAN," https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran_en
[37] Radicalisation Awareness Network (RAN), "Ex Post Paper. RAN Plenary," 30 October 2019, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/ran_plenary_brussels_30102019_en.pdf
[38] See arrests in Germany and Austria in December 2020 and February 2021 (cf. footnotes 21 and 22).

III. Conclusion

As outlined in this short paper, building on greater agreement concerning legal concepts will also have a positive effect on the ability to disrupt the online activities of the transnational movement, one of the integral mechanisms that enable the various stakeholders within the movement to communicate, cooperate and function transnationally.

Shared legal concepts will also support work towards a tighter control of the financial structures of vXRW and terrorist networks. Hindering these financial activities offers the opportunity to attack the networks within the movement at one of their strategic operations. Due to the misuse of internet services and tools for vXRW financing greater control over its online activities also can be a useful mechanism that can be brought to bear when attempting to pressure income streams of particular groups and networks within the movement.

One of the most concerning offline activities of vXRW actors are their paramilitary training activities as well as connections between vXRW and criminal networks. Both present significant potential security risks. Greater awareness of this issue and the development of appropriate countermeasures should be one of the priorities in an overall strategy countering vXRW.

Such an integrated strategy should also include a range of C/PVE measures and initiatives. In order to account for the unorganized structure of the leaderless, apocalyptic transnational vXRW and terrorist movement,[39] such measures and initiatives should involve the local, regional, national and transnational level. In order to further develop such a toolbox, lessons learned from similar work countering violent Islamist extremism and terrorism should be integrated.

The issues outlined in this short paper are clearly interconnected and common, multilateral measures that are potentially developed in these issue areas would be mutually reinforcing. Furthermore, work in any one of these issue areas will also be informative for the development of multilateral approaches in any of the other issue areas.

However, significant work still remains, in particular strengthening the common multilateral understanding that significant aspects of the transnational vXRW movement are related to terrorism[40] and the designation of respective networks and groups as terrorists on multilateral levels, including at the level of the EU.

Therefore, the work program outlined in this paper should be seen as a starting point for sustained multilateral discussions. The envisaged event series in 2021 will provide a springboard both for further research as well as enhanced policy discussions on how effective countermeasures as well as P/CVE mechanisms could be further strengthened, what adjustments may be necessary and which new mechanisms should be developed, particularly on a multilateral level.

[39] CEP XRW Report 2020, page 11f.
[40] CEP XRW Report 2020, page 6.