United Nations
Interregional Crime and Justice
Research Institute

Right- and left-wing violent extremist abuse of digital technologies in South America, Africa and Asia

Right- and left-wing violent extremist abuse of digital technologies in South America, Africa and Asia.

This document is co-published by the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the VOX-Pol Institute.

ISBN: 978-1-911669-76-0

Published in April 2025

Right- and left-wing violent extremist abuse of digital technologies in South America, Africa and Asia

Disclaimer

Acknowledgements

This report by the United Nations Interregional Crime and Justice Research Institute (UNICRI) was written by Arthur Bradley, UNICRI Consultant, under the overall guidance and editing of Ottavia Galuzzi, UNICRI. It is the product of a research initiative undertaken by UNICRI with the support of the VOX-Pol Institute. UNICRI expresses gratitude to all the members of the Group of Experts representing intergovernmental organisations, non-governmental organisations, the private sector, academia and law enforcement agencies who provided their insights in the data collection phase, especially through interviews, and their feedback during the review phase.

Particular thanks and appreciation are due to Professor Stuart Macdonald and Dr Suraj Lakhani at the VOX-Pol Institute, who provided feedback on the completed draft, and to other colleagues at VOX-Pol for their invaluable expertise and support.

Table of Contents

{ BACKGROUND }

The abuse of digital technologies by violent extremists is keeping pace with the exponential growth of new technologies, and poses multifaceted challenges to national and global security. Cyber-enabled threats manifest for example in terrorist-operated websites, the shift to alternative or fringe social media platforms, the use of the decentralised web, the exploitation of gaming and adjacent platforms, and the abuse of live-streaming technologies to amplify terrorist and violent extremist attacks. In addition to these online activities, there are concerns also around more disruptive or destructive cyber operations, such as Distributed Denial-of-Service attacks and the hacking of critical infrastructure to cause civilian casualties. In all the research on the diverse range of malicious actors behind these threats, there is comparatively little on the online activity of violent extremist movements, whether right-wing or left-wing, in the Global South.

This report forms part of UNICRI's effort to investigate the threats stemming from the complex interplay between terrorism, violent extremism and cybercriminality – threats that are often overlooked, owing to the difficulty of gathering evidence and attributing offensive cyber operations, and to the prioritisation of more pressing security threats in diverse geographic locations. UNICRI strives to shed light on the online presence, activities and trends of right- and left-wing violent extremist movements and the cyber-enabled threats they may consequently pose to global security. The report was compiled following a three-part research methodology consisting of a literature review, expert interviews and open-source investigations conducted in order to analyse the online activities of right- and left-wing violent extremist movements in South America, Africa and Asia, and examining both their intent and ability to mount offensive cyber-attacks.

The report includes particular case studies within these regions, including in Brazil, South Africa, India and Maritime South-East Asia. The case studies were selected because of the availability of public information online, the known presence of active non-state violent extremist actors with right- and left-wing ideologies, the similarities and differences these actors present, and their geographic diversity. These factors, and consequently the choice of case studies, demonstrate the global nature of the phenomenon which still requires contextually relevant solutions.

The selection of these case studies does not imply that similar threats in other geographies are not considered relevant to international peace or development, and conversely, the omission of any movements is merely the result of restricted resources and time. The groups and movements presented within this report are not necessarily referenced as violent extremists either by the United Nations or by the Member States mentioned, however, their alignment, proximity, and connection with right- and left-wing violent extremist ideologies, as well as their use of violent extremist tactics, justify mention in this report to ultimately reflect on the global dimension of the abuse of digital technologies by violent extremists.

The report is published by UNICRI in partnership with the VOX-Pol Institute, which was founded in 2024 on the success of the world-leading VOX-Pol Network of 80+ academics from more than 30 universities worldwide. The VOX-Pol Institute combines academic research with open-source data to provide actionable and policy-relevant research and training for policymakers, law enforcement agencies and technology companies, enhancing their responses to terrorism and extremism online.

{ EXECUTIVE SUMMARY }

This report finds widespread exploitation of digital platforms by right- and left-wing violent extremists based in South America, Africa and Asia. Groups and their affiliated networks use a wide variety of platforms and services for a range of different purposes, and they often seem to face fewer restrictions in terms of content moderation by technology companies, many of which are based in the United States or European countries. In particular, it found:

- As in Europe, North America, and Australasia, the online activities of right- and left-wing violent extremist groups in South America, Africa and Asia are increasingly superseded by more disparate, horizontal online networks. In many of the case studies, for example in Brazil and India, physical attacks have increasingly been carried out by lone actors or small cells, some of which may have had previous engagement with organised groups. This dynamic has implications for the ability of technology companies and law enforcement agencies to counter the threat, as planned attacks and their perpetrators may be more difficult to prevent or identify.

- Violent extremist networks and individuals are increasingly using a more diverse range of online platforms and services to further their goals. This is in line with the increase in the number of online platforms and services used by broader populations generally, but it may also be part of a concerted effort by these networks to reach a broad audience and mitigate the impact of the potential removal of their accounts or groups by technology companies. Violent extremist networks continue to exploit multiple platforms simultaneously, using outlinking between platforms to evade detection or enforcement by specific companies.

- Violent extremists comprise the minority of the perpetrators delivering cyber-attacks globally, most of which are believed to be carried out by state-backed actors, hacktivist collectives, or financially motivated criminals. Interviews with a group of 31 experts consulted as part of this research, however, indicate that the threat from cyber-attacks motivated by a belief system and delivered by individuals or groups affiliated with violent extremist movements is likely to increase in the coming years, and is likely to be particularly high in countries believed to have less developed cybersecurity defences.

- This report suggests that international technology companies are not adequately fulfilling their content moderation policies as consistently in South America, Africa and Asia as in other countries in Europe, North America, and Australasia. Also, they do not appear to be allocating sufficient resources to ensuring platform safety in

these regions, where they face significant challenges in effectively countering the exploitation of their services by violent extremist movements. Practical challenges are compounded by definitional challenges regarding contentious terms such as "violent extremism" and "terrorism", neither of which has an internationally agreed definition.[1]

- Also, technology companies, it seems, still struggle to detect and understand violent extremist content or communications effectively in languages other than English. This task is made more difficult by the challenge of interpreting and understanding local dynamics and the community-specific slang found in content, and by the efforts of malevolent networks to evade detection or enforcement by moderation teams. Evidence suggests that, to date, this – together with an imbalance in resource allocation – means that the capability of many technology companies to moderate content in languages other than English is comparatively ineffective.

- Often, a splintered regulatory landscape also makes it difficult for technology companies to apply their policies consistently across multiple jurisdictions around the world. Technology companies operating globally are subject to a variety of differing and often contradictory regulatory requirements, including those relating to designations, hate speech legislation and Internet-related laws, and companies can be under pressure from the political or cultural contexts in particular countries. This can make it difficult for these companies consistently and effectively to maintain a balance between removing violative content and upholding human rights and fundamental freedoms.

The report focuses on a set of case studies diving into the online activities of right- and left-wing violent extremist groups in South America, Africa and Asia, and the ways in which they abuse digital technologies.

- The case study of the nihilist 'eco-terrorist' group Individualistas Tendiendo a lo Salvaje (ITS) gives an instructive insight into the exploitation of digital platforms by a group with links to the international violent left-wing anarchist movement. The group has claimed to have been responsible for a succession of bombings and other violent attacks across South America and Europe, including in Mexico, Chile, Brazil and Greece since 2011. Its core membership operated a sophisticated digital infrastructure on the deep and dark web, including propaganda websites, cryptocurrency crowdfunding, and internal communication through a private chat platform. While the group's primary online presence appears to have largely diminished in recent years, its propaganda remains available elsewhere online.

1 While there is no formal definition of "terrorism", the United Nations Security Council has designated specific groups and defined different "acts" of terrorism. Further information is available at: https://main.un.org/securitycouncil/en/sanctions/information.

- Right-wing violent extremism has emerged in the Brazilian context of long-standing domestic neo-Nazism and militarism with influences from right-wing extremist movements globally, particularly in the United States. There have been several attacks by right-wing violent extremist lone actors in Brazil in recent years, including on schools, and plots involving more organised groups have been reported. The digital ecosystem of right-wing violent extremism in Brazil is extensive and reportedly growing, particularly via messaging apps, social media, and chan sites. There are also connections between domestic right-wing extremism and international disinformation networks, in particular regarding the Duginist Nova Resistência group.

- The right-wing violent extremist threat posed by white supremacist groups in South Africa has lessened since the 20th and early 21st century. Despite a decline in popular support, however, extremists there have increasingly turned to digital technologies to recruit, to socialise and to propagate their ideologies. Prominent groups such as the Suidlanders maintain a significant online presence via social media, websites, bespoke apps and encrypted messaging platforms. South African right-wing violent extremists are increasingly forging international connections, and domestic political and security issues in South Africa have inspired right-wing violent extremism elsewhere, including, for example, in a mass shooting at a predominantly black church in June 2015 in Charleston, United States.

- There is a wide-reaching and sophisticated online network of actors and groups that subscribe to a right-wing violent extremist form of Hindutva ideology in India. Hindutva is an ideological and cultural concept focused on "Hindu-ness" or the essence of being Hindu. It predates but is often associated with the ideology espoused by former and existing political parties, such as – among others – Shiv Sena and the Bharatiya Janata Party (BJP) in India. However, the same concept has been appropriated by extremist groups to justify and promote their agendas. These groups and actors maintain a vast online presence on mainstream and niche websites, platforms and messaging apps, using them to spread propaganda and misinformation and to mobilise supporters. The rise of more niche and unregulated platforms, such as chan sites, along with the operations of Hindutva-aligned hacking groups, underscores the growing sophistication and cyber capabilities of this form of right-wing extremism, in particular online harassment and cyber-attacks. For the purposes of this report, any references to 'Hindutva' pertain exclusively to the violent and extremist interpretations of the ideology, as distinct from broader political or cultural movements in India.

- The threats posed by left-wing violent extremist movements in India, such as those of the Naxalites and CPI-Maoist, have diminished in recent years thanks to coun-

ter-insurgency operations and waning popular support, but they nonetheless demonstrate consolidated experience of abusing digital technologies in their favour. Online networks affiliated with the CPI-Maoist, for instance, disseminate its ideologies via websites and blogs, all with different top-level domains (TLDs), but redirecting to the main website and mitigating the impact of takedowns of specific sites. There are documented examples of CPI-Maoist members relying on encryption solutions, such as Pretty Good Privacy and Protonmail, to encrypt their communications, thereby posing challenges to law enforcement investigations.

- Right-wing extremism in South-East Asia is a relatively understudied phenomenon in a region that has historically focused on the more prominent threat posed by groups affiliated with terrorist organisations like Islamic State in Iraq and the Levant (ISIL/Da'esh) and Al-Qaida. Recent research, however, has highlighted nascent digital networks of right-wing extremists, inspired by local dynamics combined with the influence of right-wing extremists in North America and Europe. The diversity in the ideologies of these networks reflects the diversity of general populations across the region, but they can include elements of Muslim nationalism, anti-Rohingya or anti-Muslim prejudice, Buddhist ultranationalism, anti-Semitism, and support for authoritarianism. The networks have been shown to operate on mainstream platforms like X, Facebook, Instagram and TikTok. Several nationalist hacktivist groups are also active in the region, although their connection to potentially more violent actors is unclear.

{ INTRODUCTION }

In line with UN Security Council resolutions 2178 (2014),[2] 2396 (2017)[3] and the Delhi Declaration,[4] UNICRI is committed to countering terrorist and violent extremist exploitation of information communications technology (ICT), and to ensuring that this technology remain a force for good, by means of action-oriented research, capacity-building activities, and technical assistance to Member States on emerging threats. The focus of this study is aligned with UNICRI's commitment to exploring how terrorism and violent extremism manifest online, the offline implications of this in diverse cultural contexts, and potential collaboration with other malicious actors, relying and building on evidence gathered in correlated UNICRI research. Recently, UNICRI and UNOCT jointly published a report on the terrorist and violent extremist use of the dark web and Cybercrime-as-a-Service, and their role in revolutionizing the cybercrime landscape and facilitating cyber-enabled terrorist and violent extremist attacks.[5]

To further our understanding of violent extremism online, both globally and in particular geographies, through this research UNICRI has investigated the online presence, activities and trends of right-wing and left-wing violent extremist movements in South America, Africa and Asia, and the cyber-enabled threats to national security and global stability. Among the diverse range of malicious actors behind these threats, comparatively little has been published about the online activity of right-wing and left-wing violent extremist movements in South America, Africa or Asia, unlike those in Europe, North America, Australia and New Zealand. Right- and left-wing violent extremism is not confined to the Global North, and growing trends show that, often, locally contextualised narratives and propaganda are proliferating in the Global South, forging connections to the broader right-wing and left-wing violent extremist movements.[6] The live-streamed attack in August 2024 in a tea garden in Eskisehir, Turkey, is a recent example of this trend.[7]

2 United Nations Security Council, Resolution 2178 (2014), https://documents.un.org/doc/undoc/gen/n14/547/98/pdf/n1454798.pdf.

3 United Nations Security Council, Resolution 2396 (2017), https://documents.un.org/doc/undoc/gen/n17/460/25/pdf/n1746025.pdf.

4 United Nations Security Council Counter-Terrorism Committee, Delhi Declaration, 2022, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Dec/english_pocket_sized_delhi_declaration.final_.pdf.

5 "Beneath the surface: terrorist and violent extremist use of the dark web and cybercrime-as-a-service for cyber-attacks", UNICRI, *UNOCT/UNCCT*, 2024, available at: https://unicri.it/sites/default/files/2024-07/DW_BtS.pdf.

6 Gaby Tejeda, "Far-Right Extremism Is Also a Growing Problem Throughout the Global South", The Soufan Center, 30 August 2024, available at: https://thesoufancenter.org/intelbrief-2024-august-30/.

7 Arthur Bradley, "'Dead society': Tracing the Online Dimension of a Militant Accelerationist-Inspired Attack in Turkey", GNET Insights, 2024, available at: https://gnet-research.org/2024/08/16/dead-society-tracing-the-online-dimension-of-a-militant-accelerationist-inspired-attack-in-turkey/.

This research aims to provide valuable insights and recommendations for policymakers, law enforcement, civil society practitioners, technology companies and other stakeholders on the cyber-enabled threats posed by right- and left-wing violent extremist movements in South America, Africa and Asia. It focuses on the abuse of digital technologies by these movements through a set of regional case studies, which look at right-wing violent extremism in Brazil, South Africa, India and South-East Asia; and left-wing violent extremism in Mexico, Chile, Brazil, Argentina and India. The research explores and analyses in particular the use of social networking platforms to spread propaganda; the exploitation of privacy-focused applications to communicate internally and engage in operational planning; soliciting donations via the use of cryptocurrency and crowdfunding platforms; the acquisition or sale of goods and services on digital platforms; the abuse of Internet infrastructure to host violent extremist-operated static websites; and the abuse of digital technologies to mount disruptive or destructive offensive cyber operations. It also aims to highlight the platforms most used by such movements in these regions, and it assesses the potential for their collaboration with other malicious actors in cyberspace, such as financially motivated criminals and hacktivist collectives. It also puts forward recommendations and suggests measures for identifying, investigating, preventing and disrupting such cyber-enabled threats.

Definitions

The growing and increasingly transnational threats posed by violent extremist groups are amplified by the use of the Internet and other digital technologies, as underscored in the recent Security Council high-level open debate on "Maintenance of international peace and security: addressing evolving threats in cyberspace".[8] In this regard, multistakeholder cooperations involving Member States are essential, to ensure that violent extremists do not find a safe haven online and to promote a free, open and secure Internet that respects human rights and fundamental freedoms.

8 Open debate in connection with "Addressing evolving threats in cyberspace" under the Security Council's agenda item "Maintenance of international peace and security", *UN Web TV*, 2024, video available at: http://webtv.un.org/en/asset/k1c/k1cifeuu9g.

While there is no internationally agreed definition of the term 'violent extremism', the United Nations Secretary-General's "Plan of action to prevent violent extremism" calls the term a complex one, and says that defining it is ultimately the prerogative of Member States. Such definitions must also be consistent with country obligations under international law, in particular human rights law. However, violent extremism has affected different societies in different regions of the world, and "it is driven by a mixture of personal, societal, and ideational factors whose manifestations vary from one individual to the next".[9] For the purposes of this research, the definition of violent extremism proposed by the United Nations Educational, Scientific and Cultural Organization (UNESCO) is used: "the beliefs and actions of people who support or use violence to achieve ideological, religious or political goals", including "terrorism and other forms of politically motivated and sectarian violence".[10] In this study, 'violent extremism' will be used predominantly to refer to non-state armed groups and affiliated online networks, although in several instances these groups and networks may consider themselves allied with, or otherwise linked to, state entities.

Both the United Nations General Assembly and the Security Council have stressed the need to prevent and counter violent extremism as and whenever it is conducive to terrorism. Terrorism is described in the United Nations Security Council resolution 1566 (2004) as "criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organisation to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism".[11] Violent extremism refers to a combination of ideology and violence, and encompasses a broader range of violent activities, including terrorism. The eighth review of the Global Counter-Terrorism Strategy (A/RES/77/298) condemns terrorist acts, including those committed "on the basis of xenophobia, racism and other forms of intolerance, or in the name of religion or belief",[12] calls upon Member States to take appropriate measures to address the growing frequency of these attacks, and takes note of a report prepared by the Secretary-General (A/77/266) which called for further research in order to understand better the motivations, objectives and organisation of the individuals and groups conducting attacks on such a basis, and the threat they pose.[13]

9 "Plan of action to prevent violent extremism", *United Nations General Assembly*, 2015, available at: https://documents.un.org/doc/undoc/gen/n15/456/22/pdf/n1545622.pdf.

10 "Preventing violent extremism through education: A guide for policymakers", *UNESCO,* 2017, available at: https://unesdoc.unesco.org/ark:/48223/pf0000247764.

11 "Resolution 1566 (2004) / adopted by the Security Council at its 5053rd meeting, on 8 October 2004", available at: https://digitallibrary.un.org/record/532676?ln=en&v=pdf.

12 "The United Nations Global Counter-Terrorism Strategy: eighth review", *United Nations General Assembly,* 2023, available at: https://documents.un.org/doc/undoc/gen/n23/189/01/pdf/n2318901.pdf.

13 "Report of the Secretary-General: Terrorist attacks on the basis of xenophobia, racism and other forms of intolerance, or in the name of religion or belief", *United Nations General Assembly*, 2022, available at: https://documents.un.org/doc/undoc/gen/n22/450/52/pdf/n2245052.pdf.

Nor are there any universally accepted definitions of either right- or left-wing violent extremism (also broadly referred to as 'far-right extremism'; 'far-left extremism'; 'extreme right-wing'; 'extreme left-wing'). Key characteristics of right-wing violent extremism typically include violence motivated by ultranationalism, racism, xenophobia, opposition to democracy, or advocacy of a strong state.[14] Key characteristics of left-wing violent extremism, on the other hand, include violence motivated by extreme anti-democratic and anti-capitalist beliefs, a focus on perceived injustices, and a treatment of the values of freedom or social equality as being absolute.[15] The violent non-state actors analysed here exhibit some or all these characteristics, and for the purposes of this report will be referred to as right-wing or left-wing violent extremist groups or individuals. Both forms of extremism are heterogeneous, however, and the manifestations and definitions of both, and the way in which their definitions are applied, are likely to differ depending on the national or regional context.

It should be noted that the report's scope and findings do not imply that there is a consensus among the international community that the terminology adopted in this report should have universal application, or that the Member States referenced in the case studies automatically accept that the adopted terminology and definition fully reflect the emerging and existing threats in their countries. As Member States use different language to describe the violent non-state actors active within their territories, this publication does not imply the expression of any opinion on its contents or by the Member States mentioned. This report does not seek to enter the debate of which groups are listed as violent extremists or not internationally. The scope is to bring to the forefront cases of exploitation of digital technologies by groups or individuals aligned with or supporting right-wing or left-wing violent extremist ideologies.

14 Cas Mudde, "The Far Right Today", *Wiley,* 2019; "Terrorist attacks on the basis of xenophobia, racism and other forms of intolerance, or in the name of religion or belief", *United Nations General Assembly A/77/266,* August 2022, available at: https://documents.un.org/doc/undoc/gen/n22/450/52/pdf/n2245052.pdf?token=WdVpxIaQHNMl6gmSL4&fe=true.

15 Francesco Farinelli and Lorenzo Marinone, "Contemporary Violent left-wing and anarchist extremism (VLWAE) in the EU: Analysing threats and potential for P/CVE", *Radicalisation Awareness Network,* 2021, available at: https://home-affairs.ec.europa.eu/system/files/2021-11/ran_vlwae_in_the_eu_analysing_threats_potential_for_p-cve_112021_en.pdf; "Left-wing extremism", *Bundesamt Verfassungsschutz*, available at: https://www.verfassungsschutz.de/EN/topics/left-wing-extremism/left-wing-extremism_node.html.

{ METHODOLOGY }

The findings presented in this report have been arrived at using a three-part methodology, consisting of interviews with a Group of Experts with specific expertise in the regions and topics of concern. The Group of Experts comprised 31 individuals from law enforcement agencies, non-governmental organisations, academia, intergovernmental organisations, and the private sector. In terms of their areas of specific expertise, 13 of the experts were global specialists in technology and violent extremism, 6 had regional expertise in South America, 3 in South Africa, 7 in Asia, and 2 in cybersecurity. The interviews were conducted in June and July 2024. Interviewees could choose whether or not their contributions would be directly cited in the report. The VOX-Pol Institute was instrumental in identifying and involving expert individuals in the Group of Experts, providing academic review and guidance throughout the research project, and supporting the dissemination of the report.

The report is also based on an extensive review of relevant literature on violent extremism in the regional and national contexts of concern, of the abuse of digital technologies, and of responses by the technology sector to these threats. These findings were supplemented by open-source investigations conducted into the online activities of these groups, movements and digital networks, to illustrate the findings of the interviews and literature with up-to-date, primary data.

The open-source investigations were conducted on various platforms and websites on the surface web, deep web and dark web. Platforms that were examined in the research included social media, messaging apps, file-sharing services, stand-alone websites, video-sharing platforms, and forums. Investigations were conducted initially using keywords, hashtags, phrases and other indicators commonly used by or associated with the entities being studied. These were obtained from academic articles and press reports, mainly in the native or commonly used languages of the groups or networks being researched. Where required – such as on social media networks, messaging apps or member-only forums – access was achieved using anonymous accounts. These accounts were used to collect essential data for the research objective anonymously. For ethical reasons, they did not pose as real people, nor as supporters or members of the movements under scrutiny. Digital spaces were considered for research only if they displayed an obvious affiliation with these movements and could be accessed using open-source methods, which meant that the investigation did not involve interaction, or any other form of engagement, with any other users at any stage of the research.

This report includes several images: screenshots taken as examples of content analysed in the research. Sections of these images have been redacted for data protection and ethical reasons – to protect the identities of individuals present in the images, and to reduce the risk that their inclusion in this report might unintentionally contribute to greater primary visibility online for the content. For content that was sourced from surface web spaces, aspects of images that could serve to make the content more discoverable, such as particular usernames or key phrases, have been removed. Content likely to be illegal in the jurisdiction in which it originated, and which

was covered in this report, was reported to the relevant technology company and national law enforcement agencies before the report was published, at least in the cases where contact details could be identified.

The basis for selecting cases to research was the presence of right- or left-wing violent extremist movements in countries within the regions in scope, and their exploitation of digital technologies as documented in third-party research. Their similarities and differences in ideologies, online presence and activities represent another indicator for the selection of the case studies, as they showcase the global nature of the phenomenon while outlining the specificity of different geographical contexts requiring tailored regional approaches and support to national governments. Finally, the case studies were selected because of the amount of publicly available information, facilitating a thorough review of relevant literature on violent extremism in the regional and national contexts of concern, and their geographical diversity. The case studies selected are not intended to represent a comprehensive study of violent extremist movements in these countries or regions – they were included to provide insights into potential trends in the intent and the capability of right- and left-wing violent extremist movements there to exploit digital technologies, and into the responses to this exploitation by both the technology and public sectors. The case studies comprise contextual overviews and analysis relating to known, active non-state violent extremist actors with right-wing and left-wing ideologies in South America, Africa and Asia, and aim to demonstrate their online presence, their activities, and the nature of the cyber-enabled threats they potentially pose. The selection of these case studies does not imply that similar threats in other Member States are not considered relevant to international peace or development, and conversely, the omission of any movements is merely the result of restricted resources and time.

This report is part of a larger workstream UNICRI leads, aimed at preventing and countering terrorism and violent extremism and their convergence with cybercrime and abuse of digital technologies. As such, this study has been exploratory in nature, and any information presented is indicative of potential trends and developments in South America, Africa and Asia. Further research is required to develop a complete threat picture, both in these regions and in the Global South in general.

{ VIOLENT EXTREMIST ABUSE OF DIGITAL TECHNOLOGIES }

The violent extremist activities described in this section can be classified as indirect 'enablers' of militancy, meaning that they tend not to be directly associated with acts of political violence, but they do play a key role in indirectly furthering violent extremist objectives such as recruitment and the amplification of attacks, via published footage or other forms of propaganda campaigns, in both the physical and digital domains. Examples of enabling actions include propaganda sharing, internal communication, and financing.[16] The category of 'enabling' has probably been the most widely studied aspect of violent extremist exploitation of digital platforms and technologies. This report also aims to investigate two other categories of digital abuse, namely, 'disruptive' and 'destructive' cyber operations, which are described and discussed further down in the report.

CATEGORY OF DIGITAL ABUSE	EXAMPLES
 **Enabling Actions**	Recruitment, radicalisation, planning, financing, incitement, threats, internal communication
 **Disruptive Cyber Operations**	Web defacement, data breaches, DDoS attacks, hacking of social media accounts or emails, phishing attacks
 **Destructive Cyber Operations**	Malicious software, code injection attacks, botnets, access vulnerabilities, zero-day exploits

A complex digital ecosystem

This study has found few fundamental differences in the ways violent extremist actors in the Global South and the Global North abuse digital technologies to further their objectives. Globally, violent extremist groups and networks exploit a broad variety of platforms and services simultaneously, including for propaganda, recruitment, financing, planning and internal communication. This study has broadly found, however, that there is significant scope for improvement in the response of the global technology sector to violent extremist movements in South America, Africa and Asia as opposed to those operating from European and North American countries, particularly when it comes to non-English-language content.[17]

16 Jonalan Brickey, "Defining cyberterrorism: capturing a broad range of activities in cyberspace", *CTC Sentinel,* Vol. 5, Issue 8, August 2012, available at: https://ctc.westpoint.edu/wp-content/uploads/2012/08/CTCSentinel-Vol5Iss81.pdf.

17 Based on responses from a majority of the 31 experts consulted for this study, alongside literature review and case studies, such as the 2021 Facebook files.

Unlike in regions such as North America and Europe, the exploitation of digital technologies by violent extremist movements in some parts of South America, Africa and Asia is taking place amid a rapid increase in Internet penetration and in the extent of usage by general populations there. In India, for example, there were 750 million active Internet users as of June 2024, representing a 43% increase since 2019.[18] Across the South American continent, Internet penetration rose from 43% to 78% between 2013 and 2023,[19] and in South Africa, 78% of individuals were using the Internet by 2024.[20] The increase in Internet availability and usage is likely to increase the risk of exploitation by hostile actors based in these regions, including violent extremists.

While historically the online threat posed by violent extremists was predominantly characterised by structured, named organisations, it increasingly consists of more fluid, horizontal digital structures. Relatedly, violent attacks have increasingly been carried out by lone actors or small cells that had previously engaged with extremist organisations or online communities, rather than by members of hierarchical organisations.[21] These wide-reaching digital ecosystems are more difficult to track than cohesive organisations, and the agile nature of their exploitation of digital platforms makes them more challenging to counter. In addition, they exist as part of an increasingly congested information environment, in which different online harms – including misinformation, disinformation, cybercrime, and Child Sexual Abuse material (CSAM) – increasingly overlap with violent extremism in digital spaces.[22]

Over the past decade there has been a diversification in the use of online platforms for external messaging by violent extremist actors. In the early days of social media, most violent extremist groups – like the general population – typically used only a few platforms fluently. Today, many such groups and networks operate for a variety of purposes on multiple different apps and platforms, including social networking platforms, messaging apps, crowdfunding services, file-sharing platforms, video-sharing platforms, gaming services, static websites, forums and

18 Astha Rajvanshi, "How Modi's supporters used social media to spread disinformation during the elections", Time, 3 June 2024, available at: https://time.com/6984947/india-election-disinformation-modi/.

19 "Latin America Digital Report 2023", Atlántico, 30 August 2023, available at: https://www.atlantico.vc/latin-america-digital-transformation-report-2023.

20 "The ICT Development Index 2024", International Telecommunication Union Publications, 2024, available at: https://www.itu.int/dms_pub/itu-d/opb/ind/d-ind-ict_mdd-2024-3-pdf-e.pdf

21 Raffaello Pantucci, Clare Ellis and Lorien Chaplais, "Lone-actor terrorism: Literature Review", The Royal United Services Institute, Universiteit Leiden, Chatham House, and the Institute for Strategic Dialogue, December 2015, available at: https://www.chathamhouse.org/sites/default/files/publications/research/20160105LoneActorTerrorismLiteratureReviewRUSI.pdf.

22 Interview with Nicole Matejic, Charles Sturt University, 12 June 2024; Interview with Anne Craanen, Swansea University, 11 June 2024.

message boards, on the surface, deep and dark web.[23] There is a growing tendency among these threat actors to use voice messages and audio content, which are harder to scan and analyse than text-based content.[24]

Violent extremist actors often exploit several services simultaneously, to maximise their audience size and mitigate the potential impact of account suspensions on particular platforms.[25] For instance, these threat actors split their communication into different platforms, sharing the first part of a message in one channel and the second part in a channel on another platform – making it difficult for technology companies and relevant law enforcement authorities to monitor or take action comprehensively against this type of communication.[26] Threat actors who face particular pressure from the authorities and the technology sector are increasingly quick to respond to suspensions, invariably changing their tactics and behaviours to evade further bans.[27] Violent extremists commonly link within and across platforms, using URLs to direct prospective supporters to their dissemination spaces elsewhere online. This indicates the need for cross-company coordination and information sharing, to disrupt and mitigate the threat effectively.

Despite the heightened focus on the potential exploitation of emerging technologies by nefarious actors, and their use of popular contemporary digital platforms, the long-standing exploitation of traditional static websites remains a persistent and largely unresolved issue.[28] Violent extremist actors have used websites for propaganda and communication since the early days of the Internet,[29] but decades later websites continue to play an important role in the broader ecosystem, serving as stable locations in which to host these actors' audiovisual propaganda, documents and blog posts, to fundraise, and to direct visitors to their online presence on other platforms.[30]

Web infrastructure providers tend to require high evidential and legal thresholds before taking

23 Interview with Erin Saltman, Global Internet Forum to Counter Terrorism (GIFCT), 4 July 2024; Interview with Leonardo F. Nascimento, Digital Humanities Laboratory at the Universidade Federal da Bahia, 9 July 2024; Stuart Macdonald, Kamil Yilmaz, Chamin Herath, J.M. Berger, Suraj Lakhani, Lella Nouri, & Maura Conway, "The European Far-right Online: An exploratory Twitter outlink analysis of German & French far-right online ecosystems", *Revolve Network,* May 2022.

24 Interview with Civil Society Representative, 14 June 2024.

25 Interview with the Organization for Security and Cooperation in Europe (OSCE), 20 June 2024.

26 Interview with Law Enforcement Representative, 16 July 2024.

27 Deeba Shadnia, Alex Newhouse, Matt Kriner and Arthur Bradley, "Militant Accelerationist Coalitions: A Case Study in neo-fascist accelerationist coalition building online", Center on Terrorism, Extremism and Counterterrorism at the *Middlebury Institute of International Studies at Monterey, Tech Against Terrorism and the Accelerationism Research Consortium,* June 2022, available at: https://www.middlebury.edu/institute/sites/default/files/2022-06/REDACTED%20CTEC__TAT%20Accelerationism%20Report%20.pdf?fv=I1W5uR6y.

28 "The threat of terrorist and violent extremist-operated websites", *Tech Against Terrorism,* January 2022, available at: https://www.techagainstterrorism.org/hubfs/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022-1.pdf; Arthur Bradley and Deeba Shadnia, "Examining online migration to terrorist and violent extremist domains", *Program on Extremism, George Washington University and Tech Against Terrorism,* July 2022, available at: https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/Examining_Online_Migration_to_Terrorist_and_Violent_Extremist-Owned_Domains_TATFinal.pdf; Maura Conway and Seán Looney, "Back to the future? Twenty first century extremist and terrorist websites", *Radicalisation Awareness Network,* 2021, available at: https://home-affairs.ec.europa.eu/document/download/0bdb9d9f-8853-491d-aa31-04889fffefcc_en?filename=Terrorist%20Operated%20Websites%20Workshop-paper.pdf.

29 "www.terror.net: How modern terrorism uses the internet", *United States Institute of Peace,* March 2004, available at: https://www.usip.org/sites/default/files/sr116.pdf; "Stormfront", *Southern Poverty Law Center,* available at: https://www.splcenter.org/fighting-hate/extremist-files/group/stormfront.

30 Ibid.

action on such sites, and have often been reluctant to act even in cases where there appears to be a threat to human life.[31] Attempts to disrupt violent extremist websites at the domain level can be even more challenging when this work crosses borders, for example when a violent extremist actor deliberately chooses to register and host its website in a jurisdiction where it is not violating the law.

External Messaging

Right- and left-wing violent extremists have long exploited digital technologies for external messaging, including to spread propaganda and disinformation, issue threats, recruit, and intimidate the perceived 'out-group'.[32] According to Europol, "the use of technology and the Internet – including social media platforms, instant messaging applications, online forums, and video gaming platforms – continues to play a crucial role in the radicalisation and recruitment process of individuals and in spreading propaganda material, arguably across the entire ideological spectrum".[33] These online propaganda ecosystems can often take the form of 'echo chambers' – communities in which individuals only hear narratives that they already agree with, or news stories that reinforce their worldview. Research has shown that this phenomenon applies particularly to those who are politically active, at both ends of the political spectrum. Violent extremist narratives on both sides are likely to exploit these ecosystems to recruit and to spread their narratives.[34]

Several aspects of violent extremist use of digital technologies have remained largely unchanged over the past five years, such as the heavy use of Telegram, a privacy-focused messaging app that offers its users varying degrees of anonymity.[35] Despite Telegram's attempts to mitigate the

31 Ben Makuch, Mack Lamoureux and Joseph Cox, "Cloudflare is protecting a site linked to a neo-Nazi terror group", Motherboard, 7 August 2019, available at: https://www.vice.com/en/article/j5yxxg/cloudflare-is-protecting-a-site-linked-to-a-neo-nazi-terror-group; Tasneem Akhtar, "Cloudflare and the Daily Stormer: Content moderation meets the stack", Trust & Safety Foundation, March 2022, available at: https://trustandsafetyfoundation.org/blog/cloudflare-and-the-daily-stormer-content-moderation-meets-the-stack/.

32 "EU Terrorism Situation and Trend Report", Europol, March 2007, available at: https://www.europol.europa.eu/cms/sites/default/files/documents/tesat2007_1.pdf; "EU Terrorism Situation and Trend Report 2016", Europol, July 2016, available at: https://www.europol.europa.eu/cms/sites/default/files/documents/europol_tesat_2016.pdf.

33 "Terrorism Situation and Trend Report 2023", Europol, October 2023, available at: https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf; Suraj Lakhani, "When Digital and Physical Worlds Combine: The Metaverse and the Gamification of Violent Extremism", Perspectives on Terrorism, XVII: 2: 108-125, 2023, available at: https://pt.icct.nl/sites/default/files/2023-06/PT%20-%20Vol%20XVII%2C%20Issue%20II%20-%20June%202023%20A6.pdf.

34 Thor Benson, "The small but mighty danger of echo chamber extremism", Wired, 20 January 2023, available at: https://www.wired.com/story/media-echo-chamber-extremism/.

35 "What is Telegram?", available at: https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here.

use of its services by violent actors, including in coordination with law enforcement agencies,[36] violent extremism appears to continue proliferating there.[37] Violent extremists also remain intent on spreading their messages on the largest social networks, probably because these are where they can reach a mainstream audience.[38]

Large social networking companies have made overall improvements to their ability to detect and take effective action against violent extremist content, compared with several years ago, but malevolent actors continue to operate on these networks, with varying degrees of sophistication in the tactics they use to evade detection. In South America, communications by violent extremist groups and their members have increasingly shifted from paper pamphlets to digital messaging, including in private encrypted spaces such as WhatsApp and Telegram,[39] as well as in more public digital spaces like TikTok, X, Instagram, YouTube and Facebook. Open-source investigations conducted as part of this research suggest that many of the right- or left-wing violent extremist networks on larger platforms in South America, Africa and Asia can evade moderation without the need for any sophisticated tactics, unlike their more consistently disrupted equivalents in North America, Europe and Australasia. For those more regularly facing disruption by technology companies, common evasion tactics include replacing characters in keywords, using in-group slang or 'dog whistles' to hide violent extremist intent, or editing video so that automated systems fail to detect it.

Extremist messaging and mobilisation also have a close relationship with mainstream news media. A common extremist approach is to share mainstream news items that appear to support extremist ideas, while ignoring those that do not; or to create extremist media outlets that present themselves as legitimate news media online.[40] This blurring of the lines between legitimate and extremist outlets can contribute to a blurring of the lines between mis- and disinformation, conspiracy theories and violent extremism. Such a dynamic was present during the attack on the Capitol building in Brasília, Brazil, in January 2023, when thousands of demonstrators attacked government buildings, fuelled by false or conspiratorial narratives on digital platforms alleging election fraud.[41] There have been several other similar instances of misinformation-fuelled extremist violence in recent years.

36 "Europol and Telegram take on terrorist propaganda online", *Europol,* 25 November 2019, available at: https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.

37 Jakob Guhl and Jacob Davey, "A safe space to hate: white supremacist mobilisation on Telegram", *Institute for Strategic Dialogue,* 26 June 2020, available at: https://www.isdglobal.org/wp-content/uploads/2020/06/A-Safe-Space-to-Hate2.pdf.

38 Interview with Charley Gleeson, Extrac, 10 June 2024.

39 Interview with Camilo Tamayo Gomez, University of Huddersfield, 8 July 2024.

40 Dr Melissa-Ellen Dowling, "Bad news travels fast: the co-optation of mainstream media to promote radical and extremist ideologies online", *VOX-Pol,* 10 April 2024, available at: https://voxpol.eu/bad-news-travels-fast-the-co-optation-of-mainstream-media-to-promote-radical-and-extremist-ideologies-online/.

41 Joao V.S. Ozawa, Josephine Lukito, Felipe Bailez, and Luis G. P. Fakhouri, "Brazilian Capitol attack: the interaction between Bolsonaro's supporters' content, WhatsApp, Twitter, and news media", *Harvard Kennedy School Misinformation Review,* 9 April 2024, available at: https://misinforeview.hks.harvard.edu/article/brazilian-capitol-attack-the-interaction-between-bolsonaros-supporters-content-whatsapp-twitter-and-news-media/.

Internal messaging

Like much of the general population, violent extremist actors are heavy users of end-to-end encrypted (E2EE) applications, which allow them to communicate privately with minimal risk of infiltration or detection by law enforcement. Popular apps featuring E2EE that are used by violent extremists include Telegram, Element, WhatsApp, Wire, and Signal.[42] Encryption plays a crucial role in maintaining the privacy and security of everyone, including against criminal and hostile actors, but its use by violent extremist actors continues to frustrate law enforcement investigations. Some governments and law enforcement agencies have called for so-called 'back-door' access to encrypted platforms like WhatsApp, citing security concerns, although evidence suggests that such access would compromise the security of all users, including political activists, human rights defenders and the very government officials that are calling for it.[43]

Some violent extremist actors have adopted more sophisticated tactics to maintain their anonymity, perhaps in part due to a mistrust of even the most privacy-focused apps. Violent extremist digital communities often discuss the merits of privacy-focused technology, including preferred browser choices, Virtual Private Networks (VPNs) and operating systems. Around 2018, core members of Individualistas Teniendo a lo Salvaje (ITS) in South America and Europe, for example, operated their own encrypted instance on the dark web, where they would communicate internally and share audiovisual material.[44] It is common for violent extremist actors to share tips on how to maintain their own operational security (OpSec): on the Brazilian right-wing extremist Dogolachan dark web messaging board, for example, there is a dedicated board on the topic. Investigating and disrupting illegal activity on the dark web poses significant challenges for law enforcement agencies, although countries such as Australia and the Netherlands have made progress in this area in recent years by combining the use of specialised equipment, such as network-monitoring solutions, with legal-backed measures, such as the takeover of a suspected person's online accounts.[45] These measures, when adopted for investigatory purposes, must be applied with full respect for human rights and fundamental freedoms.

42 Interview with Willem Els, Institute for Security Studies, 28 June 2024; Interview with Débora Gomes Salles, Netlab, 14 June 2024.

43 "Terrorist use of E2EE: State of play, misconceptions, and mitigation strategies", *Tech Against Terrorism,* 7 September 2021, available at: https://techagainstterrorism.org/news/2021/09/07/terrorist-use-of-e2ee-state-of-play-misconceptions-and-mitigation-strategies.

44 Sarah Martinenghi, "Progettava attentati, condannato per terrorismo l'anarchico misantropo Federico Buono", *la Repubblica,* 11 May 2023, available at: https://torino.repubblica.it/cronaca/2023/05/11/news/progettava_attentati_condannato_per_terrorismo_lanarchico_misantropo_dellits_federico_buono-399694448/; Sarah Martinenghi, "Volevo colpire parchi e metrò: anarchico confessa e poi ritratta", *la Repubblica,* 9 January 2023, available at: https://torino.repubblica.it/cronaca/2023/01/09/news/volevo_colpire_parchi_e_metro_anarchico_confessa_e_poi_ritratta-382691816/.

45 The Hon. Karen Andrews MP, "New powers to combat crime on the dark web", *Home Affairs, Australian Government,* 25 August 2021, available at: https://minister.homeaffairs.gov.au/KarenAndrews/Pages/new-powers-to-combat-crime-on-the-dark-web.aspx; Andy Greenberg, "Operation Bayonet: Inside the sting that hijacked an entire dark web drug market", *Wired,* 8 March 2018, available at: https://www.wired.com/story/hansa-dutch-police-sting-operation/https://www.wired.com/story/hansa-dutch-police-sting-operation/.

Financing

Digital technologies have enabled violent extremists across the ideological spectrum to develop, rapidly, the ways in which they finance their activities.[46] While fundraising via more 'traditional' means, such as via the banking system, drug trafficking or legal business structures, represents a major means of financing for many violent extremist organisations, cryptocurrencies are increasingly exploited as a means of soliciting donations, probably because they are perceived to be less regulated and more difficult to detect, track, counter or monitor than more conventional fundraising methods.[47] In South Africa, for example, the Suidlanders, a right-wing extremist survivalist group, has long solicited donations on its website via a Bitcoin wallet. It is believed to generate more income from its membership fee than cryptocurrency donations, however.[48]

Online technology is also used by violent extremists to acquire and sell goods and services. A teenager arrested in Singapore in 2021, on suspicion of plotting a terrorist attack inspired by right-wing violent extremist views, had reportedly engaged with a firearms dealer on a "private chat platform", although (because of suspicions about the legitimacy of the dealer) he had opted to purchase a machete via Caroussell, a Singaporean digital marketplace.[49] Some social networking sites also afford extremist actors an opportunity to monetise their content. In Brazil, for example, right-wing extremist 'influencers' and media outlets have reportedly built a profitable operating model thanks to a wide-reaching ecosystem of chat apps and mainstream platforms, including via paid advertising.[50]

46 Jessica Davis, "Technology and terrorist financing", *Global Network on Extremism & Technology*, 19 July 2021, available at: https://gnet-research.org/2021/07/19/technology-and-terrorist-financing/.

47 "Report on abuse of virtual assets for terrorist financing purposes", *Egmont Group*, June 2023, available at: https://egmontgroup.org/wp-content/uploads/2023/12/2023-July-HoFIU-06-IEWG-Project-Abuse-of-VA-for-TF-Summary-1.pdf.

48 Interview with Johannes Vreugdenburg, Individual Expert and Former Police, 8 July 2024.

49 "Detention of Singaporean Youth Who Intended to Attack Muslims on the Anniversary of Christchurch Attacks in New Zealand", *Singapore Ministry of Home Affairs Press Release*, 27 January 2021, archived from the original at: https://web.archive.org/web/20210131130757/https://www.mha.gov.sg/newsroom/press-release/news/detention-of-singaporean-youth-who-intended-to-attack-muslims-on-the-anniversary-of-christchurch-attacks-in-new-zealand.

50 Interview with Débora Salles, Netlab, 14 June 2024.

Offensive Cyber Capabilities

The two other categories of digital abuse by violent extremist actors discussed here cover a more offensive use of digital technologies, where they actively disrupt or destroy targets. Disruptive operations involve activities aimed at exposing sensitive or personally identifiable information, defacing websites, and denying access, as in Distributed Denial-of-Service (DDoS) attacks. Destructive operations are often the most sophisticated or harmful: computer code is manipulated in order to damage or destroy digital or physical assets, as in cyber-attacks that damage critical infrastructure, potentially causing human casualties or producing other significant real-world consequences.[51]

The threat of offensive cyber operations by right- and left-wing extremist actors forms part of a much broader, and growing, cybercrime landscape. As daily life is lived more and more online, more and more vulnerabilities are created for hostile actors to exploit.[52] This issue is likely to be prevalent in economies that have digitised particularly rapidly and do not necessarily have the protections they need against the risk of cross-border cyber-attacks.[53] These vulnerabilities have been recognised in the work of the Ad Hoc Committee to elaborate the United Nations Convention against Cybercrime,[54] and in the UN Secretary General's Strategy on New Technologies:

"Whilst cyberspace has come to underpin almost every aspect of our daily lives, the scale and pervasiveness of 'cyber insecurity' is also now recognised as a major concern. The political and technical difficulty of attributing and assigning responsibility for cyber-attacks encourages actors to adopt an offensive posture, not only amongst states but also from non-state armed and criminal groups and individuals seeking to develop or access potentially destabilising capabilities with a high degree of impunity".[55]

Identifying the perpetrators of cyber-attacks, or their motivations, can be difficult, but it is generally believed that the majority of such incidents are perpetrated by financially motivated or state-backed actors, not non-state violent extremists lacking state-backed support.[56] More than 90% of the 5,632 data breach incidents recorded globally in a 2024 cybersecurity report by Verizon, an American telecommunications company, were identified as relating to financially

51 *Ibid.*

52 Interview with Cybersecurity Expert, 14 June 2024.

53 Interview with Elizabeth Dickinson, International Crisis Group, 4 June 2024; Interview with Camilo Tamayo Gomez, University of Huddersfield, 8 July 2024.

54 "Countering the use of information and communications technologies for criminal purposes", *United Nations General Assembly*, 27 November 2024, available at: https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf.

55 "UN Secretary General's Strategy on New Technologies", https://www.un.org/en/newtechnologies/images/pdf/SGs-Strategy-on-New-Technologies.pdf.

56 Thomas J. Holt, Steven M. Chermak, Joshua D. Freilich, Noah Turner & Emily Greene-Colozzi, "Assessing Racial and Ethnically Motivated Extremist Cyberattacks using open-source data", Terrorism and Political Violence, Vol. 36, Issue 1, September 2022, available at: https://doi.org/10.1080/09546553.2022.2119848.

motivated actors, while only 7% were categorised as "espionage".[57] Non-state actors motivated by considerations other than financial were not given their own category within the findings; they probably came under "other", which contained around 3% of the total figure. That such actors represent only a small proportion of the overall threat should not, however, take away from the potentially wide-reaching and harmful consequences of any hostile action of theirs, especially as such actions are likely to increase in the coming years.[58]

However, the line between state actors on the one hand, and on the other, non-state cybercriminals whose motivation is not financial, is often unclear. Various real and hypothetical scenarios blur any such distinction, including where states provide non-state groups with resources or training for specific operations, which are then used by the group for other operations. Another potential scenario involves hostile actions by non-state groups who may not be cognisant of the influence on them by state actors, as in the case of extremist organisations whose narratives align with state-backed mis- or disinformation campaigns. Further complicating the categorisation of such actors, it is also often unclear to what extent pro-government hacking groups, such as those discussed in some of the case studies in this report, are linked to the government in their respective jurisdictions.

When it comes to non-state actors motivated by considerations other than financial, the actions of hacktivists represent a significant proportion of cyber-attacks motivated by a belief system. Hacktivists engage in political activism via computer hacking, using legal and/or illegal digital tools to achieve a political goal or spread a political message, targeting entities perceived as adversaries or aligned with opposing belief systems.[59] They can be motivated by a variety of causes. Many hacktivists declare support for fundamental freedoms and human rights, and they often claim to operate against perceived injustices, or in the furtherance of democracy, as in the early actions of Anonymous, a decentralised collective that originated on 4chan in around 2008.[60] While in these cases it is vital not to conflate the actions of hacktivists with those of violent extremists, actions to promote human rights and fundamental freedoms must not condone, advocate or resort to crime or violence.

57 "2024 Data Breach Investigations Report", Verizon Business, available at: https://www.verizon.com/business/resources/T3d/reports/2024-dbir-data-breach-investigations-report.pdf/.

58 The majority of the 31 experts consulted for the study believed the threat of cyber-attacks by non-state violent extremists is likely to increase in the coming five years.

59 Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" in *Networks and Netwars: The Future of Terror, Crime, and Militancy,* ed. John Arquilla and David Ronfeldt (2001), pp. 239-288, available at: https://www.jstor.org/stable/10.7249/mr1382osd.13?seq=3. "Beneath the surface: terrorist and violent extremist use of the dark web and cybercrime-as-a-service for cyber-attacks", *UNICRI, UNOCT/UNCCT*, 2024, available at: https://unicri.it/sites/default/files/2024-07/DW_BtS.pdf.

60 Tom Huddleston Jr, "What is Anonymous? How the infamous 'hacktivist' group went from 4chan trolling to launching cyberattacks on Russia", *CNBC,* 25 March 2022, available at: https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html.

Some hacktivist collectives work for more nefarious causes, however, sometimes supporting or possibly even coordinating with autocratic regimes. State affiliation is likely to increase significantly the capability of hacktivist groups to inflict damage or prolonged disruption on their targets, including via additional financing or technical expertise.[61] There are also hacktivist groups operating for similar causes to groups subscribing to extremist ideologies, and there is a risk that some hacktivists motivated by considerations other than financial may potentially become radicalised into violent extremism. Cases have been reported of hackers becoming involved in terrorist groups, notably groups like the Islamic State in Iraq and the Levant (ISIL/Da'esh).[62] And some violent extremist organisations, including left-wing extremist groups in South America, have deliberately sought out recruits with technical skill sets in an attempt to bolster their cyber capabilities.[63]

Another way in which the cyber capabilities of non-state violent extremist actors may potentially be increased is via Cybercrime-as-a-Service (CaaS). The proliferation of CaaS products available online risks lowering the bar to entry for more disruptive or destructive cyber operations by violent extremist non-state actors, including those that do not have a high level of computing skills.[64] Although the most skilled hackers are likely to code their own attacks, there is an extensive illicit digital market of off-the-shelf tools and services available for use by less technically skilled malicious actors.[65] Products include personal data, ransomware, malware, botnets-for-hire, DDoS tools, and access to compromised systems.[66] In 2023 Europol highlighted the presence of malicious Large Language Model (LLM) products on the surface and dark web, servicing cyber-attack perpetrators and those engaged in social engineering.[67]

Although the progression from holding extremist ideas to engaging in violence is not linear, it is important to consider the inherent potential risks. It is likely that those hackers with ideological proximity to extremist belief systems are most at risk of radicalisation into these movements: for example, social justice-focused actors may be exposed to networks connected with left-wing

61 Interview with David Wells, Honorary Research Associate, Swansea University, Cyber Threats Research Centre, 13 June 2024.

62 Nafees Hamid, "The British hacker who became the Islamic State's Chief Terror Cybercoach: A profile of Junaid Hussein", *CTC Sentinel,* Vol. 11, Issue 4, April 2018, available at: https://ctc.westpoint.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/.

63 Interview with Elizabeth Dickinson, International Crisis Group, 4 June 2024.

64 Michael Hill, "DDoS attack-for-hire services thriving on Dark Web and cyber criminal forums", *Cyber Security Hub,* 4 December 2023, available at: https://www.cshub.com/attacks/news/ddos-attack-for-hire-services-thriving-on-dark-web-and-cyber-criminal-forums.

65 "The Rise of cybercrime-as-a-service", *Field Effect,* 19 April 2023, available at: https://fieldeffect.com/blog/cybercrime-as-a-service.

66 "Beneath the surface: terrorist and violent extremist use of the dark web and cybercrime-as-a-service for cyber-attacks", *UNICRI, UNOCT/UNCCT.* 2024, available at: https://unicri.it/sites/default/files/2024-07/DW_BtS.pdf.

67 "Internet Organised Crime Threat Assessment 2023", *Europol,* available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf.

violent extremism, or misogynistic and chauvinistic hackers lured into right-wing violent extremist movements.[68] This risk is liable to be heightened by unfolding global violent events. Evidence gathered in previous UNICRI research indicates that threat actors motivated by a belief system rather than purely financial considerations are engaging with cybercriminal elements in the dark web and the broader cybercrime underground in the context of Cybercrime-as-a-Service.[69] Examining these threat actors can reveal how a confluence through Cybercrime-as-a-Service may increase the risk of violent extremism-related cyber-attacks, although the likelihood appears to be higher in countries with a more robust and sophisticated cyber infrastructure.

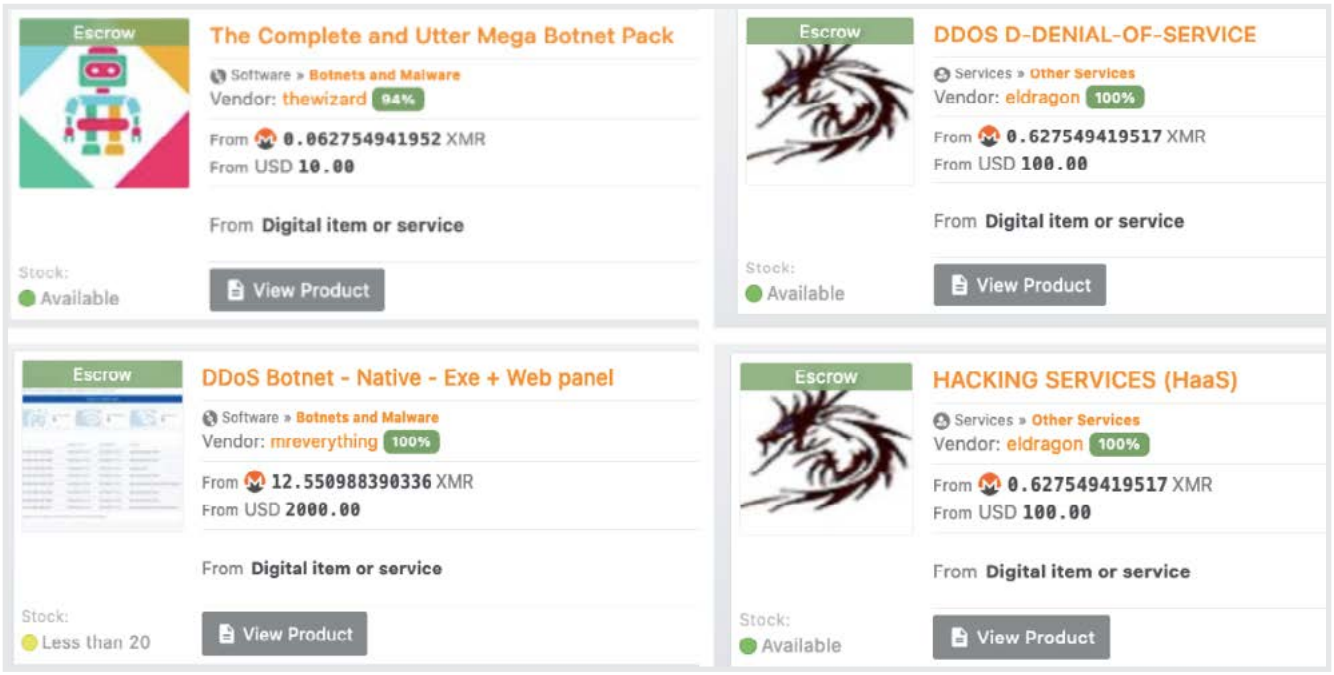

Figure 1. CaaS examples on a prominent dark web market, captured in July 2024.

Despite the availability of these tools and services on the dark web and encrypted messaging platforms, this study found few indications of frequent or widespread use of them by violent extremist actors in South America, Africa or Asia. The reasons for this are unclear, but it may suggest a general lack of intent to prioritise offensive cyber operations over more traditional forms of activism or violence, such as propaganda, threats or offline kinetic activities.[70] Lack of Internet infrastructure or access in the areas where some violent extremist groups operate is likely to contribute to this dynamic. Violent extremist groups may also be reluctant to risk intro-

68 Tim Jordan and Paul Taylor, "Hacktivism and Cyberwars: Rebels with a cause", *Routledge*, 2004, available at: https://www.thing.net/~rdom/ucsd/3somesPlus/hacktivismcyberwars.pdf; Interview with Thomas J. Holt, Michigan State University, 2 July 2024; Thomas Holt, Joshua Freilich, Steven Chermak et al., "Exploring the subculture of ideologically motivated cyber attackers", *Journal of Contemporary Criminal Justice*, Vol. 33, Issue 3, 4 April 2017, available at: https://journals.sagepub.com/doi/10.1177/1043986217699100.

69 "Beneath the surface: terrorist and violent extremist use of the dark web and cybercrime-as-a-service for cyber-attacks", UNICRI, UNOCT/UNCCT.

70 Interview with Charley Gleeson, Extrac, 10 June 2024.

ducing external actors into clandestine operations,[71] and there is a belief too that cyber-attacks may not provide the impactful spectacle of a physical act.[72] Furthermore, any such activity may well go undetected, owing to the difficulty of assigning responsibility and identifying the source of the tooling used by perpetrators.

The cyber capabilities of right- and left-wing violent extremist actors in the Global South

In some instances, right- and left-wing violent extremist actors in South America, Africa and Asia have shown a sophisticated understanding of how to exploit digital technologies to spread their message, communicate, remain anonymous, and fundraise. There is little evidence to suggest that they have engaged in destructive cyber-attacks in significant measure, possibly as a result of a lack of intent or capability.[73] Overall, violent extremist actors globally are probably more interested in defensive technical tooling geared towards hiding their identities, for example – such as encryption, cryptocurrency, Tor, or Virtual Private Networks (VPNs) – than in computer hacking or other more cyber offensive tactics.[74] State backing for, or affiliation with, non-state violent extremist movements, however, may increase those movements' capability to engage in more sophisticated cyber-attacks, provided they are intent on doing so. There are precedents for the provision of financial or other operational backing for non-state hacking groups by states, mostly relating to Advanced Persistent Threat (APT) groups,[75] although confirming the existence and nature of these relationships is often difficult.

The case studies section of this report gives examples of hacktivist collectives with ideological proximity to some violent extremist movements, and individuals more closely affiliated with those movements, that have engaged in mostly disruptive cyber activities. They include nationalist hacktivist groups in India and South-East Asia. Recurring tactics include DDoS attacks, data breaches, web defacement and coordinated trolling or abuse campaigns. In an indication of the tactics adopted by right-wing extremist hackers globally, a 2022 study found that, of the fourteen racially and ethnically motivated cyber-attacks on United States targets identified between 2005 and 2020, three related to web defacement, one to a data breach, two to doxxing and six to "other" forms of hacking, such as gaining access to social media accounts, email spam or

71 Interview with Erin Saltman, Global Internet Forum to Counter Terrorism (GIFCT), 4 July 2024.

72 "Beneath the surface: terrorist and violent extremist use of the dark web and cybercrime-as-a-service for cyber-attacks", *UNICRI, UNOCT/UNCCT*; Maura Conway, "Reality Check: Assessing the (un)likeihood of cyberterrorism" in Tom Chen, Lee Jarvis and Stuart Macdonald (eds), *Cyber Terrorism: Understanding, Assessment and Response,* (Springer, New York), pp. 102-122.

73 Interview with Thomas J. Holt, Michigan State University, 2 July 2024; Conclusion based on extensive literature review conducted as part of this study.

74 Thomas J. Holt, Steven M. Chermak, Joshua D. Freilich, Noah Turner & Emily Greene-Colozzi, "Assessing Racial and Ethnically Motivated Extremist Cyberattacks using open-source data", *Terrorism and Political Violence,* Vol. 36, Issue 1, September 2022, available at: https://doi.org/10.1080/09546553.2022.2119848.

75 "Groups", MITRE | ATT&CK, available at: https://attack.mitre.org/groups/; "Glossary: Advanced Persistent Threat", NIST, Computer Security Resource Center (CSRC), available at: https://csrc.nist.gov/glossary/term/advanced_persistent_threat.

harassment.[76] More research is required specifically on the cyber capabilities of right- and left-wing violent extremist movements in the Global South, in order to ascertain the extent to which these findings are also applicable to other regional contexts.

Left-wing extremist actors were found in another US-focused study to be more sophisticated than right-wing actors, particularly when it came to data breach attacks against commercial targets.[77] The study found 26 instances of cyber-attacks by "far-left" groups and affiliated actors in the United States, the United Kingdom and Canada between 2000 and 2015, including "a substantive increase in the frequency of cyber-attacks performed since 2011, and a decrease in the frequency of physical attacks". This suggests that left-wing groups may be opting for cyber operations rather than real-world violence, which has been the more deadly threat of right-wing extremists in many countries in the Global North in recent years.[78]

Overall, the risks of destructive cyber-attacks delivered by right- and left-wing violent extremist actors heighten as more skilled actors converge around shared belief systems for opportunistic reasons. The majority of the experts interviewed for this study believed that the cyber threat posed by right-wing and left-wing violent extremist movements was likely to get worse in the coming five years, owing in part to the widespread accessibility of technical tooling combined with the growing availability of digital technologies and Internet access among the general population. In most of the responses, experts – especially with reference to South America and Asia – also described the likelihood of a sophisticated cyber-attack by non-state violent extremist actors causing human casualties as somewhat likely, or highly likely. Even if limited, these responses signal the need to explore further the online interplay between financially motivated cybercriminals, violent extremist individuals and groups, and threat actors motivated by considerations other than financial, such as hacktivist collectives or state-backed entities.

76 Thomas J. Holt, Steven M. Chermak, Joshua D. Freilich, Noah Turner & Emily Greene-Colozzi, "Assessing Racial and Ethnically Motivated Extremist Cyberattacks using open-source data", *Terrorism and Political Violence,* Vol. 36, Issue 1, September 2022, available at: https://doi.org/10.1080/09546553.2022.2119848.

77 Interview with Thomas Holt, Michigan State University, 2 July 2024; Thomas J. Holt, Mattisen Stonhouse, Joshua Freilich and Steven M. Chermak, "Examining ideologically motivated cyberattacks performed by far-left groups", *Terrorism and Political Violence*, Vol 33, Issue 3, January 2019, available at: https://doi.org/10.1080/09546553.2018.1551213.

78 Katarzyna Jasko, Gary LaFree and Michael H. Becker, "A comparison of political violence by left-wing, right-wing, and Islamist extremists in the United States and the world", *Proceedings of the National Academy of Sciences,* Vol. 119, Issue 30, July 2022, available at: https://doi.org/10.1073/pnas.2122593119.

Emerging technologies

Government security agencies and technology industries are working tirelessly to mitigate the exploitation of new and emerging technologies by violent extremist actors. Livestreaming, in particular, has been exploited globally since at least 2019 by right-wing violent extremists wishing to broadcast their attacks in real time, including in India and Singapore.[79] Violent extremist actors are also frequent users of platforms built using decentralised technology, which sometimes makes the permanent removal of illegal material more difficult than it would be on conventional platforms.[80]

Recent research has highlighted the risk of the abuse of Artificial Intelligence (AI)-powered digital tooling by violent extremists, given the rapid growth in the technology's popular use, availability and features.[81] There is evidence to suggest that violent extremist actors globally have begun using Generative AI tools to produce synthetic audiovisual propaganda, for example, and even to create chatbots that mimic violent extremist figures like Adolf Hitler.[82] Nevertheless, this research found few examples of the use of Generative AI tools by right- or left-wing violent extremist actors in South America, Africa or Asia, aside from some instances where they shared imagery that was clearly AI-generated. Violent extremism and mis- or disinformation are often interlinked, and AI has the potential to serve as an amplifier, including by spreading false content at accelerated rates. AI technologies may also enable violent extremist actors to tailor propaganda to different audiences, for example by using gendered narratives to appeal to different demographics.[83]

79 "Delhi: shooter was livestreaming just before attack at Jamia", *Times of India,* 31 January 2020, available at: https://timesofindia.indiatimes.com/city/delhi/shooter-was-livestreaming-just-before-attack-at-jamia/articleshow/73785525.cms; "Singapore boy held for Christchurch-inspired mosque attack plot", *BBC News,* 28 January 2021, available at: https://www.bbc.co.uk/news/world-asia-55836774.

80 Lorand Bodo and Inga Kristina Trauthig, "Emergent technologies and extremists: the DWeb as a new internet reality?", *Global Network on Extremism & Technology,* July 2022, available at: https://gnet-research.org/wp-content/uploads/2022/07/GNET-Report-Emergent-Technologies-Extremists-Web.pdf.

81 "The state of AI in 2023: Generative AI's breakout year", *McKinsey & Company,* 1 August 2023, available at: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year.

82 David Wells, "The next Paradigm-shattering threat? Right-sizing the potential impacts of Generative AI on terrorism", *Middle East Institute,* March 2024, available at: https://mei.edu/sites/default/files/2024-03/Wells%20-%20The%20Next%20Paradigm-Shattering%20Threat%20Right-Sizing%20the%20Potential%20Impacts%20of%20Generative%20AI%20on%20Terrorism.pdf; David Gilbert, "Here's how violent extremists are exploiting Generative AI tools", *Wired,* 9 November 2023, available at: https://www.wired.com/story/generative-ai-terrorism-content/; Interview with Barbara Molas, International Centre for Counter Terrorism, 11 June 2024; Mark Sellman, "Hitler chatbot 'a clear security threat' amid radicalisation fears", *The Times,* 11 February 2024, available at: https://www.thetimes.com/business-money/technology/article/hitler-chatbot-prompts-fears-of-online-radicalisation-djwbsdm08; Interview with Joshua Fisher-Birch, Counter Extremism Project, 12 June 2024.

83 OSCE, "Summary Document of Expert-Level Event, Artificial Intelligence in the Context of Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism: Risks and Opportunities", 2024, available at: https://www.osce.org/files/f/documents/4/f/575877.pdf.

Nonetheless, there is the potential for the advent of AI adoption in these regions to facilitate violent extremism and related cyber-enabled threats further, including by using these tools to create incendiary deep fakes or by increasing their technical capability to mount more offensive cyber-attacks.[84] There is also a risk that AI may enable violent extremists to produce a greater volume of content adapted to multiple specific local audiences. The radicalising impact of synthetic as opposed to human-generated AI, however, is not yet clear.[85] Additionally, AI systems used for content moderation can over-remove legitimate content through a lack of contextual understanding: this can affect marginalised voices disproportionately, and can lead to self-censorship, as individuals fear being tracked and identified – thereby further threatening freedom of expression.[86]

Technology Sector Responses

Technology companies face significant challenges in effectively moderating violent extremist use of their platforms globally while also balancing user privacy, freedom of expression and other fundamental human rights.[87] They have come under increasing pressure in recent years, including from governments and civil society organisations, to keep their platforms safe and free from illegal or otherwise 'harmful' content. Legislation in various jurisdictions imposes requirements on technology companies regarding their response to illegal activity on their platforms.[88] There have also been a number of separate high-profile lawsuits and congressional hearings in which companies have faced accusations of direct responsibility for allegedly abetting violence via user-generated content posted on their platforms.[89]

84 Interview with Senior Tech Company Representative, 10 June 2024; Interview with David Wells, Honorary Research Associate, Swansea University, Cyber Threats Research Centre, 13 June 2024.

85 Wells, "The Next Paradigm-Shattering Threat? Right-Sizing the Potential Impacts of Generative AI on Terrorism".

86 OSCE, "Safeguarding freedom of expression in the age of artificial intelligence," 2021, available at: https://www.osce.org/files/f/documents/8/f/510332_1.pdf.

87 "Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook", Human Rights Watch, 21 December 2023, available at: https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and.

88 "The online regulation series handbook 3.0", *Tech Against Terrorism,* July 2023, available at: https://techagainstterrorism.org/news/online-regulation-series-3.0.

89 Kari Paul, "Zuckerberg tells parents of social media victims at Senate hearing: I'm sorry for everything you've been through", *The Guardian,* 31 January 2024, available at: https://www.theguardian.com/us-news/2024/jan/31/tiktok-meta-x-congress-hearing-child-sexual-exploitation; "Myanmar: Facebook's systems promoted violence against Rohingya; Meta owes reparations – new report, *Amnesty International,* 29 September 2022, available at: https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/; Caroline Crystal, "Facebook, Telegram, and the ongoing struggle against online hate speech", *Carnegie Endowment for International Peace,* 7 September 2023, available at: https://carnegieendowment.org/research/2023/09/facebook-telegram-and-the-ongoing-struggle-against-online-hate-speech.

In response to these threats – to user safety, to their own reputation, and to their revenue[90] – the larger technology companies each employ as many as tens of thousands of people focused on content moderation,[91] and there are a growing toolkit of technical approaches[92] and a burgeoning industry of third-party vendors.[93] Moderators working for Facebook, the world's largest social network, reportedly made three million daily moderation decisions in 2020, while by 2024 its users were uploading billions of pieces of content per day.[94] Recently, however, some social media companies, such as X (formerly Twitter), have severely cut their internal resources for content moderation, and their safety and public policy personnel, with potential repercussions for existing measures to tackle terrorist and violent extremist content and online hate overall.[95]

Some experts argue that ongoing advances in AI-driven tools, which have long played a role in content moderation systems, are likely to revolutionise the ability of technology companies effectively to detect and remove illegal content posted on their services.[96] In their current form, however, such technologies do not appear to have comprehensively resolved issues around interpreting contextual linguistic nuance, reliable sound, weapon detection, or the detection of content that has been deliberately modified.[97]

Some platforms appear to have dedicated disproportionate resources to moderating English-language content compared with other languages. According to internal company files leaked by a whistleblower in 2021, for example, Facebook spent 87% of its budget on combating misinformation on English-language content at a time when just 9% of its users were English-speaking.[98] Transparency reports published in 2023, as required by the European Union's Digital Services

90 Ryan Mac and Kate Conger, "X May Lose up to $75 Million in Revenue as More Advertisers Pull Out", The *New York Times,* 24 November 2023, available at: https://www.nytimes.com/2023/11/24/business/x-elon-musk-advertisers.html; Tiffany Hsu and Eleanor Lutz, "More than 1,000 companies boycotted Facebook. Did it work?", *The New York Times,* 1 August 2020, available at: https://www.nytimes.com/2020/08/01/business/media/facebook-boycott.html.

91 Paul M. Barrett, "Who moderates the social media giants?", *Center for Business and Human Rights, New York University,* June 2020, available at: https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/5ed9854bf618c710cb55be98/1591313740497/NYU+Content+Moderation+Report_June+8+2020.pdf.

92 T.G. Thorley and E. Saltman, "GIFCT tech trials: combining behavioural signs to surface terrorist and violent extremist content online", *Studies in Conflict and Terrorism,* 1-26 (2023), available at: https://doi.org/10.1080/1057610X.2023.2222901; "GIFCT technical approaches working group: Gap Analysis and recommendations for deploying technical solutions to tackle the terrorist use of the internet", *Tech Against Terrorism and the Global Internet Forum to Counter Terrorism,* July 2021, available at: https://gifct.org/wp-content/uploads/2021/07/GIFCT-TAWG-2021.pdf.

93 Tim Bernard, "The evolving trust and safety vendor ecosystem", *Tech Policy Press,* 24 July 2023, available at: https://www.techpolicy.press/the-evolving-trust-and-safety-vendor-ecosystem/.

94 John Koetsier, "Report: Facebook makes 300,000 content moderation mistakes every day", *Forbes,* 30 June 2021, available at: https://www.forbes.com/sites/johnkoetsier/2020/06/09/300000-facebook-content-moderation-mistakes-daily-report-says/; "41 up-to-date Facebook facts and stats", *Wishpond,* available at: https://blog.wishpond.com/post/115675435109/40-up-to-date-facebook-facts-and-stats.

95 "Report reveals the extent of deep cuts to safety staff and gaps in Twitter/X's measures to tackle online hate", *eSafetyCommissioner, Australian Government*, January 2024, available at: https://www.esafety.gov.au/newsroom/media-releases/report-reveals-the-extent-of-deep-cuts-to-safety-staff-and-gaps-in-twitter/xs-measures-to-tackle-online-hate.

96 Interview with Adam Hadley, Tech Against Terrorism, 20 June 2024; Interview with Senior Tech Company Representative, 04 July 2024.

97 Interview with Nicole Matejic, Charles Sturt University, 12 June 2024; Billy Perrigo, "Social media companies vowed to stop videos of terror attacks. Buffalo showed they have more work to do", *Time*, 17 May 2022, available at: https://time.com/6177640/buffalo-shooting-twitch-social-media/; Stuart Macdonald, Ashley Mattheis and David Wells, "Using Artificial Intelligence and Machine Learning to Identify Terrorist Content Online", *Tech Against Terrorism Europe,* 15 January 2024, available at: https://tate.techagainstterrorism.org/news/tcoaireport.

98 Dan Milmo, "Facebook revelations: what is in cache of internal documents?", *The Guardian,* 25 October 2021, available at: https://www.theguardian.com/technology/2021/oct/25/facebook-revelations-from-misinformation-to-mental-health.

Act (DSA), indicated a similar trend across many of the major platforms, at least with regard to European languages.[99]

In a reflection of the adverse impact of this imbalance in resource allocation, almost all of the 31 experts interviewed as part of this research believed that the large technology companies were unable to moderate content in South America, Africa or Asia as effectively as in countries in the Global North. There is also evidence to suggest that technology companies sometimes do not maintain as close a working relationship with law enforcement or government departments in South America, Africa or Asia as they do with governments in the Global North, which means that governments sometimes struggle to establish consistent contact with some companies.[100] Technology companies also have difficulty deciphering cultural nuances and the contextual circumstances of violative posts, especially when these emanate from geographical contexts they lack cultural understanding of.[101] As a result, platforms may fail to moderate material that violates their terms of service, or may remove innocuous content disproportionately from marginalised communities, at the risk of suppressing legitimate speech.

Additionally, international technology companies find themselves in a varied and complex jurisdictional landscape around the world, in which the norms and laws of different countries often contradict one another. It is common for violent extremist movements to be banned in one country but not in another; a dynamic that is even more common for right- and left-wing violent extremist groups than for groups like the Islamic State in Iraq and the Levant (ISIL/Da'esh) or Al-Qaida.[102] A popular approach to resolving such jurisdictional inconsistencies, adopted by technology companies, is to 'geoblock' content that violates specific local laws, rendering it inaccessible to users in one particular country but not others. At the government's request, in 2023 X (formerly Twitter) reportedly geoblocked accounts and tweets relating to anti-government activists in India, for example, following a longstanding lawsuit filed during the tenure of

99 "How Big Tech platforms are neglecting their non-English language users", *Global Witness*, 30 November 2023, available at: https://www.globalwitness.org/en/campaigns/digital-threats/how-big-tech-platforms-are-neglecting-their-non-english-language-users/.

100 Jasper Jackson, Lucy Kassa, Kathleen Hall, Zecharias Zelalem, "Facebook accused by survivors of letting activists incite ethnic massacres with hate and misinformation in Ethiopia", *The Bureau of Investigative Journalism,* 20 February 2022, available at: https://www.thebureauinvestigates.com/stories/2022-02-20/facebook-accused-of-letting-activists-incite-ethnic-massacres-with-hate-and-misinformation-by-survivors-in-ethiopia/. Feedback gathered from national stakeholders during UNICRI workshops and activities in the field.

101 Interview with David Wells, Honorary Research Associate, Swansea University, Cyber Threats Research Centre, 13 June 2024.

102 "Who designates terrorism? The need for legal clarity and transparency to moderate terrorist content online", *Tech Against Terrorism,* 23 March 2023, available at: https://techagainstterrorism.org/hubfs/TAT-Designation-Report-March-2023.pdf.

the company's former owner, Jack Dorsey, in which such government requests were described by Twitter in 2021 as an "abuse of power".[103]

Definitional and legal differences between countries regarding concepts such as terrorism and violent extremism, and the obligations placed on technology companies on the basis of those norms, are likely to be particularly problematic for the technology industry when it comes to right- and left-wing violent extremism. Unlike organisations such as the Islamic State in Iraq and the Levant (ISIL/Da'esh) and Al-Qaida, many of the individuals, groups and organisations discussed in the case studies in this report are not widely designated as terrorist, nor are many of them banned or otherwise sanctioned in the countries in which they operate. In some jurisdictions, even where such content incites violence or violates the terms of service in other ways, there can sometimes be no clear domestic legal framework – or no effective enforcement of existing laws – forcing technology companies to remove it.[104] These differences and challenges increase the risk of 'differential disruption', whereby different malicious actors are subject to very different levels of disruption and content moderation online.[105] The problem is made more difficult by the ability of many extremist actors to toe the line of acceptability online deliberately, taking care not to cross over into illegal messaging or content that would violate companies' terms of service.

In addition, technology companies are sometimes reluctant to take action on violent extremist actors' use of their services when those actors are supported by or linked to the authorities in a particular geographical context.[106] India is an attractive market for Meta, where it has more users than in the United States,[107] and noting the shared ideological origins of the Hindutva extremists and the BJP, it appears that Meta has been disinclined to take action against groups or individuals when they could be viewed as supporting or being affiliated with the Hindutva belief as a whole – even when content is likely in violation of the company's policies.[108] A 2023 report in *The Washington Post* cited employee testimonies and internal Facebook documents as saying that the reluctance to moderate material there was related to "political sensitivities".[109] Such

103 Mike Masnick, "'Free speech' Twitter is now globally blocking posts critical of the Modi government", *TechDirt,* 11 April 2023, available at: https://www.techdirt.com/2023/04/11/free-speech-twitter-is-now-globally-blocking-posts-critical-of-the-modi-government/; Karishma Mehrotra and Joseph Menn, "How India tamed Twitter and set a global standard for online censorship", *The Washington Post,* 8 November 2023, available at: https://www.washingtonpost.com/world/2023/11/08/india-twitter-online-censorship/.

104 Interview with Stuart Macdonald, Swansea University, 14 June 2024..

105 Conway, M. et al., "A Snapshot of the Syrian Jihadi Online Ecology: Differential Disruption, Community Strength, and Preferred Other Platforms", *Studies in Conflict & Terrorism*, pp. 1-17, 2021, https://doi.org/10.1080/1057610X.2020.1866736.

106 Interview with Erin Saltman, Global Internet Forum to Counter Terrorism (GIFCT), 4 July 2024; Interview with Anuradha Sajjanhar, University of East Anglia, 24 June 2024.

107 Shilpa Ranipeta, "India, home to Meta's largest consumer base across Facebook, WhatsApp and Instagram", *CNBC TV18,* 4 August 2024, available at: https://www.cnbctv18.com/technology/india-home-to-metas-largest-consumer-base-across-facebook-whatsapp-and-instagram-17439461.htm.

108 Joseph Menn and Gerry Shih, "Under India's pressure, Facebook let propaganda and hate speech thrive", *The Washington Post,* 26 September 2023, available at: https://www.washingtonpost.com/world/2023/09/26/india-facebook-propaganda-hate-speech/.

109 *Ibid.*

apparent inconsistencies in the application of technology company policy can be attributed to several factors. Companies must weigh up the pros and cons of the potential side-effects of severing good relations with certain governments, for example by a country-wide ban[110] which could drastically reduce their revenue there, exacerbate the risk of human rights abuses going unreported and, potentially, jeopardise the safety of local staff.[111]

Several global Internet-focused initiatives have emerged in recent years as collaborative responses to the exploitation of digital technology by violent extremists and other hostile actors, providing support for technology companies large and small in combating such online threats. The Global Internet Forum to Counter Terrorism (GIFCT), for example, is a non-governmental membership organisation founded in 2017 by Meta, Microsoft, YouTube and X, which by 2024 had more than 30 member companies, most of them based in the United States.[112] An independent Human Rights Assessment conducted for the GIFCT in 2021 identified several challenges the organisation faced in expanding its membership geographically.[113] Another such initiative, Tech Against Terrorism, is a public-private partnership launched by the United Nations Counter Terrorism Executive Directorate (UNCTED) in 2017. It aims to disrupt terrorist and violent extremist content online, via engagement with the technology and public sectors, and to provide smaller companies with dedicated assistance in this regard.[114] Finally, the Christchurch Call Foundation is a global multistakeholder initiative launched by the governments of New Zealand and France following the March 2019 attacks in Christchurch, New Zealand. Its community consists of 55 national governments and the European Commission, 19 online service providers, 13 partner organisations and more than 50 civil society experts and organisations.[115]

110 Pjotr Sauer, "Russia bans Facebook and Instagram under 'extremism' law", *The Guardian,* 21 March 2022, available at: https://www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and-instagram-under-extremism-law.

111 Interview with Senior Tech Company representative, 4 July 2024.

112 "GIFCT – About", available at: https://gifct.org/about/.

113 "Human Rights Assessment: Global Internet Forum to Counter Terrorism", BSR, 2021, available at: https://gifct.org/wp-content/uploads/2021/07/BSR_GIFCT_HRIA.pdf.

114 "Tech Against Terrorism", available at: https://techagainstterrorism.org/home.

115 "The Christchurch Call", available at: https://www.christchurchcall.org/.

{ CASE STUDIES }

The case studies below do not seek to enter the debate of which groups and movements are referenced as violent extremist or not internationally and do not place any responsibility on the Member States mentioned. The case studies do not imply that there is a consensus among the international community that the terminology adopted in this report should have universal application, or that the Member States referenced in the case studies automatically accept that the adopted terminology and definition fully reflect the emerging and existing threats in their countries. As Member States use different language to describe the violent non-state actors active within their territories, this publication does not imply the expression of any opinion on its contents by the Member States mentioned.

The case studies aim to illustrate examples of exploitation of digital technologies by groups and individuals aligned with or supporting right-wing and left-wing violent extremist ideologies, deploying violent extremist-like tactics, modus operandi and other means to spread specific ideologies and perpetuate violence.

Violent anarcho-primitivism in South America: ITS

Background

Individualistas Tendiendo a lo Salvaje (Individuals Tending towards the Wild, ITS) is an international violent extremist group that originated in Mexico in 2011. The group is heavily influenced by the ideology and tactics of Ted Kaczynski, known as the 'Unabomber', who mounted a campaign of mail bombings in the United States between 1978 and 1995.[116] In a statement published online in 2013, ITS said its engagement in violence was part of its "struggle against the techno-industrial system" and that it acted in defence of "wild nature". Like Kaczynski, the group sees technological progress as leading civilisation to an inevitable ecological catastrophe. It advocates nihilist violence, the destruction of technology and a return to a hunter-gatherer lifestyle.

Although ITS does have links to the international anarchist movement, it has rejected that label. Its use of indiscriminate violence has been divisive in anarchist circles, some denouncing the group as "eco-fascist".[117] Press reports have described ITS as "eco-terrorist",[118] although its modus operandi does not resemble that of other radical environmentalists, and it has condemned the "leftism" of green anarchism.[119] The group's leader has admitted being influenced by the organisational and tactical approach of Temple ov Blood, a nexion of the Order of Nine Angles, a violent Satanic group that originated in the United Kingdom.[120]

On its website the group has celebrated a broad range of incidents causing loss of human life globally, regardless of their cause, motivation or victims; including the earthquake and tsunami afflicting Sumatra, Indonesia in December 2018, and the terrorist attacks motivated by right-wing extremist views in Christchurch, New Zealand, in March 2019. The messaging and ideology of ITS are often nihilist in nature.

116 Sean Fleming, "The Unabomber and the origins of anti-tech radicalism", Journal of Political Ideologies, Vol. 27, No. 2, 7 May 2021, available at: https://www.tandfonline.com/doi/epdf/10.1080/13569317.2021.1921940?needAccess=true.

117 Scott Campbell, "There's nothing anarchist about eco-fascism: A condemnation of ITS", *Its going down,* 12 May 2017, available at: https://itsgoingdown.org/nothing-anarchist-eco-fascism-condemnation/.

118 Joge Andrés Cash, "El ecoterrorismo y la paradoja de la locura total", *Elmostrador*, 16 January 2019, available at: https://www.elmostrador.cl/noticias/opinion/2019/01/16/el-ecoterrorismo-y-la-paradoja-de-la-locura-total/; Felipe Diaz, ""Ecoterroristas" reaparecen con revista digital y advertencia de nuevos atentados", *La Tercera*, 31 July 2019, available at: https://www.latercera.com/la-tercera-pm/noticia/ecoterroristas-reaparecen-revista-digital-advertencia-nuevos-atentados/761792/; Robert Beckhusen, "In manifesto, Mexican eco-terrorists declare war on nanotechnology", Wired, 12 March 2013, available at: https://www.wired.com/2013/03/mexican-ecoterrorism/.

119 Fleming, "The Unabomber and the origins of anti-tech radicalism".

120 Daveed Gartenstein-Ross, Emelie Chace-Donahue and Thomas Plant, "The Order of the Nine Angles", *Foundation for Defense of Democracies,* 25 July 2023, available at: https://www.fdd.org/analysis/2023/07/25/the-order-of-nine-angles/.

ITS claimed its first attacks in 2011 in Mexico. During that year its members said they sent two package bombs to scientists at universities in Tultitlan and Mexico City, in April and August respectively.[121] Later, the group also claimed to have been responsible for shooting dead a biotechnology researcher, although the findings of a police investigation contradicted this.[122] According to a report by the Center for Research and National Security (Cisen) in Mexico, ITS carried out the majority of the 306 attacks classified under anarchism, extremism and eco-terrorism there in 2016.[123] In 2017, ITS claimed responsibility for a shooting in Querétaro, Mexico, in which a pilgrim was killed.[124] However, the veracity of several of the group's claims – many of which were made under the name of ITS's subgroup Reacción Salvaje (RS) – were disputed by police.

ITS published a manifesto on *Liberación Total,* an anarchist blog, in February 2013. Hard copy versions of the manifesto had been found in the packages sent to Mexican universities two years earlier. In it the group distanced itself from left-wing anarchism, saying that it was not against "all authority" but only the authority imposed by the "techno-industrial system". It criticised eco-fascism and national socialism as "the result of unintelligent minds". The manifesto advocated instead the "hunter-gatherer-nomadic" lifestyle, a way of life for which it said humans were "biologically programmed".

Current threat picture: regional expansion and transnational connections

Between 2016 and 2019, ITS expanded regionally in South America, claiming responsibility for multiple attacks it said were perpetrated by its affiliates in Chile, Argentina and Brazil. Its Brazilian affiliate, Sociedade Secreta Silvestre (SSS), said it was responsible for a pressure-cooker bombing in Brasilia in August 2016, in which no one was injured.[125] Threats made by SSS to government officials, including then President Jair Bolsonaro, the Minister for the Environment and the Minister for Women, Family and Human Rights, were reported in the Brazilian press in 2019.[126]

121 Robert Beckhusen, "In Manifesto, Mexican eco-terrorists declare war on nanotechnology", *Wired,* 12 March 2013, available at: https://www.wired.com/2013/03/mexican-ecoterrorism/.

122 "Detienen a presunto asesino del investigador Ernesto Méndez Salinas", *La Policíaca,* 27 January 2012, archived from the original at: https://web.archive.org/web/20130316103902/https://www.lapoliciaca.com/nota-roja/detienen-a-presunto-asesino-del-investigador-ernesto-mendez-salinas/.

123 Rigoberto Hernández, "¿Qué es la ITS?", *Instituto Igualdad,* 26 January 2017, available at: https://institutoigualdad.cl/2017/01/26/que-es-la-its/.

124 "Muere uno de los peregrinos agredidos a balazos", *Quadratin Querétaro,* 29 October 2017, available at: https://queretaro.quadratin.com.mx/muere-uno-los-peregrinos-agredidos-balazos/.

125 "Grupo eco-extremista assume autoria de explosão de panela-bomba em Brasília", *Bahia Notícias,* 3 August 2016, available at: https://www.bahianoticias.com.br/noticia/194184-grupo-eco-extremista-assume-autoria-de-explosao-de-panela-bomba-em-brasilia.

126 Thiago Bronzatto and Laryssa Borges, "Líder de grupo terrorista revela plano para matar Bolsonaro", *Veja,* 19 July 2019, available at: https://veja.abril.com.br/brasil/bolsonaro-terror-capa-veja; "Integrante da Sociedade Secreta Silvestre tem plano para matar Bolsonaro", *Correio Braziliense,* 19 July 2019, available at: https://www.correiobraziliense.com.br/app/noticia/politica/2019/07/19/interna_politica,772202/atentado-a-bolsonaro.shtml.

ITS cells claimed responsibility for several attacks in Chile from 2016 to 2019.[127] It said it had posted an explosive package to an executive of Codelco, a Chilean state-owned copper corporation, in January 2017.[128] An ITS-claimed bombing at a bus stop in Santiago in January 2019 injured five people,[129] and ITS also claimed responsibility for sending an explosive package to a senior director of the Chilean metro in March 2019.[130] Cells in Chile included the Sureños Incivilizados and Horda Mística del Bosque (HMB).[131] HMB claimed responsibility for the majority of ITS attacks in Chile between 2016 and 2019.[132]

Figure 2. Photos uploaded to the ITS website between 2016 and 2019, sourced from Archive.org.

Two ITS-affiliated cells also claimed to operate in Buenos Aires, Argentina: Constellaciones Salvajes (CS) and Secta Rojo Sangre. Among the incidents claimed by ITS in Argentina was a package explosion in a postal distribution centre in Monte Grande, Buenos Aires, in December 2017.[133] In 2019, police raids on members of a group called "22 de Agosto", who they said were linked to ITS-Chile, found firearms and components for a vehicle-borne explosive device. ITS had

127 Prado Recabarren and Diego Alfonso, "El lobo solitario", *Universidad de Chile,* 2024, available at: https://repositorio.uchile.cl/handle/2250/198280.

128 "Eco-terrorist parcel bomb explodes at Chilean mining head's home", *The Costa Rica Star,* 14 January 2017, available at: https://news.co.cr/eco-terrorist-parcel-bomb-explodes-at-chilean-mining-heads-home/55249/.

129 "Explosión en Santiago: al menos 5 personas heridas en una parada de autobús en la capital de Chile", *BBC News,* 4 January 2019, available at: https://www.bbc.com/mundo/noticias-america-latina-46765000.

130 Maria Jose Villarroel, "Individualistas Tendiendo a lo Salvaje califica de 'suertudo' a De Grange tras frustrado ataque", *BioBio Chile,* 9 May 2019, available at: https://www.biobiochile.cl/noticias/nacional/region-metropolitana/2019/05/09/individualistas-tendiendo-a-lo-salvaje-califica-de-suertudo-a-de-grange-tras-frustrado-ataque.shtml.

131 "¿Qué es el Eco-extremismo? Análisis de 'Individualistas Tendiendo a lo Salvaje", *Bio-Bio,* 2017, available at: https://media.biobiochile.cl/wp-content/uploads/2017/01/qu-es-el-eco-extremismo-un-anlisis-a-individualistas-tendiendo-a-lo-salvaje.pdf.

132 Prado Recabarren and Diego Alfonso, "El lobo solitario", *Universidad de Chile*, 2024, available at: https://repositorio.uchile.cl/handle/2250/198280.

133 "Hubo una explosión en una sefa del Correo Argentino de Esteban Echeverría", *La Nacion,* 6 December 2017, available at: https://www.lanacion.com.ar/buenos-aires/hubo-una-explosion-en-una-sede-del-correo-argentino-de-esteban-echeverria-nid2088914/.

reportedly said in its messaging that explosives used in Chile had been sent from Argentina.[134] Another police operation in 2022 led to the arrest of a father and son from Buenos Aires, identified via Internet activity from their IP address, on suspicion of involvement in the maintenance of the group's website.[135]

ITS has also claimed responsibility for attacks in Europe, which it says were mounted by its members there. No one was injured when bomb disposal experts carried out a controlled explosion of a crude device that had been left in a public space in Edinburgh, Scotland, in January 2018, for which ITS claimed responsibility both on its website and in an email reportedly sent to local police.[136] A former Greek serviceman, who said he was a member, was found guilty in February 2022 of the attempted bombing in Scotland.[137] In Greece, the group claimed attacks under the name of its "Iconoclastic Sect" and "Nocturnal Hunters" cells, including a bombing at a church in the Kolonaki area of Athens in December 2018. The device injured two people, including a police officer.[138]

The veracity of a significant proportion of ITS claims between 2016 and 2019 was not corroborated by official sources, however. A "bomb" purportedly left in April 2018 by a member of the group in Valencia, Spain, does not appear to have been reported in the Spanish press, which suggests that either the device was so small as to go undetected or the attack did not actually take place.[139] In some instances, the findings of police investigations have contradicted the group's claims of responsibility. The group said in November 2019, for instance, that its members had killed two "tech executives" in California, United States.[140] Police investigations into the two separate cases found no evidence of ITS involvement, however, and instead attributed them to an employee dispute and death by natural causes, respectively.[141]

134 "Detectan lazos entre los anarquistas que atacaron en Chile y un grupo extremista argentino", *Clarin,* November 2019, available at: https://www.clarin.com/politica/detectan-lazos-violencia-chile-grupo-extremista-argentino_0_FWQWxML_.html.

135 "Villa Urquiza: allanaron a un padre y a su hijo por vínculos con un grupo terrorista internacional especializado en bombas", *Infobae,* 16 March 2022, available at: https://www.infobae.com/sociedad/policiales/2022/03/16/villa-urquiza-allanaron-a-un-padre-y-a-su-hijo-por-vinculos-con-un-grupo-terrorista-internacional-especializado-en-bombas/.

136 Andy Shipley, "Mexican anarchist group probed over Princes Street Gardens shoe bomb box", *Daily Record,* 9 May 2020, available at: https://www.dailyrecord.co.uk/news/scottish-news/mexican-anarchist-group-probed-over-21996539.

137 "HMA v Nikolaos Karvounakis", *Judiciary of Scotland,* 16 February 2022, available at: https://judiciary.scot/home/sentences-judgments/sentences-and-opinions/2022/02/16/hma-v-nikolaos-karvounakis.

138 Vassilis Lambropoulos, "Βόμβα στον Αγ.Διονύσιο: Η «Εικονοκλαστική Σέχτα» και οι «οικοτρομοκράτες»", *In*, 28 January 2019, available at: https://www.in.gr/2019/01/28/greece/vomva-ston-ag-dionysio-eikonoklastiki-sexta-kai-oi-oikotromokrates/.

139 "(Spain) 52 Communique of the ITS", *Eco-Extremist Curse,* 23 April 2018, accessed via Archive.org.

140 "(USA) 90 Communique of ITS", *Eco-Extremist Curse,* 9 November 2019, accessed via Archive.org.

141 Mike Moffitt, "Police: Tushar Atre was murdered by people who worked for him", *SFGate,* 21 May 2020, available at: https://www.sfgate.com/bayarea/article/Police-Tushar-Atre-murder-arrests-suspects-15287085.php; Melia Russell, "A 33-year-old tech founder went to Silicon Valley on business and was found dead in her car a week later. Her cause of death was just identified as 'natural causes' following 'an acute manic episode'.", *Business Insider,* 6 February 2020, available at: https://www.businessinsider.com/erin-valenti-cause-of-death-2020-2.

Abuse of digital technologies

Unlike many other violent extremist groups, in South America or globally, ITS has not attempted to maintain an active or widespread official presence on mainstream social networking platforms, probably in part because of its antipathy towards technological progress. Rather, its public online messaging has come primarily via its dedicated website and niche, privacy-focused messaging apps, social networking sites or video-sharing services. The website "Maldición Eco-Extremista" (Eco-Extremist Curse) was ITS's primary messaging platform from at least February 2016, when its first iteration was hosted on the espivblogs.net server, maintained and used by Greek anarchists and ideologically aligned movements globally. The website's interface was built using open-source WordPress software, operating as a simple blog on which the group would post claims of responsibility for attacks, articles and other news in multiple languages. From captured versions of the website on Archive.org, the site appears to have gone offline in the first half of 2017.

Figure 3. Screengrabs of three iterations of ITS's "Eco-Extremist Curse" website, retrieved from Archive.org.

In January 2017 ITS began posting on a new website, located on a subdomain hosted by Altervista, an Italian web hosting company.[142] The website hosted the group's communiqués and had sections for material in multiple languages including English, Turkish, Italian, Spanish, Portuguese, Romanian and Czech. By 2019 the group had a mirror version of the website on the .onion network, accessible via Tor – probably intended as a backup in case the surface web version went offline. Maldición Eco-Extremista also operated a mirror site on a subdomain of WordPress. The websites linked to a network of affiliated websites and publications on espiv.net, Altervista and .onion.

Other information available on the website indicated a sophisticated use of private and encrypted communications tools by ITS's core membership. The group advertised an email address on ProtonMail, an end-to-end encrypted email provider, and a channel "for the publication of ITS communiqué[s]" on Riot (now Element), an encrypted and decentralised messaging platform. The group ran at least one account on Disaporing.ch, a now defunct, privacy-focused social networking service operated by FairSocialNet, a non-profit organisation.[143] It has also shared

142 https://en.altervista.org/.

143 Archived version of diasporing.ch, captured 11 August 2018, available at: https://web.archive.org/web/20180811210311/https://diasporing.ch/.

multimedia content via Vimeo, MediaFire and MediaGoblin, a decentralised media publishing platform, including via .onion domains.[144] In January 2017, for example, the group shared an instructional video on its website titled "how to make a package bomb", with links to LiveLeak, Vimeo and Goblin Refuge via the surface web and the Onion network.

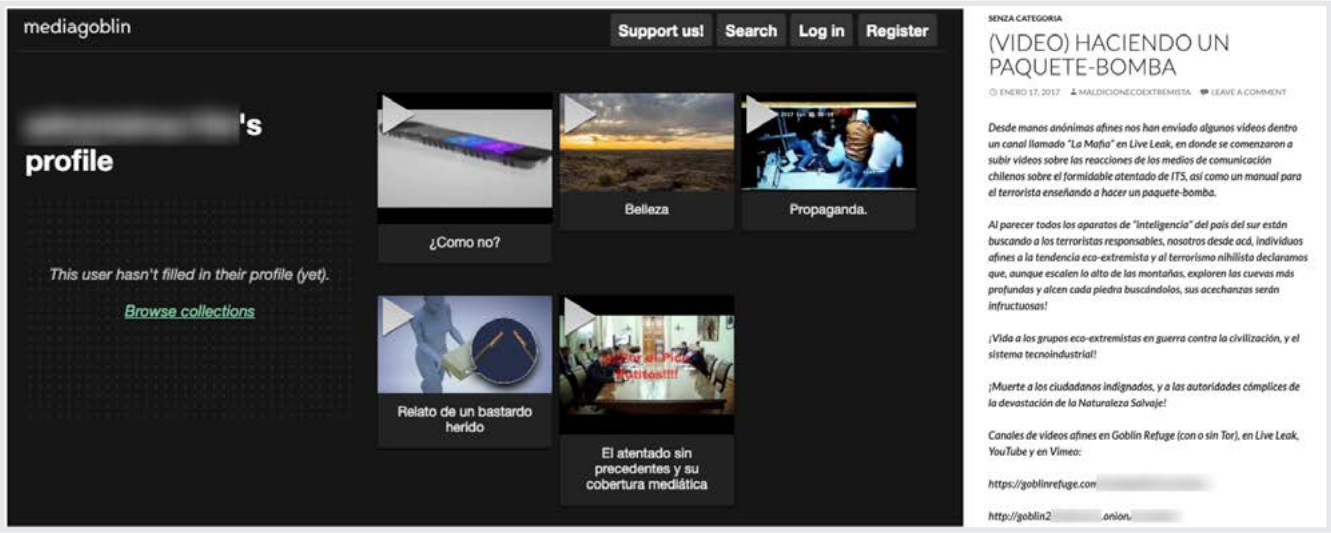

Figure 4. (left) An ITS account on MediaGoblin; (right) a post on Maldición Eco-Extremista titled "How to make a package bomb".

ITS also publicised cryptocurrency wallets in December 2018 to crowdfund its operations. It included crypto wallets relating to Bitcoin, Litecoin, Ethereum, Zcash and Dash. The post said any funds raised would contribute to ITS's "war against civilisation", adding: "contribute and watch the world burn". A lookup on the wallets in July 2024 using publicly available tools indicated that none of them contained any funds. A duplicate version of the post was also shared on Telegra.ph, a publishing tool created by the messaging app Telegram.[145]

The site existed as part of a broader network of anarchist, nihilist or "eco-extremist" blogs and video channels on the surface and dark web. The homepage of "Maldición Eco-Extremista" included links to webpages for 6 magazines, including "*Ajajem*", "*Regresión*", "*Anhangá*" and "*Atassa*"; 10 video channels, 10 "eco-extremist" blogs, 8 recommended websites for "egoistic nihilist terrorism", 11 "related" dark web blogs and 17 other "recommended" blogs that were ideologically close to ITS.[146] One of the group's primary magazines was *Ajajem*, a lengthy manual containing instructional material for attacks, and threats of further violence. Its first publication in July 2019 was 76 pages long and included a diagram on how to make a letter bomb.[147]

144 "Deploying MediaGoblin", *MediaGoblin,* available at: https://mediagoblin.org/.

145 "Telegra.ph Client", *Google Play Store,* available at: https://play.google.com/store/apps/details?id=com.completeapps.telegraph-publisher.

146 Information based on an archived version of Eco-Extremist Curse, captured 26 March 2019 on Internet Archive.

147 Felipe Diaz, "'Ecoterroristas' reaparecen con revista digital y advertencia de nuevos atentados", *La Tercera,* 31 July 2019, available at: https://www.latercera.com/la-tercera-pm/noticia/ecoterroristas-reaparecen-revista-digital-advertencia-nuevos-atentados/761792/.

The core of ITS's online infrastructure, including its primary websites and video channels, was dismantled by law enforcement around 2019. Italian police reportedly arrested a man in Turin, Italy, in March 2022, on suspicion of being a founder and administrator of the ITS website along with four other individuals in Mexico, Brazil, Argentina and Chile. Press reports on the case mentioned the man's role in managing ITS's clandestine exploitation of digital technologies to communicate privately and to publicise the group's operations online via a virtual machine.[148]

Multiple ITS members have been arrested in recent years, and the group's website has been offline since it was seized by the Italian government in the first half of 2022.[149] Open-source research shows that the group's material remains widely available online, however, particularly via a network of anarchist and self-described "eco-extremist" blogs, including on WordPress, Blogspot, EspivBlogs and BlackBlogs. A hip-hop track seemingly dedicated to the group is also accessible on SoundCloud, where, by late 2024, it had been listened to 1,800 times since it was uploaded six years before.[150]

148 Sarah Martinenghi, "Progettava attentati, condannato per terrorismo l'anarchico misantropo Federico Buono", *la Repubblica,* 11 May 2023, available at: https://torino.repubblica.it/cronaca/2023/05/11/news/progettava_attentati_condannato_per_terrorismo_lanarchico_misantropo_dellits_federico_buono-399694448/; Sarah Martinenghi, "'Volevo colpire parchi e metrò': anarchico confessa e poi ritratta", *la Repubblica,* 9 January 2023, available at: https://torino.repubblica.it/cronaca/2023/01/09/news/volevo_colpire_parchi_e_metro_anarchico_confessa_e_poi_ritratta-382691816/.

149 Archived version of Maldición Eco-Extremista, captured 1 July 2022, available at: https://web.archive.org/web/20220701042959/http://www.maldicionecoextremista.altervista.org/.

150 "Salvaje Individualidad", *Iconoclasta,* available at: https://soundcloud.com/nihilahab/salvaje-individualidad.

Right-wing violent extremism in South America: the Brazilian context

Background

Right-wing violent extremism in Brazil shares many of the characteristics discernible in the right-wing violent extremist movements in North America, Europe and Australia. Broadly, it rejects progressive left-wing ideals such as feminism, multiculturalism and 'globalism'. It opposes domestic cultural Marxism, real or perceived, and promotes a Christian nationalist agenda.[151] It is also heavily influenced, however, by its own domestic historical context, including racism and legacies of Nazism and militarism. Despite the country's ethnic diversity, Brazilians continue to experience racial prejudice, discrimination and inequality.[152] Nazism in the country has its roots in the 1920s and 1930s, when a wave of German immigrants settled in the southern states, initially living in relative isolation from broader Brazilian society. Some 4,000 former Third Reich officials also settled there.[153] Brazil was once home to the largest Nazi party outside of Europe, with around 3,000 members during the Second World War.[154] The repressive military dictatorship in Brazil from 1964 to 1985 also continued to influence the ideological mindset of contemporary right-wing extremists there, including through nostalgia for the dictatorship and a glorification of militarisation.[155]

Current threat picture: transnational connections

The threat from right-wing extremism has been steadily increasing in Brazil in recent years, with for example, annual figures on federal police investigations into the promotion of domestic Nazi ideology increasing from 21 to 93 between 2010 and 2020.[156] Glorification of the armed forces manifested particularly under the right-wing administration of Jair Bolsonaro – a retired military officer who served as Brazil's president from 2018 to 2020. Critics of Bolsonaro's government

151 Odilon Caldeira Neto, "The Brazilian far-right and the path to January 8th", *Global Network on Extremism and Technology,* 23 January 2023, available at: https://gnet-research.org/2023/01/23/the-brazilian-far-right-and-the-path-to-january-8th/.

152 Shari Wejsa and Jeffrey Lesser, "Migration in Brazil: The making of a multicultural society", *Migration Policy Institute,* 29 March 2018, available at: https://www.migrationpolicy.org/article/migration-brazil-making-multicultural-society; Edward Telles, "Racial Discrimination and Miscegenation: The Experience in Brazil", *United Nations Chronicle*, available at: https://www.un.org/en/chronicle/article/racial-discrimination-and-miscegenation-experience-brazil.

153 Stephen Gibbs, "The police officers hunting Brazil's 'neo-Nazis'", *The Sunday Times,* 3 September 2023, available at: https://www.thetimes.com/world/latin-america/article/brazil-wary-of-its-southern-states-after-raids-target-neo-nazis-wz2n87m7d.

154 Mattia Bottino, "What is left of Bolsonarism: The many faces of the Brazilian far-right", *Eurac Research,* 14 May 2024, available at: https://www.eurac.edu/en/blogs/eureka/what-is-left-of-bolsonarism-the-many-faces-of-the-brazilian-far-right.

155 Fanny Lothaire, Valeria Saccone, Louise Raulais, Anne-Laure Desarnauts and Amin Guidara, "Brazil still grappling with dark period of military dictatorship, 60 years on", *France24,* 3 May 2024, available at: https://www.france24.com/en/tv-shows/revisited/20240503-brazil-still-grappling-with-dark-period-of-military-dictatorship-60-years-on.

156 Beatriz Farrugia, "The Alarming Increase in Neo-Nazi Groups in Brazil", no date, available at: https://biafarrugia.github.io/neo-nazi-brazil/.

have claimed that it created a permissive environment for right-wing extremism.[157] In 2019, for example, Bolsonaro, reversing an earlier government policy, reinstated commemorations for the 1964 coup that had begun the two decades of military dictatorship in the country.[158] During its tenure, the administration also faced accusations of direct affiliation with fascism.[159] In January 2020, then Culture Secretary Roberto Alvim was fired after appearing to copy the words of Joseph Goebbels, Hitler's Minister of Propaganda, in a speech promoted on social media.[160]

Social media is reported to have played a significant role in the violent attack on federal government buildings in Brasilia on 8 January 2023.[161] The incident shared characteristics with the pro-Trump insurrection in Washington DC on 6 January the previous year.[162] It followed the electoral defeat of Bolsonaro in favour of his rival, President Lula da Silva. Months of social media mis- and disinformation relating to electoral fraud in the run-up to the presidential election, combined with ongoing vocal support for domestic military intervention, culminated in online calls for a putschist mobilisation on Telegram and WhatsApp.[163] Around 4,000 demonstrators arrived in Brasilia on buses from around the country; they proceeded to descend on three government buildings, vandalising them and stealing property there. By the end of the day, police had arrested at least 300 people.[164]

Right-wing violent extremists in Brazil have mounted several attempted or completed acts of mass murder in recent years. A juvenile gunman who killed 3 people and injured 13 others at two schools in Aracruz, southern Brazil, in November 2022, wore a swastika arm band and a skull mask during the attack.[165] In three separate, similar attacks in schools in February,

157 Steven Grattan, "Neo-Nazi groups multiply in a more conservative Brazil", *Reuters,* 13 June 2023, available at: https://www.reuters.com/world/americas/neo-nazi-groups-multiply-more-conservative-brazil-2023-06-13/; Gibbs, "The police officers hunting Brazil's 'neo-Nazis'".

158 Brazil: Bolsonaro Celebrates Brutal Dictatorship", *Human Rights Watch,* 27 March 2019, available at: https://www.hrw.org/news/2019/03/27/brazil-bolsonaro-celebrates-brutal-dictatorship; Anne Warth and Julia Lindner, "Planalto confirma ordem de Bolsonaro para comemorar aniversário do golpe de 1964", *Estadão,* 25 March 2019, available at: https://www.estadao.com.br/politica/planalto-confirma-ordem-de-bolsonaro-para-comemorar-aniversario-do-golpe-de-1964/.

159 Tom Phillips, "Jair Bolsonaro denies he is a fascist and paints himself as a Brazilian Churchill", *The Guardian,* 30 October 2018, available at: https://www.theguardian.com/world/2018/oct/30/jair-bolsonaro-denies-he-is-a-fascist-brazilian-churchill.

160 Gil Alessi, "Secretário da Cultura de Bolsonaro imita fala de nazista Goebbels e é demitido", *El País*, 17 January 2020, available at: https://brasil.elpais.com/brasil/2020-01-17/secretario-da-cultura-de-bolsonaro-imita-discurso-de-nazista-goebbels-e-revolta-presidentes-da-camara-e-do-stf.html.

161 Damien Leloup, "Riots in Brazil: An attempted insurrection openly organised on social media", *Le Monde,* 10 January 2023, available at: https://www.lemonde.fr/en/international/article/2023/01/10/riots-in-brazil-an-attempted-insurrection-organized-openly-on-social-media_6010980_4.html; Dr. Bàrbara Molas, "The Insurrection Wave: A comparative assessment of anti-government attacks in Germany, the US, and Brazil", International Centre for Counter-Terrorism, September 2023, available at: https://www.icct.nl/sites/default/files/2023-09/Molas%20-%20The%20Insurrection%20Wave%20final%20to%20publish.pdf.

162 Interview with Débora Salles, Netlab, 14 June 2024.

163 Ariel Goldstein, "The Hate Ministries: far-right social media extremism in Argentina and Brazil", *Global Network on Extremism and Technology,* 9 July 2024, available at: https://gnet-research.org/2024/07/09/the-hate-ministries-far-right-social-media-extremism-in-argentina-and-brazil/.

164 "Terrorismo em Brasília: o dia em que bolsonaristas criminosos depredaram Planalto, Congresso e STF", *g1,* 8 January 2023, available at: https://g1.globo.com/df/distrito-federal/noticia/2023/01/08/o-dia-em-que-bolsonaristas-invadiram-o-congresso-o-planalto-e-o-stf-como-isso-aconteceu-e-quais-as-consequencias.ghtml.

165 "Boy, 16, 'wore swastika' during fatal school shootings in Brazil", *The Guardian,* 26 November 2022, available at: https://www.theguardian.com/world/2022/nov/26/boy-16-killed-three-people-and-wounded-13-in-two-schools-in-brazil.

March and August 2023 in São Paulo, the assailants all exhibited signs of right-wing violent extremism combined with other ideologies.[166] The incidents followed multiple other attacks on schools by lone actors or small cells, although not all of them are believed to have been motivated by right-wing extremism.[167] Data released by the Ministry of Justice and Public Security in October 2023 indicated that the police had made more than 400 arrests in the first six months of an initiative to tackle the threat of school attacks,[168] and most of the perpetrators being minors had been exposed to a wide range of hateful and violent content online.[169]

Other such cases indicate the presence of larger, more organised groups of right-wing extremists. In September 2022, police in the southern Brazilian state of Santa Catarina raided a meeting of a suspected local chapter of the Hammerskins, a neo-Nazi group founded in Dallas, United States, in 1988.[170] One of the eight individuals arrested had previously been convicted of the attempted murder of three Jewish people, and police found a bomb-making guide on a device found at the property.[171] In another case, police said a neo-Nazi cell called "The New SS of Santa Catarina" had manufactured 3D-printed firearms and discussed killing homeless people.[172]

Digital technologies are likely to have enabled the internationalisation of right-wing extremism operating in Brazil. Portuguese-language networks have interacted with global right-wing violent extremist organisations and movements online, including those affiliated with Atomwaffen Division, which originated in the United States but has since produced affiliates globally.[173] In an indication of the involvement of Brazilians in violence internationally, Telegram posts made in recent years by the administrators of channels affiliated with the neo-Nazi Misanthropic Division have indicated donations to the group from Brazilian supporters, and the physical presence of Brazilian members in its combat operations in Ukraine.[174]

166 Julia Vargas Jones, "Brazil Cracks Down on Surprising New Threat: Neo-Nazis", The New York Times, 7 November 2023, available at: https://www.nytimes.com/2023/11/07/world/americas/brazil-neo-nazis-extremism.html.

167 Interview with Kerry-Ann Barrett and Mariana Gonzalez, Organization of American States (OAS), 6 June 2024; Lais Martins, "Inspired by Columbine, Brazil pair kill 8 and themselves in school shooting", *Reuters,* 14 March 2019, available at: https://www.reuters.com/article/world/inspired-by-columbine-brazil-pair-kill-8-and-themselves-in-school-shooting-idUSKBN1QU1UX/; "Police: Student kills 2, wounds 4 in Brazil school shooting", *Associated Press,* 20 October 2017, available at: https://apnews.com/general-news-603d633fd7bb4d3d9e7b62b5f2c03b0a.

168 "Lançada em abril, Operação Escola Segura já efetuou 400 prisões e apreensões", *Ministério da Justiça e Segurança Pública,* 3 October 2023, available at: https://www.gov.br/mj/pt-br/assuntos/noticias/lancada-em-abril-operacao-escola-segura-ja-efetuou-400-prisoes-e-apreensoes.

169 Michele Prado, "Extremismo violento em ambiente escolar", Nota Tecnica 15, Monitor do Debate Político no Meio Digital - Grupo de Políticas Públicas para o Acesso à Informação – Escola de Artes, Ciências e Humanidades – USP, March 2023, available at: https://www.monitordigital.org/wp-content/uploads/2023/03/nota-tecnica-15.pdf.

170 Caroline Borges, "Neonazistas presos em SC e RS recrutavam jovens de outras células através de 'sistema rigoroso', diz delegado", *Globo,* 3 April 2023, available at: https://g1.globo.com/sc/santa-catarina/noticia/2023/04/03/grupo-de-neonazistas-preso-recrutava-jovens-de-outras-celulas-atraves-de-sistema-rigoroso-diz-delegado-de-sc.ghtml.

171 Gibbs, "The police officers hunting Brazil's 'neo-Nazis'".

172 Mauren Luc, "Suspeitos de integrarem grupo neonazista são presos em SC", *Portal Geledés,* 25 October 2022, available at: https://www.geledes.org.br/suspeitos-de-integrarem-grupo-neonazista-sao-presos-em-sc/.

173 Ashley Mattheis, "Atomwaffen Division and its affiliates on Telegram: Variations, Practices, & Interconnections", *Resolve Network,* April 2022, available at: https://www.resolvenet.org/system/files/2022-04/RSVE_RST_AWDandAffiliatesTelegram_Mattheis-Apr2022.pdf.

174 Seth Harp, "Foreign fighters in Ukraine could be a time bomb for their home countries", *The Intercept,* 30 June 2022, available at: https://theintercept.com/2022/06/30/ukraine-azov-neo-nazi-foreign-fighter/.

To forge international connections, there is evidence that Nova Resistência, a Brazilian neo-fascist group, has also participated in sending Brazilian foreign fighters to join the war in Ukraine on the side of the Russian Federation. Raphael Machado, the group's leader, is reported to have led the Frente Brasileira de Solidariedade com a Ucrânia (the Brazilian Front for Solidarity with Ukraine), a group that operated in support of Russia's proxies in the Donbas region of Ukraine. The group was formed in 2011 following the collapse of an American white nationalist organisation, American Front. The Brazilian chapter is likely the most developed and active of its branches, and it has an extensive online presence.

Nova Resistência engages frequently with actors in other countries. In addition to its affiliates in Canada and Italy, in 2022 it announced the formation of the Central de Liberación Americana ("Central Committee on American Liberation"), which it said would act as a "meeting place" for ideologically aligned groups across Latin America. The network purportedly includes groups in Peru, Colombia, Argentina, Mexico and Chile.[175] Although it has white supremacist origins, it promotes the "Fourth Political Theory" ideology of Aleksandr Dugin, a Russian ideologue, which purports to unite right- and left-wing extremist groups internationally with the aim of destabilising democracy.[176] Nova Resistência's website shares a Moscow-based IP address with several Russia-aligned disinformation websites. The company administering the address also administers the website of DarkSide, a ransomware group believed to be originated in Russia.[177] Nova Resistência has a large following on mainstream social media platforms, with 23,000 and 15,000 subscribers on YouTube and X respectively, in addition to accounts on Telegram, Vkontakte and Odysee.[178]

Figure 5. Members of Misanthropic Division Brasil, sourced from Telegram in July 2024.

Abuse of digital technology

Right-wing extremist networks are extensive users of digital technologies in Brazil. SaferNet, an organisation that works with the Brazilian government to combat online crime, recorded 1,200 complaints in 2017 relating to the abuse of digital technologies by neo-Nazis. By 2021, the

175 *Ibid.*

176 "The Dugin International", *Irregular Horizons,* 8 May 2023, available at: https://irregularhorizons.substack.com/p/the-dugin-international.

177 "Exporting Pro-Kremlin Disinformation: The Case of Nova Resistência in Brazil", US Department of State Global Engagement Center, 19 October 2023, available at: https://www.state.gov/gec-special-report-exporting-pro-kremlin-disinformation-the-case-of-nova-resistencia-in-brazil/.

178 Interview with Leonardo F. Nascimento, Digital Humanities Laboratory at the Universidade Federal da Bahia, 9 July 2024.

volume and frequency of these complaints had increased to 14,500 annually.[179] These figures have since fallen significantly, possibly due to a migration by right-wing extremist networks to more private online spaces. But reports of other hate crimes have continued to increase: complaints of xenophobia, for example, increased from 1,097 in 2021 to 10,686 in 2022. Complaints relating to anti-LGBTQ+ narratives, misogyny and racism also all increased significantly between 2021 and 2022.[180]

Online manifestations of right-wing extremism in Brazil comprise a broad ecosystem across a range of different platforms and websites. In a country that consumes large volumes of audio-visual content, extremists particularly favour TikTok and YouTube, where potentially illegal hate speech or incitement in video or audio may be harder to detect than in other formats.[181] Right-wing extremist "influencers" and related organisations have also been reported to have monetised their online activity with significant audiences on mainstream platforms. This dynamic has helped blur the lines between fringe extremism and mainstream public discourse.[182]

Explicit violent right-wing extremism in Brazil is prevalent in the more private or insular online spaces. They include platforms like WhatsApp, Telegram, Signal and Discord, where violative content and accounts are the focus of varying levels of moderation by companies, in part owing to the inaccessibility of communications on end-to-end encrypted applications.[183] An extensive Portuguese-language community also exists on StormFront, a long-standing white supremacist forum heavily used by US-based extremists.[184] Within this sub-forum there is a Brazil-specific section, where the most popular of the 2,400 threads had been viewed by more than 1.6 million people by July 2024.

179 *Ibid.*

180 "XENOFOBIA CRESCEU 874% NA INTERNET EM 2022", *Livre Concorrência,* 9 February 2023, available at: https://livreconcorrencia.com.br/xenofobia-cresceu-874-na-internet-em-2022/.

181 Interview with Débora Salles, Netlab, 14 June 2024; Isabela Palhares and Isabella Menon, "Com táticas de disfarce, conteúdo nazista se dissemina pelo TikTok", *Folha de S.Paulo,* 28 October 2023, available at: https://www1.folha.uol.com.br/cotidiano/2023/10/com-taticas-de-disfarce-conteudo-nazista-se-dissemina-pelo-tiktok.shtml.

182 Interview with Débora Salles, Netlab, 14 June 2024; Interview with the Organization of American States (OAS), 6 June 2024.

183 "TSE desmonetiza quatro canais e suspende divulgação de documentário", *Tribunal Superior Eleitoral,* 20 October 2022, available at: https://www.tse.jus.br/comunicacao/noticias/2022/Outubro/tse-desmonetiza-quatro-canais-e-suspende-divulgacao-de-documentario; Interview with Débora Salles, Netlab, 14 June 2024; Interview with Kerry-Ann Barrett and Mariana Gonzalez, Organization of American States (OAS), 6 June 2024;

184 "Stormfront", *Southern Poverty Law Center,* no date, available at: https://www.splcenter.org/fighting-hate/extremist-files/group/stormfront; Alex Newhouse, Gabriela Zayas-Alom, Sophie Liebel, Paulo Magalhães de Paula, Carles Andreu, and Mike Donnelly, "CTEC Investigation: White Supremacy, Anti-Semitism, and Violence in Spanish and Portugese Online Communities", *Center on Terrorism, Extremism and Counterterrorism, Middlebury Institute of International Studies at Monterey,* 31 July 2020, available at: https://www.middlebury.edu/institute/academics/centers-initiatives/ctec/ctec-publications/ctec-investigation-white-supremacy-anti.

Figure 6. Screengrab of the Brazil section of the white nationalist StormFront forum, captured in July 2024.

Chan sites also play a role in the digital socialisation of right-wing extremists operating in Brazil, including radicalisation to violence. Sites such as 55chan, Dogolachan, Hispachan and 4chan are popular with Spanish- and Portuguese-speaking right-wing extremists, and some have been linked to acts of violence in Brazil. Probably the most notorious of these, Dogolachan, was founded in 2012. The site's community is similar in ideology and behaviour to that of the predominantly English-language website 8chan, which was used by the perpetrators of right-wing mass shootings in Christchurch, New Zealand; Poway, California; and El Paso, Texas, all in 2019.[185] Dogolachan users, known as "dogoleiros", have engaged in trolling, doxxing, death threats and "flamebaiting"[186] against public figures and activists, and have also explicitly inspired and celebrated attacks.[187]

Following its creation in 2012, Dogolachan was available on the surface web, but it migrated to the deep web upon the arrest of one of its creators in 2018. It had gained notoriety that year after its users voiced support for the perpetrators of a mass shooting in a school in Suzano, São Paulo. The Brazilian website owner was sentenced to more than 40 years for offences including terrorism, dissemination of child sexual abuse material, racism, and incitement to commit crimes.[188] As with 8chan, there have been several acts of murder or other forms of violence committed by its users. In 2018, a moderator on the forum announced his intention to take his own life. Encouraged by other forum members to kill minorities before doing so, the individual shot and killed a woman in the street in São Paulo before killing himself.[189]

185 "What is 8chan?", *BBC News,* 5 August 2019, available at: https://www.bbc.com/news/blogs-trending-49233767.

186 Content or messages posted online that are intended to provoke anger in a target audience.

187 Leonardo Coelho and Maria Teresa Cruz, "Procurador aponta incapacidade da PF em monitorar fóruns de ódio na internet", *Ponte,* 15 March 2019, available at: https://ponte.org/procurador-aponta-incapacidade-da-pf-em-monitorar-foruns-de-odio-na-internet/; Leonardo Coelho and Robert Evans, "Dogolachan and the ghost of massacres past", *Bellingcat,* 7 November 2019, available at: https://www.bellingcat.com/news/2019/11/07/dogolachan-and-the-ghost-of-massacres-past/; "Chans, máquinas de ódio na internet, ganham notoriedade após massacre de Suzano", *Journal do Brasil,* March 2019, available at: https://www.jb.com.br/pais/2019/03/991058-chans--maquinas-de-odio-na-internet--ganham-notoriedade-apos-massacre-de-suzano.html.

188 Leonardo Coelho and Maria Teresa Cruz, "Procurador aponta incapacidade da PF em monitorar fóruns de ódio na interne".

189 *Ibid.*

An investigation on Dogolachan in July 2024 in preparation for this report found recent examples of users expressing support for mass shootings and other forms of indiscriminate violence there, including in schools. Racism, misogyny, xenophobia and anti-LGBTQ+ narratives were also prevalent. There were indications of advanced technical knowledge among some users, too, including an interest in hacking and other forms of cybercrime. On the /opsec/ board of Dogolachan in June 2024, for example, a user requested information on data breach sources. The investigation also identified examples of doxxing on 55chan, targeting a Brazilian influencer, and the listing of the IP addresses of targets perceived by the site's users as being linked to Israeli military operations in Gaza.

Another case illustrates the potential impact of cyber-attacks to stoke right-wing extremism in Brazil. During the municipal elections in November 2020, malicious actors targeted the Superior Electoral Court (TSE) in a Distributed Denial-of-Service (DDoS) attack. The attack resulted in outages to the TSE's website and some of its other services. The attackers also leaked a TSE database online, which investigators believe they had accessed around a month before pub lishing it online.[190] According to SaferNet the attacks, described as a "coordinated and planned operation", aimed at "discrediting the Electoral Court and eventually alleging fraud in the result", had no impact on the vote count. But they reportedly led to an increase in claims from right-wing conspiracy theorists that the electoral process was fraudulent, particularly as the vote count was unexpectedly delayed, for an unrelated reason.[191] According to the TSE, the hackers' IP address was in Portugal, indicating that they were either based there or had coordinated the attack via computers there. Later that month, Portuguese police arrested the leader of a hacker group called CyberTeam on suspicion of responsibility for the attack. The 19-year old man said that while he considered himself anti-government, he had not intended to fuel right-wing conspiracy theories in Brazil – rather, he had wanted to mount a "small protest" demanding investigations into prisons in Brazil, Portugal and elsewhere.[192]

190 Patricia Campos Mello, "Investigação aponta operação coordenada em ataque ao TSE e postagens alegando fraude", *Folha de S.Paolo,* 16 November 2020, available at: https://www1.folha.uol.com.br/poder/2020/11/investigacao-aponta-operacao-coordenada-em-ataque-a-tse-e-postagens-alegando-fraude.shtml.

191 Rafael Arbulu, "Ataque ao TSE foi ação coordenada e planejada para as eleições, diz ONG", *Olhar Digital,* 16 November 2020, available at: https://olhardigital.com.br/2020/11/16/seguranca/ataque-ao-tse-foi-acao-coordenada-e-planejada-para-as-eleicoes-diz-ong/.

192 Vinicius Valfre, "'Não sou um criminoso, sou uma boa pessoa', diz hacker preso", *Terra,* 29 November 2020, available at: https://www.terra.com.br/noticias/eleicoes/nao-sou-um-criminoso-sou-uma-boa-pessoa-diz-hacker-preso,bfc85b25ad55540a980640e22ae275bcro9hsg3e.html; Raphael Hernandes, "Grupo hacker que atacou o TSE é conhecido por iniciativas semelhantes", *Folha de S.Paolo,* 16 November 2020, available at: https://www1.folha.uol.com.br/poder/2020/11/grupo-hacker-que-atacou-o-tse-e-conhecido-por-iniciativas-semelhantes.shtml.

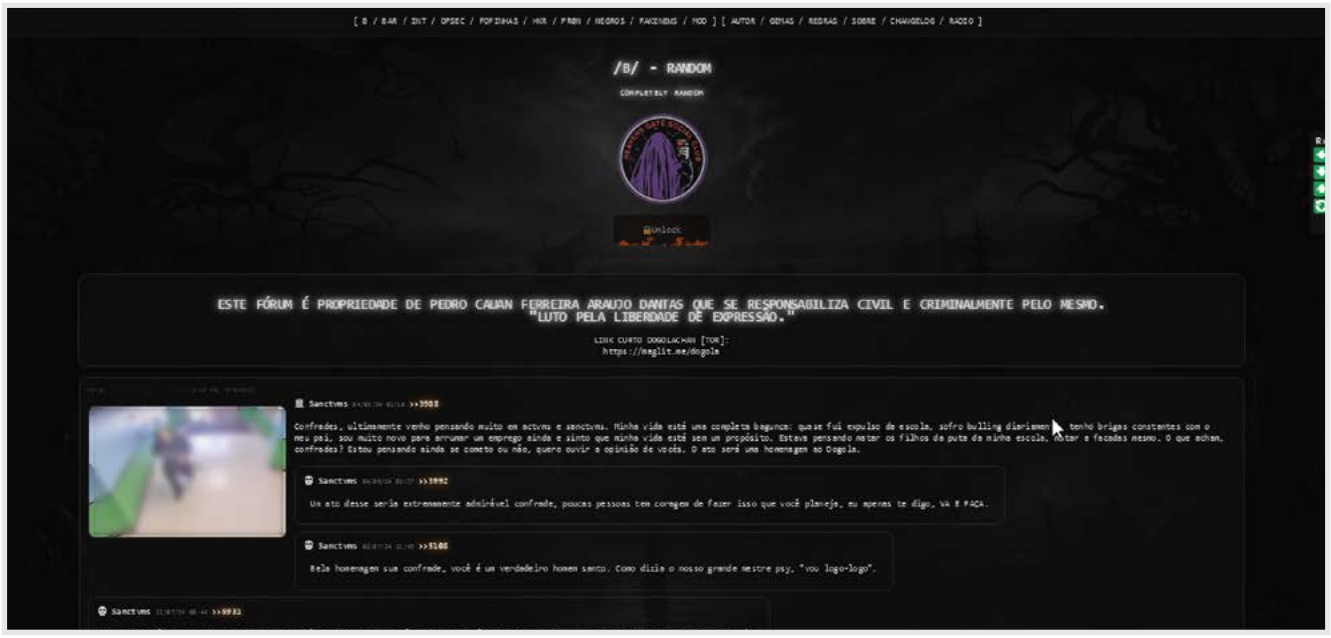

Figure 7. A Dogolachan user enquires about data breach sources, captured in June 2024.

White Supremacy in Africa: the South African context

Background

Violent Afrikaner nationalism as a manifestation of right-wing extremism has a long and complex history in South Africa.[193] Since at least 1910, when British rule was imposed in the Union of South Africa following the end of the Anglo-Boer wars, extreme right-wing Afrikaner nationalists have resisted integration with other ethnic groups, in particular black South Africans. These right-wing extremists broadly subscribe to a belief in the supremacy of the Afrikaner race and culture, and to the goal of an independent ethnostate known as an Afrikaner Volkstaat (People's State).[194] Also crucial to the ideology driving right-wing violence in South Africa is a religious belief system called Israel Vision.[195]

Over the past century there have been a number of flashpoints in South Africa relating to right-wing extremist violence. During the Second World War, for example, a fascist paramilitary organisation called Ossewa Brandwag (OB), with ties to National Socialism, mounted a series of attacks domestically in an attempt to disrupt the pro-British national war effort, including through intimidation, assassinations, and bombings targeting national infrastructure.[196] In the 1970s, the right-wing violent extremist organisation Afrikaner Weerstandsbeweging (Afrikaner Resistance Movement, AWB) was founded. At its peak in the 1980s and 1990s the AWB had as many as 15,000 members, and around ten times as many active sympathisers.[197]

In the last two decades of the 20th century, the AWB was responsible for multiple acts of political violence in South Africa. In April 1994, for example, members of the group mounted a series of bombings around Johannesburg, including at sites where black South Africans congregated, such as the International Airport and other transport hubs.[198] Following the collapse of apartheid post-1994, deep divisions emerged in the extreme right-wing Afrikaner movement, although further instances of violence continued to occur in the following years. In October 2002, for example, a group known as the Boeremag (Boer Force) detonated seven bombs in Soweto, a large black township near Johannesburg, killing one woman.[199] The group also plotted to

193 Wessel Visser, "Labour and Right-Wing Extremism in the South African Context – A Historical Overview".

194 *Ibid.*

195 Interview with Johannes Vreugdenburg, Individual Expert and Former Police, 8 July 2024; Interview with Willem Els, Institute for Security Studies, 28 June 2024.

196 *Ibid.*

197 *Ibid.*

198 "Terreblanche accepts bomb guilt", *BBC News,* 18 June 1998, available at: http://news.bbc.co.uk/1/hi/world/africa/115690.stm.

199 Ruth Maclean, "Supremacists jailed over Mandela murder plot", *The Times,* 30 October 2013, available at: https://www.thetimes.com/article/supremacists-jailed-over-mandela-murder-plot-sgpg5pwdg6s.

overthrow the government, in an operation intended to begin with the assassination of Nelson Mandela in a roadside bombing.[200]

In November 2019 the South African police arrested members of a group called the National Christian Resistance Movement (NCRM), also known as "Crusaders", on suspicion of plotting attacks against black South Africans, including through the use of biological weapons. Upon the prosecution of the group's leader in 2022, a National Prosecuting Authority spokesperson said the man had claimed to have been "ordained" by God to "reclaim South Africa for white people", adding that the group had planned to "attack government institutions" including "police and military institutions". The statement said that the man had "also identified townships and informal settlements occupied by African persons as targets for attack".[201]

Current threat picture

The threat posed by domestic right-wing violent extremist groups has reduced in South Africa since its peak in the late 20th century.[202] Right-wing violent extremism in South Africa in 2024 lacks popular support, but several paramilitary and extremist groups remain active. According to the AWB's website, the group continues to "campaign for the freedom struggle of the Boer people". Under its current leader, Steyn von Rönge, it purportedly aims to "let the Boer people live in a safe haven on their own territory in their fatherland", while criticising the "communist-minded state and government order". As of 2020, the AWB was reported to have around 5,000 members.[203] Groups have become more inward-facing, diffused and uncoordinated than in previous years, and they are now unlikely to gain the support of the majority of Afrikaners.[204] Racism is still prevalent among the groups that remain active, however, and they continue to believe in the ideal of a sovereign ethnostate for Afrikaners. The narratives pushed by extremist groups in the country are also still liable to resonate with certain sections of the population there, including narratives involving latent racism, religious-political identity, domestic violent crime and issues of perceived Afrikaner marginalisation and socio-economic threats.[205]

200 "White extremists' trial resumes in Jo'burg", *Al Jazeera,* 5 August 2003, available at: https://www.aljazeera.com/news/2003/8/5/white-extremists-trial-resumes-in-joburg; Martin Schonteich and Henri Boshoff, "'Volk Faith and Fatherland: The Security Threat Posed by the White Right", *Institute for Security Studies*, 1 April 2003.

201 Nicole McCain, "Right-wing leader Harry Knoesen jailed for life for plotting terror attacks on black people", News24, 28 September 2022, available at: https://www.news24.com/news24/southafrica/news/right-wing-leader-harry-knoesen-jailed-for-life-for-plotting-terror-attacks-on-black-people-20220928.

202 Interview with Johannes Vreugdenburg, Individual Expert and Former Police, 8 July 2024; Interview with Willem Els, Institute for Security Studies, 28 June 2024; Raeesah Cassim Cachalia and Albertus Schoeman, "Violent Extremism in South Africa: Assessing the Current Threat", *Institute for Security Studies,* May 2017, available at: https://issafrica.s3.amazonaws.com/site/uploads/sareport7.pdf; Max du Preez, "Right-wing Extremism has run out of steam", Vrye Weekblad, 10 November 2023, available at: https://www.vryeweekblad.com/en/opinions-and-debate/2023-11-10-right-wing-extremism-has-run-out-of-steam/.

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

204 Schoeman, "Violent Extremism in South Africa".

205 Interview with Bobuin Jr Valery Gemandze Oben and Gugu Nonjinge, Centre for the Study of Violence and Reconciliation (CSVR), 6 June 2024.

The issue of farm murders (known as Plaasmoorde) is prominent in the narratives of right-wing extremists in South Africa – a country that experiences high rates of violent crime, including burglary and murder.[206] Although most perpetrators of these crimes are financially motivated, and target black people,[207] a perception remains among some white South Africans that such crimes targeting Afrikaners are racially motivated.[208] Right-wing extremists, both in South Africa and internationally, have long focused on the issue of farm murders, claiming that violent crime is being directed at the white South African minority as a whole in an effort ultimately to diminish the group.[209] These domestic narratives have intertwined with global right-wing extremist claims of the perceived disenfranchisement of white people, such as the conspiracy theories of an ongoing "great replacement" or "white genocide".[210]

A religious philosophy known as Israelvisie (Israel Vision) is fuelling racism against black people among a minority of white South Africans. This belief system is rejected by mainstream Afrikaner theology, so its adherents mostly meet digitally or in private, rather than in dedicated places of worship. Followers of Israel Vision (which is sometimes referred to as a cult) believe that the bloodline of white Afrikaner South Africans can be traced back to biblical Israelites.[211] They use this claim to justify the revival of racial segregation and to proclaim the Afrikaner Volkstaat a divine right.[212] Israel Vision has been linked to several of the violent extremist attacks in South Africa, including the "Crusaders" plot in 2019 and the Boeremag bombings in the 1990s.[213]

In an indication of the ongoing threat posed by right-wing violent extremism in South Africa, a national risk assessment of terrorism financing in June 2024 cited the country's "history of racial domination and violence" as contributing to its being a "fertile breeding ground for white supremacist hate groups".[214] It said domestic right-wing extremist groups were engaged in ongoing "quasi-military training" and the recruitment of members for their organisations, and specifically referred to the "possibility of lone actor attacks" as being a "national security concern".[215]

206 "Crime in South Africa up in 2022/23", *Department of Statistics, Republic of South Africa,* 24 August 2023, available at: https://www.statssa.gov.za/?p=16562.

207 Geoff Hill, "What's the truth about South Africa's 'genocide' of white farmers?" *The Spectator,* 29 December 2023, available at: https://www.spectator.co.uk/article/whats-the-truth-about-south-africas-genocide-of-white-farmers/; Interview with Johannes Vreugdenburg, Individual Expert and Former Police, 8 July 2024.

208 Interview with Willem Els, Institute for Security Studies, 28 June 2024.

209 Visser, "Labour and Right-Wing Extremism in the South African Context – A Historical Overview".

210 Carla Hill and Mark Pitcavage, "The Racist Obsession with South African "White Genocide", *Anti-Defamation League,* 24 August 2018, available at: https://www.adl.org/resources/blog/racist-obsession-south-african-white-genocide.

211 Rebecca Davis, "Israel Vision – How the religious cult that drove the Boeremag still flourishes online", *Daily Maverick,* 29 May 2022, available at: https://www.dailymaverick.co.za/article/2022-05-29-israel-vision-how-religious-cult-that-drove-boeremag-still-flourishes-online/.

212 *Ibid.*

213 Leonie Meyfarth and Marius Nel, "Israelvisie, die Nuwe Suid-Afrika en 'Afrikaners'", *In Die Skriflig / In Luce Verbi,* Vol. 57, No. 1, March 2023, available at: https://indieskriflig.org.za/index.php/skriflig/article/view/2917.

214 "South African National Terrorism Financing Risk Assessment", *Financial Intelligence Centre,* 24 June 2024, available at: https://www.fic.gov.za/wp-content/uploads/2024/06/National-risk-assessment-%E2%80%93-Terrorist-financing-national-risk-assessment-2024.pdf.

215 *Ibid.*

Several other paramilitary or survivalist groups remain active in South Africa. Kommandokorps, Suidlanders, Bittereinders and Boerelegioen are examples of groups that claim to operate in defence of white Afrikaners, providing military-style training for young people in the name of community protection.[216] The Suidlanders, a prominent example of a domestic group which explicitly believes in a coming race war, has long been a vocal promoter of the "white genocide" conspiracy theory, particularly with regard to farm murders.

These groups purport to exist for defensive purposes and are not believed to be actively planning offensive violence.[217] But all claim to be preparing to activate in the event of civil unrest. Given that the threshold for action by these groups is poorly defined, and the levels of violent crime in South Africa (including farm murders) remains high, there remains a risk that future violent events may act as a catalyst for action by militant right-wing extremists at an individual or group level.[218] Indeed, the national risk assessment report of June 2024 specifically referred to the "possibility of lone actor attacks" as being a "national security concern".[219]

Abuse of digital technologies

The cyber-enabled threats from networks affiliated with right-wing violent extremism in South Africa appear to have increased in recent years.[220] While the use of digital technologies was not a predominant characteristic of the perpetrators of violent extremist bombings or other acts of violence in the 1990s and early 2000s, right-wing extremists involved in the 2019 "Crusaders" plot heavily exploited digital platforms to communicate and plan their attacks. The group made prolific use of WhatsApp to communicate internally, even appointing a "social media manager" to administer its accounts.[221] The group's leader, Harry Knoesen, had reportedly created accounts on Facebook and other social media platforms in an attempt to solicit broader support, including from within the South African National Defence Force.[222]

In the broader right-wing extremist ecosystem in South Africa, many of the paramilitary groups also maintain a public Internet presence. This study found no evidence that South African right-wing extremists are using digital technologies to mount offensive cyber operations. Groups

216 Max du Preez, "Right-wing extremism has run out of steam", *Vrye Weekblad,* 10 November 2023, available at: https://www.vryeweekblad.com/en/opinions-and-debate/2023-11-10-right-wing-extremism-has-run-out-of-steam/.

217 Interview with Johannes Vreugdenburg, Individual Expert and Former Police, 8 July 2024; Interview with Willem Els, Institute for Security Studies, tra Els e 28 June 2024.

218 Interview with Willem Els, Institute for Security Studies, 28 June 2024.

219 "South African National Terrorism Financing Risk Assessment".

220 Interview with Johannes Vreugdenburg, Individual Expert and Former Police, 8 July 2024; Interview with Willem Els, Institute for Security Studies, 28 June 2024.

221 Vincent Cruywagen, "Witness gives damning testimony about 'General' Harry Knoesen's right-wing insurrection plot", *Daily Maverick,* 12 May 2022, available at: https://www.dailymaverick.co.za/article/2022-05-12-witness-gives-damning-testimony-about-general-harry-knoesens-right-wing-insurrection-plot/.

222 Vincent Cruywagen, "Right-wing extremist 'General Harry' Knoesen guilty of plotting to overthrow government", *Daily Maverick,* 7 June 2022, available at: https://www.dailymaverick.co.za/article/2022-06-07-right-wing-extremist-general-harry-knoesen-guilty-of-plotting-to-overthrow-government/.

such as the Suidlanders, Boerelegion, AWB and Bittereinders, however, all operate websites on the surface web, although the AWB site began showing an error message in April 2024. Some of these groups also maintain accounts on mainstream social media and video-sharing platforms such as Facebook, Instagram, X and YouTube. In some cases, they have a considerable number of followers. At the time of writing, in July 2024, the Bittereinders and Boerelegioen had, respectively, 77,000 and 125,000 followers on Facebook, while almost 30,000 people subscribed to the Suidlanders' YouTube channel.

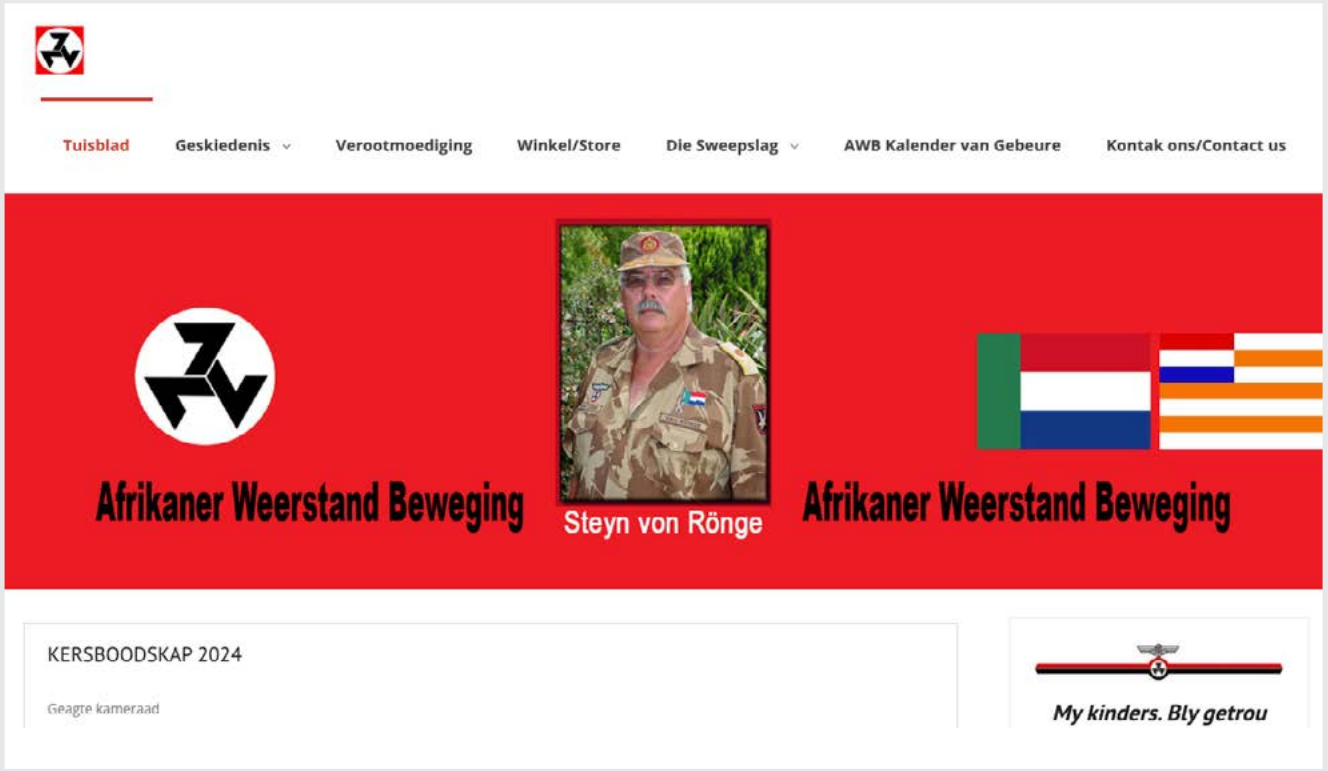

Figure 8. The AWB website's homepage, captured in April 2024.

There are also indications that these groups are using more private or encrypted channels to communicate. On its website and social media channels, for example, Boerlegioen has included a WhatsApp number. In another example, an AWB application form, accessible via its website and dated 2019, includes a Gmail address as point of contact. Training videos and other audiovisual content are freely available on large social media sites. The messaging there remains mostly defensive in nature, however, rather than advocating offensive violence.

Of the various groups listed above, Suidlanders is probably the most sophisticated in its use of online platforms. The group promotes a radio station, RadioGrootrivier, and an app, which is accessible only to members but is available for download on the Google Play and Apple stores. Previews of the app indicate that it features a heat map for localised unrest and other forms of violence in South Africa, together with contact details for local chapters of the group. On a dedicated subdomain of the group's website, Suidlanders also hosts a marketplace for local businesses, such as hospitality, security, weaponry and survivalist companies, to promote their

services. The group also has a publicly advertised Bitcoin wallet for donations. The transaction history of the wallet indicates just 19 donations between October 2021 and July 2024, when its balance was around 1,700 USD. The majority of the group's funding comes from its membership fee, rather than online donations.[223]

Beyond the named organisations listed so far in this case study, there exists an extensive network of South African-focused right-wing extremist accounts on social media and messaging platforms, particularly platforms like X, Facebook, YouTube, Telegram and TikTok – some with tens of thousands of followers. These accounts routinely point to violence against white South Africans as examples of ongoing "white genocide", often sharing graphic material depicting the aftermath of these crimes. Israel Vision is similarly pervasive across a broad range of social media platforms, typically accompanied by hashtags such as #yeshua, #yahweh or #boervolk.[224]

The increased social media presence of such actors has coincided with a greater level of international communication and collaboration with extremist actors outside of South Africa. In the past year, for example, the Suidlanders have frequently interacted with US-based white supremacists and anti-Semites on X, and its leader, Simon Roche, has previously travelled to the United States to engage in person with prominent individuals such as white supremacist Jared Taylor and David Duke, the former "grand wizard" of the Ku Klux Klan.[225] Recent threads on the "South Africa General" section of the white nationalist StormFront Forum, which is based in the United States, had been viewed by more than 280,000 people when it was accessed during the research for this report in July 2024. In a further indication of synergies between the South African domestic context and white supremacy worldwide, American violent extremist organisation The Base has previously recruited in South Africa.[226] Additionally, the perpetrators of the shootings in Christchurch, New Zealand in 2019, in Charleston, United States in 2015, and in Utöya, Norway in 2011, referred to the perceived plight of white people in South Africa in their manifestos.

223 Interview with Johannes Vreugdenburg, Individual Expert and Former Police, 8 July 2024.

224 Rebecca Davis, "Israel Vision – How the religious cult that drove the Boeremag still flourishes online".

225 Lloyd Gedye, "White genocide: how the big lie spread to the US and beyond", *Mail and Guardian,* 23 March 2018, available at: https://mg.co.za/article/2018-03-23-00-radical-right-plugs-swart-gevaar/.

226 Benjamin Wallace, "The Prep School Nazi", *New York Magazine,* 30 March 2020, available at: https://nymag.com/intelligencer/2020/03/rinaldo-nazzaro-the-base-norman-spear.html.

Right-wing violent extremism in Asia: Hindutva

Background

Hindutva has its origins in the 1920s in the writings of Vinayak Damodar Savarkar (1883-1966), an Indian nationalist writer considered by many to be the ideological father of the present-day movement. Its emergence coincided with the growth of the desire for self-rule during the First World War, when India was under British colonial power. Savarkar's text "The Essentials of Hindutva" characterised Hindus as being the rightful owners of India as the religion had originated there.[227]

During the 1920s and 1930s the Hindutva movement drew influence from fascist movements in Europe, including the Mussolini regime in Italy and Hitler's Third Reich in Germany. Hindutva increasingly subscribed to National Socialism, against the background of a growing domestic movement for independence from colonial British rule. Unlike its right-wing extremist counterparts in Germany, Hindutva was not focused on race, although it did view Hindus as being bound together by 'blood', while Muslims and Christians were seen as having divided loyalties and also as the 'other', because the holy lands of their religions were located outside India.[228] Linkages between the Indian subcontinent and Germany were also present in a myth, believed by some Nazis, that the 'bloodline' of the Aryan race originated in South Asia, leading the German Nazi Heinrich Himmler to send an investigative team there in 1938.[229] Anti-Muslim hatred came to be a dominant characteristic of the right-wing extremist form of Hindutva ideology, with Islam and Muslims perceived as being an existential threat to Hinduism and India.

Following independence from the British in 1947, the Rashtriya Swayamsevak Sangh (RSS, or "National Volunteer Corps") became the predominant Hindu nationalist organisation in India, aligned with the right-wing extremist form of Hindutva ideology. The group broadly aims to unify the cultural, political and religious identity of Hindus in India. It was briefly banned in 1948, however, because of its alleged involvement in the assassination of Mahatma Gandhi. From a mere organisation, the RSS has turned into a system by creating a large number of 'affiliates' and maintaining a connection with diverse political parties, such as the Bharatiya Jana Sangh (BJS) formed in 1951.[230] However, it has always been a complicated task for RSS to structure its relationship with BJS first, and later with the Bharatiya Janata Party (BJP), which was founded

227 "Hindutva", *Institute for Strategic Dialogue,* 21 June 2023, available at: https://www.isdglobal.org/explainers/hindutva-hindu-nationalism/.

228 Amarnath Amarasingham, Sanober Umar and Shweta Desai, "'Fight, Die, and If Required Kill': Hindu Nationalism, Misinformation, and Islamophobia in India", *Religions,* 13 (5), April 2022, available at: https://doi.org/10.3390/rel13050380.

229 "When Nazis tried to trace Aryan race myth in Tibet". BBC News, 15 September 2021, available at: https://www.bbc.co.uk/news/world-asia-india-58466528.

230 Pralaya Kanungo, "Myth of the Monolith: The RSS Wrestles to Discipline Its Political Progeny", Social Scientist 34, no. 11/12 (2006): 51–69, available at: http://www.jstor.org/stable/27644183

in 1980 after a split in the Janata Party.[231] As mentioned in the Executive Summary, Hindutva predates but is often associated with the ideology espoused by former and existing political parties, such as – among others –the Shiv Sena,[232] today split into two other parties, and the Bharatiya Janata Party (BJP), for the commonalities of determining "Hindu-ness" by nationality, culture and race. However, the same concept has been appropriated by extremist groups to justify and promote their agendas.[233] For the purposes of this report, any references to 'Hindutva' pertain exclusively to the violent and extremist interpretations of the ideology, as distinct from broader political or cultural movements in India.

Concerning the right-wing violent extremist interpretations of Hindutva ideology, the Indian population has witnessed increasing violent tensions and attacks between Hindus and Muslims. Violent riots involving Hindus and Muslims and the deadly acts of communal violence date back to at least 1993[234] and continue to affect and target marginalised and minority groups heavily. Such incidents of unrest and communal violence between religious groups are often fuelled by dis- or misinformation online related to particular violent incidents, such as the outbreak of localised demonstrations over the filmed murder of a Hindu shopkeeper by allegedly two Muslim men in Udaipur, Rajasthan, in June 2022.[235]

Current threat picture

Right-wing violent extremism has been growing in India during the last decade and has leveraged the content of recently implemented pieces of legislation, such as the Citizenship Amendment Act (CAA) aimed to facilitate fast-tracked citizenship pathways and overall tackle illegal immigration. Some human rights activists and press outlets argued that the law, which excludes Muslims from neighbouring countries and other marginalised groups from fast-tracked citizenship, may be perceived by extremists to justify discrimination against religious minorities.[236] Members of vigilante organisations espousing the right-wing violent extremist form of Hindutva ideology such as the Bajrang Dal and Sri Ram Sena have been responsible for multiple acts of violence against minorities, particularly Muslims.[237] These attacks come in various forms, such

231 Bharatiya Janata Party. https://www.britannica.com/topic/Bharatiya-Janata-Party.

232 Jayant Lele, "Saffronisation of Shiv Sena: Political Economy of City, State and Nation", Economic and Political Weekly 30, no. 25 (1995): 1520–28, available at: http://www.jstor.org/stable/4402914.

233 "Hindutva", Institute for Strategic Dialogue; Amarasingham, Umar and Desai, "'Fight, Die, and If Required Kill': Hindu Nationalism, Misinformation, and Islamophobia in India".

234 Jim Masselos, "The Bombay riots of January 1993: The politics of urban conflagration", *South Asia: Journal of South Asian Studies 17,* (1994): 79–95, available at: https://doi.org/10.1080/00856409408723217

235 Samriddhi Sakunia, "Fear and anger in India's Udaipur where Hindu tailor was killed", Al Jazeera, 5 July 2022, available at: https://www.aljazeera.com/news/2022/7/5/fear-and-anger-in-indias-udaipur-where-hindu-tailor-was-killed; GIFCT, "Incident Response: CI Activated in Response to Attack in Udaipur", 28 June 2022, available at: https://gifct.org/2022/06/28/content-incident-activated-udaipur-rajasthan-india-attack/.

236 Nikhila Henry and Kathryn Armstong, "CAA: India to enforce migrant law that excludes Muslims", BBC News, 12 March 2024, available at: https://www.bbc.co.uk/news/world-asia-68538260; "India: government policies, actions target minorities", *Human Rights Watch,* 19 February 2021, available at: https://www.hrw.org/news/2021/02/19/india-government-policies-actions-target-minorities.

237 Apoorvanand, "Hatred and violence against Muslims have spread like an epidemic in India", The Wire, 5 September 2024, available at: https://thewire.in/communalism/hatred-and-violence-against-muslims-have-spread-like-an-epidemic-in-india.

as targeted murders, lynchings, and honour-based violence, including as isolated incidents or during communal riots and localised unrest.[238] An example reported in October 2024 described how vigilante supporters of the right-wing violent extremist form of Hindutva ideology affiliated with the Vishva Hindu Parishad (VHP), a Hindu nationalist organisation, coordinate activism on WhatsApp in Bastar, Chhattisgarh. The activists reportedly coordinate on the messaging app to recruit and organise real-world mob activism, for example to destroy a building site for a planned local church, and to intimidate locals into converting to Hinduism.[239]

The majority of these violent incidents are manifestations of a desire by right-wing extremists to "protect" India from a perceived threat allegedly posed by Muslims.[240] These beliefs are further driven by the popularity of conspiracy theories such as 'love jihad',[241] a moral panic at the alleged seduction and forced conversion of Hindu women to Islam by Muslim men.[242] In an example of an incident in which the conspiracy theory has fuelled real-world violence, on the morning of 7 December 2017 the police discovered the burnt corpse of a Muslim labourer in Rajasthan, western India. The man had been hacked and burned to death by an individual inspired by right-wing violent extremist views, who filmed the murder with an accomplice and uploaded the footage onto YouTube.[243] In the video, which reportedly spread widely online, the assailant addresses the camera after attacking the man with a bladed weapon, warning against so-called "love jihad", before setting the man's body on fire.[244]

Aspects of the Hindutva worldview also manifest themselves in the ideology and messaging of right-wing violent extremists in Europe and North America, as can be seen in particular in the writings of Savitri Devi, a French writer and neo-Nazi sympathiser who died in 1982.[245] Devi spent time with the RSS and other Hindutva groups in the 1930s, and echoed the Hindutva ideology, claiming that Adolf Hitler was a reincarnation of the god Vishnu.[246] Quotations and imagery

238 Interview with Gazbiah Sans, PVE Works, 12 June 2024.

239 Parth MN, "WhatsApp vigilantes in India are converting Christians by force", Rest of World, 15 October 2024, available at: https://restofworld.org/2024/whatsapp-intimidation-forced-conversion-targets-christians-india/.

240 Mohammed Amaan Siddiqui, "The role of far-right media houses and organisations in disseminating Hindu nationalist 'Love Jihad' narratives on X", *Global Network on Extremism and Technology,* 5 January 2024, available at: https://gnet-research.org/2024/01/05/the-role-of-far-right-media-houses-and-organisations-in-disseminating-hindu-nationalist-love-jihad-narratives-on-x/.

241 "Mood of the Nation | Are Muslim men indulging in 'love jihad'? 53% respondents say yes", *India Today,* 26 January 2023, available at: https://www.indiatoday.in/mood-of-the-nation/story/mood-of-the-nation-2326853-2023-01-26.

242 Aastha Tyagi and Atreyee Sen, "Love-Jihad (Muslim Sexual Seduction) and ched-chad (sexual harassment): Hindu nationalist discourses and the Ideal/deviant urban citizen in India", *Gender, Place and Culture,* Vol. 27, Issue 1, 11 May 2019, available at: https://doi.org/10.1080/0966369X.2018.1557602.

243 "Wheels of justice moving at slow pace in Rajsamand hate killing case", *The Hindu,* 3 July 2022, available at: https://www.thehindu.com/news/national/other-states/wheels-of-justice-moving-at-slow-pace-in-rajsamand-hate-killing-case/article65592702.ece.

244 Zeenat Saberin, "Hate crime in India: Muslim man hacked, burned to death", *Al Jazeera*, 7 December 2017, available at: https://www.aljazeera.com/news/2017/12/7/hate-crime-in-india-muslim-man-hacked-burned-to-death. Saurabh Sharma, "'Saving someone who saved his religion': Hindu nationalist on why he's offering Shambhulal Regar a ticket in 2019", *First Post,* 18 September 2019, available at: https://www.firstpost.com/politics/saving-someone-who-saved-his-religion-hindu-nationalist-on-why-hes-offering-shambulal-regar-a-ticket-in-2019-5210481.html.

245 "Savitri Devi: The mystical fascist being resurrected by the alt-right", *BBC News,* 29 October 2017, available at: https://www.bbc.com/news/magazine-41757047.

246 Eviane Leidig, "Hindutva as a variant of right-wing extremism", *Patterns of Prejudice,* Vol. 54, No. 3, 2020, available at: https://www.tandfonline.com/doi/epdf/10.1080/0031322X.2020.1759861?needAccess=true.

relating to Devi have appeared in the messaging of multiple esoteric Hitlerist groups affiliated with "Siege Culture", including Feuerkrieg Division and the satanic Order of Nine Angles, and neo-Nazi content creators like Dark Foreigner, despite their racist hostility towards people of South Asian ethnicity.[247] Devi's writings are more prevalent in the messaging of white supremacists than Hindu nationalist extremists, however, despite Hindutva's rise in popularity in India.

Figure 9. Savitri Devi pictured in front of the sunwheel neo-Nazi symbol, sourced from Telegram in July 2024.

Abuse of digital technology

Supporters of the right-wing violent extremist form of Hindutva ideology have used the Internet for political messaging and other forms of communication for a long time – websites and chat forums since the 1990s, even.[248] Today, Hindutva has a complex and wide-reaching information ecosystem on digital platforms.[249] Official accounts run by organisations like the RSS and VHP, known collectively as Sangh Parivar, each have millions of followers on mainstream social media platforms like X, Facebook, Instagram and YouTube.

More niche and militant offshoots also command significant followership in mainstream digital public spaces, seemingly without moderation by technology companies. The vigi-

247 Bethan Johnson and Matthew Feldman, "Siege Culture after Siege: Anatomy of a neo-Nazi terrorist doctrine", *International Centre for Counter Terrorism,* July 2021, available at: https://www.icct.nl/sites/default/files/2022-12/siege-culture-neo-nazi-terrorist-doctrine.pdf.

248 Ingrid Therwath, "Cyber-Hindutva: Hindu nationalism, the diaspora and the web", *Social Science Information,* 51 (4), 2012, available at: http://www.e-diasporas.fr/working-papers/Therwath-Hindutva-EN.pdf.

249 Interview with Arvind Kumar, Royal Holloway, University of London, 10 July 2024.

lante youth wing of the VHP, Bajrang Dal, had 89,000 followers on Facebook at the time of writing in July 2024, with a similar following on X and smaller numbers of subscribers on its official pages on Telegram and Instagram. Supporter groups on Facebook had as many as 42,000 followers. Bajrang Dal emphasises physical strength among its members and supporters, who have frequently carried out vigilante violence against minorities, including murders, in the name of perceived anti-'love jihad', and anti-religious conversion activities.[250]

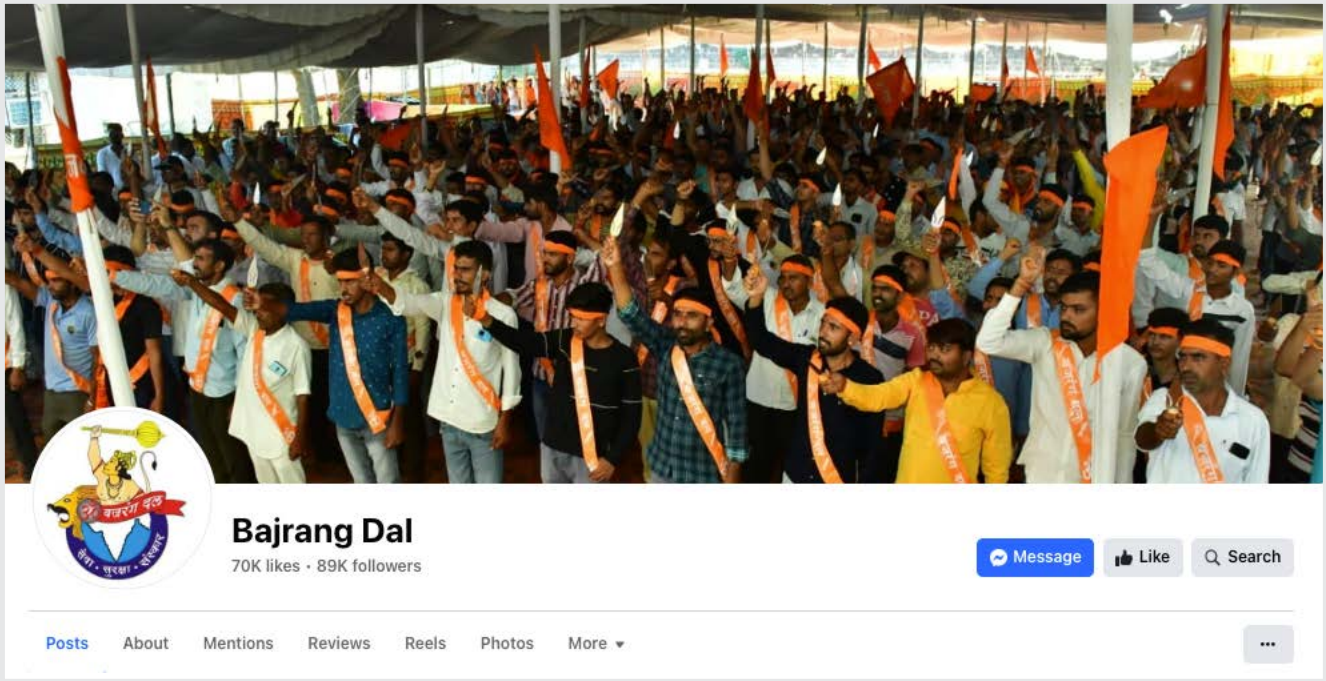

Figure 10. A Facebook account affiliated with the Hindutva organisation Bajrang Dal, captured in July 2024.

These organisations' digital communications strategy involves official public messaging on social media combined with a vast and complex network of more than five million WhatsApp groups, managed by the organisations' multiple IT cells.[251] Unverified mis- and disinformation is common with these groups and elsewhere in the digital ecosystem, including synthetic, realistic deep fakes and coordinated inauthentic political propaganda campaigns by fake media outlets.[252]

250 Nistula Hebbar, "Bajrang Dal | The aggressive arm of Hindutva", *The Hindu,* 6 August 2023, available at: https://www.thehindu.com/news/national/bajrang-dal-the-aggressive-arm-of-hindutva/article67162932.ece; "Karnataka: One of the accused in Mohammed Fazil's murder case gets bail", *Siasat,* 15 September 2022, available at: https://www.siasat.com/karnataka-one-of-the-accused-in-mohammed-fazils-murder-case-gets-bail-2413450/; Ashok Kumar, "Haryana communal violence | In the shadow of the millennium city", *The Hindu,* 5 September 2023, available at: https://www.thehindu.com/news/national/other-states/in-the-shadow-of-the-millennium-city/article67158990.ece; "What we know about Delhi shooter, who posted live Facebook videos before firing", *Scroll,* 30 January 2020, available at: https://scroll.in/article/951609/jamia-shooting-what-we-know-about-ramgopal-bhakt-who-posted-live-facebook-videos-before-firing.

251 Interview with Shaswati Das, previously at University of York, 10 June 2024; Interview with Siddarth Venkataramakrishnan, Institute for Strategic Dialogue, 11 June 2024; Amrita Madhukalya, "50 lakh WhatsApp groups and transmission anywhere in 12 minutes — What BJP is doing on social media for 2024", *Deccan Herald,* 23 March 2024, available at https://www.deccanherald.com/elections/india/political-theatre-bjp-on-social-media-2950186; Interview with Arvind Kumar, Royal Holloway, University of London, 10 July 2024.

252 Usha M. Rodrigues, "Are social media, AI and misinformation undermining Indian democracy?", *East Asia Forum,* 17 May 2024, available at: https://eastasiaforum.org/2024/05/17/are-social-media-ai-and-misinformation-undermining-indian-democracy/; Alexandre Alaphilippe, Gary Machado, Roman Adamczyk and Antoine Grégoire, "Uncovered: 265 coordinated fake local media outlets serving Indian interests", *EU Disinfo Lab,* 26 November 2019, available at: https://www.disinfo.eu/publications/uncovered-265-coordinated-fake-local-media-outlets-serving-indian-interests/.

This is compounded by the involvement of an organic network of political activists supportive of these organisations known as 'Cyber Hindus', who edit, reformat and reinterpret the messaging on third-party troll pages and WhatsApp groups. Even initially accurate and innocuous political messaging can become distorted as it is repurposed and forwarded many times, resulting in potentially incendiary mis- or disinformation.[253] The prolific forwarding of WhatsApp messages, including by Hindu nationalist extremist networks, has become a key feature of mis- and disinformation campaigns in India – an issue that has been exacerbated by the ability of some users there to have up to nine SIM cards.[254] Networks of 'Cyber Hindus' have also frequently engaged in harassment against their perceived enemies, particularly activists, as part of a broader effort to silence opponents.[255] Messaging campaigns supporting the Hindutva ideology can also reach beyond the domestic Indian population to diaspora communities, potentially boosting support for the movement globally.[256]

WhatsApp has also been used by right-wing violent extremists operating in India to organise and coordinate violence.[257] During attacks on anti-CAA protesters in Delhi in February 2020, right-wing violent extremist actors reportedly coordinated on WhatsApp to mobilise violence against Muslims, including by attempting to enlist the support of the RSS, VHP and Bajrang Dal.[258] During those same anti-CAA protests in January of that year, a gunman linked to Bajrang Dal fired a pistol, injuring a Muslim protester. The man had streamed on Facebook Live in the minutes before the incident and posted several status updates, including one saying that he was acting in "revenge" for the death of a right-wing activist killed in communal clashes in 2018. Earlier posts on the account showed the perpetrator with firearms and swords, often next to messages about protecting Hindu honour. Facebook removed the account following the attack.[259]

Figure 11. Screenshot of the /indiachan/ board on 8chan.

253 Interview with Siddarth Venkataramakrishnan, Institute for Strategic Dialogue, 11 June 2024; Interview with Shaswati Das, previously at University of York, 10 June 2024.

254 Interview with Shaswati Das, previously at University of York, 10 June 2024.

255 Sriram Mohan, "Locating the 'Internet Hindu': Political Speech and Performance in Indian Cyberspace", *Television & New Media,* Vol. 16, Issue 4 (March 2015), available at: https://doi.org/10.1177/1527476415575491.

256 Soumya Shankar, "India's Liberal Expats are Modi's Biggest Fans", *Foreign Policy,* 7 May 2019, available at: https://foreignpolicy.com/2019/05/07/indias-liberal-expats-are-modis-biggest-fans/.

257 Interview with Anuradha Sajjanhar, University of East Anglia, 24 June 2024.

258 Ismat Ara, "Tear Them Apart': How Hindutva WhatsApp Group Demanded Murder, Rape of Muslims in Delhi Riots", *The Wire,* 6 July 2020, available at: https://thewire.in/communalism/delhi-riots-hindutva-whatsapp-muslims-murder-rape.

259 "What we know about Delhi shooter, who posted live Facebook videos before firing", *Scroll,* 30 January 2020, available at: https://scroll.in/article/951609/jamia-shooting-what-we-know-about-ramgopal-bhakt-who-posted-live-facebook-videos-before-firing.

The more overtly violent extremist networks also congregate in more niche, dedicated and insular spaces online. Indiachan and BharatChan are examples of imageboard websites that are populated mostly by Hindu nationalist extremists, although they have also been active on chan sites like 8chan and 4chan.[260] While Indiachan and Bharatchan are clearly inspired by their equivalents based in North America or Europe, including in terms of their layout, community culture and ideological tendencies, they have an explicitly Indian focus.

A review of Bharatchan in June 2024 found multiple examples of explicit incitement to violence against Muslims, in addition to trolling, anti-Semitism and Hindu supremacism. An "Indiachan" board on 8chan in July 2024 featured the swastika at the top of the page, and a message that it was dedicated to "uncensored discourse". Indian chan sites and boards also show signs of a more technical cyber capability among right-wing extremists. Related discussions observed there in June 2024 included tips on hacking Wi-Fi, and learning TypeScript, together with guides on "how to be a hacker" and how to use AI tools.

Figure 12. The /pol/ board on Bharatchan, captured in June 2024.

In parallel with the right-wing extremist networks online in India, there exists an extensive community of Hindutva-aligned hacking groups. While these groups rarely endorse violence explicitly, they often engage in disruptive hacking activities against perceived enemies, including Islamic targets and websites perceived to be affiliated with states such as Pakistan, China, Palestine and Indonesia. Tactics typically include DDoS, web defacement and the hacking of CCTV cameras in target countries.

260 Interview with Benjamin Mok and Saddiq Basha Bin Cekendar Basha, S. Rajaratnam School of International Studies (RSIS), 6 June 2024.

A hacking group called Indian Cyber Force, for example, has an active presence on Telegram, X and Instagram, and has claimed responsibility for multiple alleged cyber-attacks on targets affiliated with perceived enemy states. They include a campaign against Canada called #OpCanada, in which it mounted DDoS attacks in September 2023 against Canadian military, parliament and electoral websites, and a handful of others operated by small businesses in the country.

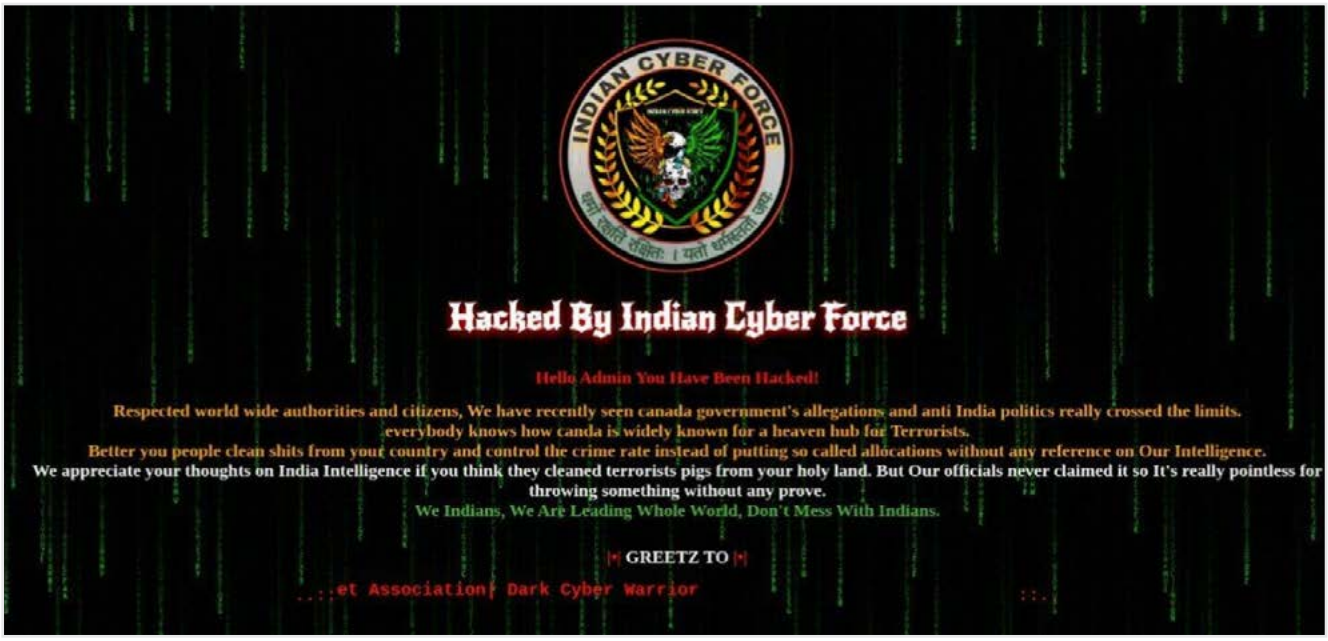

Figure 13. A message allegedly displayed on the website of a Canadian business allegedly hacked by Indian Cyber Force, shared by the group on X in September 2023.

Left-wing violent extremism in Asia: Naxals

Background

The ongoing left-wing violent extremist insurgency waged by the Naxalite and Maoist movement in India has its ideological origins in 1925, when the Communist Party of India (CPI) was created in Kanpur. Several internal alliances and splits then followed within the Indian communist movement over the following years. The CPI was split in 1964, leading to the formation of the Communist Party of India (Marxist).[261] In subsequent years the CPI-M itself split, notably following another communist uprising in 1967 in Naxalbari, a village in the Indian state of West Bengal. An imprisoned communist ideologue, Charu Mazumbar, then produced a series of writings that would form the basis of the Naxalite ideology: influenced less by Marxism than by the Maoism of the 20th century in China, and emphasising the importance of a revolution coming from the peasants in rural areas of India, rather than the working class.[262] As the movement spread throughout the central Indian states of Bihar, Orissa and Andhra Pradesh, Mazumbar led a split from CPI-M in 1969 and formed the CPI-Marxist Leninist (CPI-ML). Despite its name, the CPI-ML was more inspired by Maoism than by Marxism or Leninism. A government offensive against the CPI-ML and other disparate left-wing violent extremist groups in 1971 severely damaged and fractured the movement, and there was a decline in activity over the next two decades.[263]

The movement resurfaced in India during the late 1980s, when the economy was liberalising and multinational mining companies were becoming increasingly present in rural areas. During this time, efforts were made to unite the more than 40 disparate Naxalite groups. These led in 2004 to a merger of the two most powerful communist groups, with the creation of CPI-Maoist and its armed wing, the People's Liberation Guerrilla Army (PLGA).[264] The CPI-Maoist outlined its aims and objectives in a press release published in October 2004. The group said it intended to continue the "protracted people's war" to overthrow what it described as the "semi-colonial, semi-feudal system under the neo-colonial form of indirect rule, exploitation, and control".[265] It said its "centre of gravity" would remain in the countryside alongside "complementary"

261 "A historical introduction to Naxalism in India", *European Foundation for South Asia Studies,* December 2019, available at: https://www.efsas.org/publications/study-papers/an-introduction-to-naxalism-in-india/.

262 "A historical introduction to Naxalism in India", *European Foundation for South Asia Studies,* December 2019, available at: https://www.efsas.org/publications/study-papers/an-introduction-to-naxalism-in-india/.

263 Sameer Lalwani, "India's approach to counterinsurgency and the Naxalite problem", *CTC Sentinel,* October 2011, available at: https://ctc.westpoint.edu/wp-content/uploads/2011/11/CTCSentinel-Vol4Iss102.pdf.

264 "Communist Party of India-Maoist (CPI-Maoist), all its formations and front organisations", *South Asia Terrorism Portal,* available at: https://www.satp.org/terrorist-profile/india/communist-party-of-india-maoist-cpi-maoist-all-its-formations-and-front-organizations.

265 "Joint Press Statement on Merge of MCCI and CPI-ML(PW)", cited in "A historical introduction to Naxalism in India", European Foundation for South Asia Studies, December 2019, available at: https://www.efsas.org/publications/study-papers/an-introduction-to-naxalism-in-india/.

operations in urban areas.[266] The left-wing extremist insurgency grew in strength throughout the 2000s until the then Prime Minister, Dr Manmohan Singh, described the Naxalite insurgency in 2010 as India's greatest internal security challenge.[267] At its peak, the CPI-Maoist was estimated to have around 20,000 members and to occupy territory in states containing 20% of the country's population.[268] The movement killed 8,863 people between 2004 and 2023, according to the Indian Ministry of Home Affairs. The majority of these were civilians, killed by Maoists after being branded by them as "police informers".[269]

Current threat picture

Counter-insurgency operations and waning popular support have significantly reduced the threat posed by CPI-Maoist and other Naxalite groups in recent years.[270] Indian press reports indicate that security forces killed an unprecedented number of left-wing extremists in security operations in the first half of 2024, especially in the Maoist stronghold of Chhattisgarh.[271] Government data indicates an 85% reduction in the frequency of killings of civilians by left-wing violent extremists since the movement's peak: from 720 in 2010 to 106 in 2023.[272] Bombings against security forces and targeted killings of civilians continue to occur, however, and the movement still has a presence in the rural areas of Chhattisgarh, Jharkhand, Odisha, West Bengal, Andhra Pradesh, Telangana, Maharashtra, Madhya Pradesh and Kerala.[273]

Official testimonies of operations have sometimes been contradicted in the local press, for example by witnesses alleging the killing of innocent civilians by security forces.[274] An operation in May 2024 in the Bijapur district of Chhattisgarh, for example, resulted in the deaths

266 "Joint Press Statement on Merge of MCCI and CPI-ML(PW)", cited in "A historical introduction to Naxalism in India", European Foundation for South Asia Studies, December 2019, available at: https://www.efsas.org/publications/study-papers/an-introduction-to-naxalism-in-india/.

267 "Naxalism biggest threat to internal security: Manmohan", *The Hindu,* 24 May 2010, available at: https://www.thehindu.com/news/national/Naxalism-biggest-threat-to-internal-security-Manmohan/article16302952.ece.

268 Devika Shanker-Grandpierre,"The evolution of Indian left-wing extremism in the digital era: tactics, impact, and counter strategy", *Global Network on Extremism & Technology,* 27 October 2023, available at: https://gnet-research.org/2023/10/27/the-evolution-of-indian-left-wing-extremism-in-the-digital-era-tactics-impact-and-counter-strategy/.

269 "Left-wing extremism division", *Government of India Ministry of Home Affairs,* available at: https://www.mha.gov.in/en/divisionofmha/left-wing-extremism-division.

270 Murali Krishnan, "Why has Maoist violence subsided in India?". *Deutsche Welle,* 1 May 2023, available at: https://www.dw.com/en/why-has-maoist-violence-subsided-in-india/a-64292819; Bidisha Saha, "Explained: What's behind the skyrocketing maoist killings this year", India Today, 19 July 2024, available at: https://www.indiatoday.in/india/story/maoist-killing-india-encounter-chhattisgarh-bastar-mahashtra-2569239-2024-07-19.

271 "Explained: What's behind the skyrocketing maoist killings this year", *India Today,* 19 July 2024, available at: https://www.indiatoday.in/india/story/maoist-killing-india-encounter-chhattisgarh-bastar-mahashtra-2569239-2024-07-19.

272 "Frequently Asked Questions", *Government of India Ministry of Home Affairs,* available at: https://www.mha.gov.in/sites/default/files/2024-05/faqLWEDIVISION_06052024.pdf.

273 *Ibid.*

274 Bibhu Prasad Routry, "Counter-LWE security operations: Season of success?" – Analysis", *Eurasia Review,* 17 May 2018, available at: https://www.eurasiareview.com/17052018-counter-lwe-security-operations-season-of-success-analysis/.

of 12 Maoists, according to the police. But civilian witnesses speaking to the press said that the police had killed civilian farmers, not left-wing extremists.[275] There have been claims that left-leaning political actors were inaccurately branded by political opponents as being affiliated with CPI-Maoist, for example via the hashtag campaign #UrbanNaxals, and through the use of hacking techniques to plant false evidence on activists' devices.[276] In this context, such claims and actions pose severe concerns and risks of human rights abuses, which require to be acknowledged in order to be addressed.

CPI-Maoist has long engaged in a propaganda campaign to highlight the real and perceived inadequacies of the existing state structure. In addition to its focus on guerrilla warfare, CPI-Maoist operates several front organisations tasked with facilitating recruitment and radicalisation through ostensibly democratic means.[277] Historically the group's members have circulated handwritten letters or pamphlets to rural populations and have disseminated its message via direct engagement with the Indian press.

Abuse of digital technologies

CPI-Maoist has also long exploited digital platforms to spread its message and recruit. At its peak, in the late 2000s, the group operated several dozen websites and blogs hosting press releases and other publications, many of which mirrored one another, in order to mitigate the impact of their being blocked by the authorities. In an effort to reach both Indian and international audiences, the websites hosted CPI-Maoist material in multiple languages. According to Bibhu Prasad Routray, an expert on Naxalism, the group has reduced its direct engagement with the press while increasingly relying on websites to spread its message.[278]

One of the group's primary propaganda products in recent decades has been *People's March*, a magazine banned in India and that serves to circulate the ideology, objectives and operations of CPI-Maoist and the broader left-wing violent extremist movement. Its first issue was produced in 1999, and more than 70 issues were published between then and 2023. After existing initially only as a hardcopy publication, the magazine went digital in 2014 and was disseminated via the

275 Ritesh Mishra, "Villagers allege Bijapur encounter was fake and those killed were civilians", *Hindustan Times,* 12 May 2024, available at: https://www.hindustantimes.com/cities/others/villagers-allege-bijapur-encounter-was-fake-and-those-killed-were-civilians-101715521493743.html.

276 Vernon Gonsalves and Arun Ferreira, "A propaganda tool called #UrbanNaxal", *Rediff,* 13 July 2018, available at: https://www.rediff.com/news/column/a-propaganda-tool-called-urbannaxal/20180713.htm; "Andy Greenberg, "Police linked to hacking campaign to frame Indian activists", *Wired,* 16 June 2022, available at: https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/; Interview with Nicole Matejic, Charles Sturt University, 12 June 2024.

277 "Left-wing extremism division", Government of India Ministry of Home Affairs, available at: https://www.mha.gov.in/en/divisionofmha/left-wing-extremism-division.

278 Bibhu Prasad Routray, "Online Maoist propaganda: how India should respond", *Eurasia Review,* 4 May 2022, available at: https://www.eurasiareview.com/04052022-online-maoist-propaganda-how-india-should-respond-analysis/.

group's network of websites and blogs, each with different top-level domains (TLDs) but redirecting to the main website. By using this approach the group was able to mitigate the impact of takedowns of particular sites, and to diversify its audience.[279]

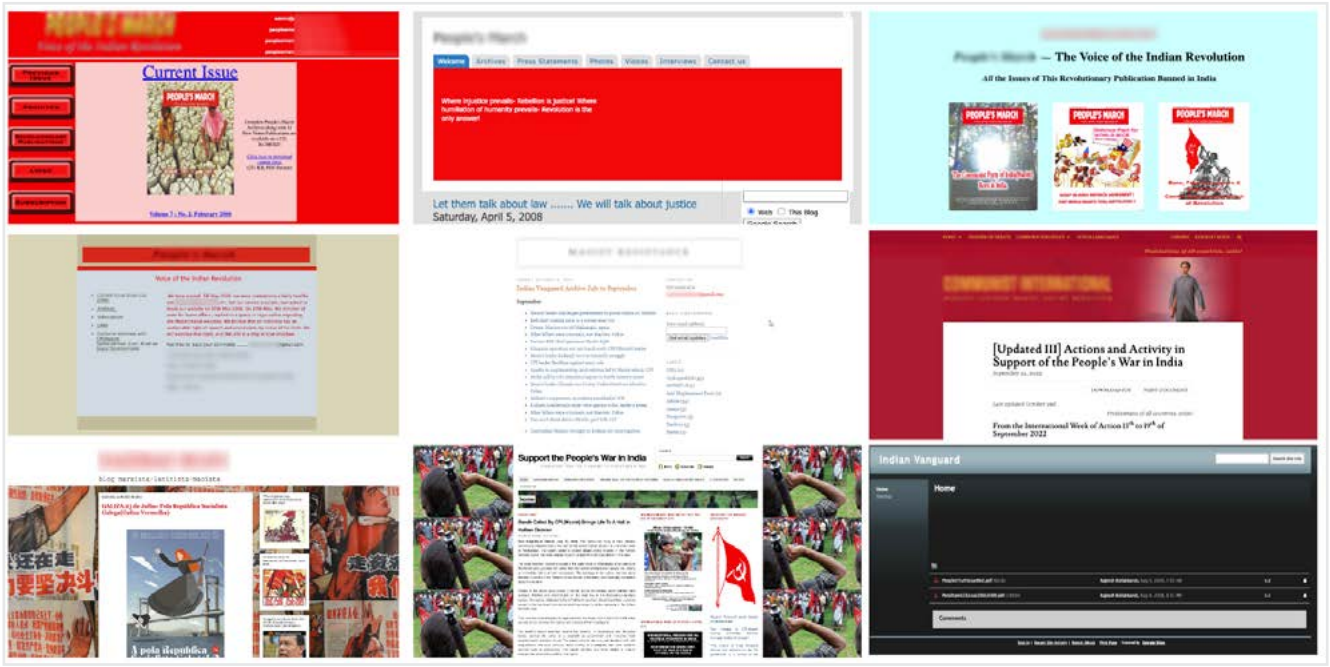

Figure 14. Examples of websites operated by or in support of CPI-Maoist, sourced from web and Archive.org in July 2024.

By July 2024, many of the CPI-Maoist's primary dissemination websites were either inactive or had ceased to exist, but the group had increasingly garnered the support of international left-wing extremist movements and their networks online, through which its propaganda and message remained available on the Internet. One such example is the International Committee to Support the People's War in India (ICSPW), which works to garner support for CPI-Maoist and other militant Naxals.[280] The group has operated a WordPress site since at least 2013. It held an "internationalist meeting" in Milan, Italy, in December 2018, which it claimed attracted attendees from Italy, France, Austria, Germany, Switzerland, Turkey and Spain.[281]

Police statements in the Indian press also indicate the use of more private, encrypted communication technology between CPI-Maoist and its affiliated networks in India. A January 2020 report cited police as saying it had difficulty investigating members of an alleged Maoist front

279 Devika Shanker-Grandpierre, "The evolution of Indian left-wing extremism in the digital era: Tactics, Impact, and Counter Strategy", *Global Network on Extremism & Technology*, 27 October 2023, available at: https://gnet-research.org/2023/10/27/the-evolution-of-indian-left-wing-extremism-in-the-digital-era-tactics-impact-and-counter-strategy/.

280 Mohua Chatterjee, "Red groups seek global support for 'people's war in India'", *The Economic Times*, 20 February 2011, available at: https://economictimes.indiatimes.com/news/politics-and-nation/red-groups-seek-global-support-for-peoples-war-in-india/articleshow/7531641.cms.

281 "1 – Report meeting in Italy that launched the next international campaign 21/27 January – ICSPWI Report internationalist meeting India – Milan 8th December", *ICSPWI*, 13 January 2019, available at: https://icspwindia.wordpress.com/2019/01/13/1-report-meeting-in-italy-that-launched-the-next-international-campaign-21-27-january-icspwi-report-internationalist-meeting-india-milan-8th-december/.

group, the Telangana Praja Front, owing to "complex" encryption on their devices.[282] The article cited the use of Pretty Good Privacy (PGP)[283] by the targets of the investigation, to encrypt documents, rendering them inaccessible to investigators. A press article on a police investigation into CPI-Maoist in August 2023 also reported that the left-wing extremists were using Protonmail, an end-to-end encrypted email provider, to communicate internally. It also said they were using the "dark web" to "purchase arms, weapons, explosives, raw materials and electronic devices used in combat zones".[284] The article provided no further information on how successful or widespread this reported use was, but quoted a police officer as saying Maoist use of the dark web in India was "nothing new".

282 Marri Ramu, "Maoists using complex communication system, police tell High Court", *The Hindu,* 30 January 2020, available at: https://www.thehindu.com/news/cities/Hyderabad/maoists-using-complex-communication-system-police-tell-high-court/article30695924.ece.

283 Pretty Good Privacy (PGP) is a security program used to decrypt and encrypt email and authenticate e-mail messages through digital signatures and file encryption.

284 Soumitra Bose, "Maoists using dark web to talk, buy arms and ammo", *The Times of India,* 9 August 2023, available at: https://timesofindia.indiatimes.com/city/nagpur/maoists-using-dark-web-to-talk-buy-arms-and-ammo/articleshow/102555962.cms.

Right-wing violent extremism in South-East Asia

Background

Contemporary right-wing extremism in South-East Asia can be traced back to at least the early 1900s, when actors in the region aligned themselves ideologically with fascist movements in Europe. The Nederlandsche Indische Fascisten Organisatie (NIFO) and the Nationaal-Socialistische Beweging (NSB) attracted support among the local population living in the territory of the modern state of Indonesia.[285] In the 1930s the Partai Fasis Indonesia (Indonesian Fascist Party, PFI) was established in present-day Jakarta by a Javanese supremacist, inspired by Hitler and Mussolini, upon his return from studies in Berlin.[286] The party failed to attract popular support, however.[287]

In the late 1930s and 1940s, Japanese imperial rule popularised the anti-Western and pan-Asian concept of "Asia for Asians",[288] including via the fascist Kapisanan ng Paglilingkod sa Bagong Pilipinas (KALIBAPI) in the Philippines.[289] Phibun Songkhram, former Prime Minister of Thailand, was strongly influenced by European fascism and sought to militarise the nation in support of Japan's war against Allied forces.[290] Such actors and movements were attracted to fascist ideologies in part because of their ideals of ethnic and cultural supremacy, military power, and national strength.[291]

285 Rudolf Mrázek, "Sjahrir: Politics and Exile in Indonesia", *Studies on Southeast Asia,* No.14, 1994, p. 108; Munira Mustaffa, "Right-wing extremism has deep roots in southeast Asia", Global Network on Extremism & Technology, 14 July 2021, available at: https://gnet-research.org/2021/07/14/right-wing-extremism-has-deep-roots-in-southeast-asia/.

286 Solichan Arif, "Kisah Partai Fasis Indonesia Tak Berumur Panjang karena Gagasannya Ditolak Kaum Pergerakan", *Okezone News,* 19 February 2022, available at: https://nasional.okezone.com/read/2022/02/19/337/2549823/kisah-partai-fasis-indonesia-tak-berumur-panjang-karena-gagasannya-ditolak-kaum-pergerakan.

287 Munira Mustaffa, "Right-wing extremism has deep roots in southeast Asia", *Global Network on Extremism & Technology,* 14 July 2021, available at: https://gnet-research.org/2021/07/14/right-wing-extremism-has-deep-roots-in-southeast-asia/.

288 Andre Magnatay, ""Asia for Asians": Revisiting Pan-Asianism through the Propaganda Arts of the Greater East Asia Co-Prosperity Sphere", *Manusya: Journal of Humanities,* Vol. 26, Issue 1 (2024), available at: https://doi.org/10.1163/26659077-26010015.

289 Sven Matthiessen, "Re-Orienting the Philippines: The KALIBAPI party and the application of Japanese Pan-Asianism, 1942-45", *Modern Asian Studies,* Vol. 53, Issue 2, January 2019, available at: https://www.cambridge.org/core/journals/modern-asian-studies/article/abs/reorienting-the-philippines-the-kalibapi-party-and-the-application-of-japanese-panasianism-194245/5321E58C10D0C551663C170DDC7C0076.

290 E. Bruce Reynolds, "Phibun Songkhram and Thai Nationalism in the Fascist Era", *European Journal of East Asian Studies,* Vol. 3, Issue 1, January 2004, available at: https://www.researchgate.net/publication/233623709_Phibun_Songkhram_And_Thai_Nationalism_in_the_Fascist_Era.

291 Munira Mustaffa, "Right-wing extremism has deep roots in southeast Asia".

These ideals continue to influence the ideologies of right-wing extremists in the region today.[292] In Malaysia there is a "Malay Power" music scene, composed of nationalist extremists who self-identify as neo-Nazis and who believe in the maintenance of a "pure" Malay community across the Malay archipelago.[293] Also, as the Second World War is associated more with the advances of Imperial Japan than the crimes of Nazi Germany, Neo-Nazism does not conjure up the same negative connotations for some Asians as it does in Europe or North America.[294] These attitudes have led to several reported instances of Asians adopting Nazi logos, symbols and costumes in recent years, including in countries like Thailand and Indonesia.[295] This phenomenon has been attributed more to a lack of historical understanding and an affinity for 'strongman' figures, however, than to explicit support for the Nazi ideology.[296]

Current threat picture

Right-wing extremism in South-East Asia is as ideologically diverse as the region itself. Its manifestations vary depending on the national context in which it appears, and on the ethnic or religious identities of the actors concerned. Right-wing extremist movements across the region feed off deep-rooted racism or xenophobia, and a significant proportion of right-wing extremism there stems from ultranationalism.[297] Depending on the context, the ideology and objectives of these actors can include, but are not limited to, Muslim nationalism, anti-Rohingya or anti-Muslim prejudice, Buddhist ultranationalism, historical revisionism, neo-Nazism, antisemitism, and support for authoritarianism.[298] Despite the ideological heterogeneity of right-wing extremist movements in the region, they are broadly similar in terms of their adherence to racism or xenophobia, which are prejudices deeply rooted in these local networks.

292 Munira Mustaffa, "Radical Right Activities in Nusantara's Digital Landscape: A Snapshot", *Global Network on Extremism & Technology*, April 2022, available at: https://gnet-research.org/wp-content/uploads/2022/04/GNET-Report-Radical-Right-Activities-in-Nusantaras-Digital-Landscape.pdf.

293 Nick Chester, "Meet the Malaysian neo-Nazis fighting for a pure Malay race", *Vice,* 18 May 2013, available at: https://www.vice.com/en/article/jmv73p/the-malaysian-nazis-fighting-for-a-pure-race.

294 Ben Westcott, "'Nazi-chic': Why dressing up in Nazi uniforms isn't as controversial in Asia", *CNN World,* 28 December 2016, available at: https://edition.cnn.com/2016/12/27/asia/taiwan-nazi-school-asia/index.html.

295 "Hot for HItler: Decoding SE Asia's obsession with Nazi iconography", *The Nation,* 3 March 2019, available at: https://www.nationthailand.com/perspective/30365120; Riysiana Muthia, "How do Indonesians who dress as Hitler and Nazi soldiers justify their obsession?", *South China Morning Post,* 18 September 2017, available at: https://www.scmp.com/lifestyle/article/2111337/how-do-indonesians-who-dress-hitler-and-nazi-soldiers-justify-their.

296 "Thailands Nazi pop culture phenomenon", *DW Story,* 11 March 2019, available at: https://www.youtube.com/watch?v=rSRwxGCZ-JKs; "Southeast Asia's fixation with Nazi symbols", *The ASEAN Post,* 4 March 2019, available at: https://theaseanpost.com/article/southeast-asias-fixation-nazi-symbols.

297 Interview with Munira Mustaffa, Chasseur Group,13 June 2024.

298 Mustaffa, "Radical Right Activities in Nusantara's Digital Landscape: A Snapshot".

The views of ultranationalist right-wing extremist actors can often influence and overlap with efforts by authoritarian state actors, including in the latter's attempts to control or repress those who oppose their political agenda.[299] A striking example of this was Buddhist nationalists in MaBaTha influenced government policy against the Rohingya minority in Myanmar in 2014 and 2015, prior to the widespread and genocidal[300] ethnic cleansing of that minority group by the military there in 2017.[301] Ideological proximity to or cooperation between right-wing extremists and state-backed actors can mean that the potential security threats they pose risk being overlooked, disregarded or even, in some national contexts, permitted by authorities.[302]

In addition to ultranationalist actors like those outlined above, there also exists an emerging pan-Asian movement whose members more closely resemble adherents of fascism and white supremacy in countries in the Global North. This movement is composed of a mixture of nationalities and identities but it defines its in-group as people of Asian ethnicity, those of other ethnicities being ostracised as the "out-group".[303] Recent research and government assessments on this relatively understudied phenomenon have described it as an emerging threat[304] that has coalesced in particular in digital online communities, blending Asian right-wing extremist ideologies and narratives with those of their "alt-right" counterparts.[305] Unlike nationalist or ethnonationalist movements in particular jurisdictions, the pan-Asian movement has so far failed to resonate with the broader population, possibly owing to the variations in the ideological focus of the different domestic movements across the region.[306]

In an indication of the threat posed by right-wing violent extremists in South-East Asia, in November 2020 police arrested a 16-year-old boy in Singapore on suspicion of plotting a terrorist attack. The boy had reportedly made plans to mount knife attacks on two mosques in

299 Janjira Sombatpoonsiri, "Manipulating civic space: cyber trolling in Thailand and the Philippines", *German Institute of Global and Area Studies,* June 2018, available at: https://www.giga-hamburg.de/assets/tracked/pure/21580615/web_asien_2018_03_english.pdf; Benjamin YH Loh and Sarah Ali, "Cybertrooper activity in state elections marks irreversible trend in Malaysia politics", *Channel News Asia,* 20 August 2023, available at: https://www.channelnewsasia.com/commentary/malaysia-state-election-politics-cybertrooper-social-media-ph-bn-pn-3707791; Interview with Nicole Matejic, Charles Sturt University, 12 June 2024.

300 "Report of the independent international fact-finding mission on Myanmar, *Office of the United Nations High Commissioner for Human Rights,* 12 September 2018, available at: https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf.

301 Eleanor Albert and Lindsay Maizland, "The Rohingya Crisis", Council on Foreign Relations, 23 January 2020, available at: https://www.cfr.org/backgrounder/rohingya-crisis.

302 "Terrorism and counterterrorism in southeast Asia", The Soufan Center, June 2021, available at: https://thesoufancenter.org/wp-content/uploads/2021/06/TSC-Report_Terrorism-and-Counterterrorism-in-Southeast-Asia_June-2021.pdf; Interview with Benjamin Mok and Saddiq Basha, RSIS, 6 June 2024; Interview with Munira Mustaffa, Chasseur Group, 13 June 2024.

303 Mustaffa, "Radical Right Activities in Nusantara's Digital Landscape: A Snapshot".

304 Hariz Baharudin, "External terrorism threats to region include Islamist and far-right extremists: ISD", *The Straits Times,* 24 June 2021, available at: https://www.straitstimes.com/singapore/external-terrorism-threats-to-region-include-islamist-and-far-right-extremists-isd.

305 "Alt-right", *Southern Poverty Law Center,* available at: https://www.splcenter.org/fighting-hate/extremist-files/ideology/alt-right.

306 Interview with Munira Mustaffa, Chasseur Group, 13 June 2024.

Singapore, having been inspired by the March 2019 attacks in Christchurch, New Zealand.[307] Press reports said he believed in the "great replacement" conspiracy theory.[308] In November 2023 Singaporean law enforcement arrested another teenage right-wing extremist, this time a 16-year-old, self-identified white supremacist of Chinese ethnicity, who had reportedly expressed a desire to commit a mass shooting, having "developed a strong hatred" of "African Americans, Arabs and LGBTQ+" people.[309]

Incidents of attempted or actual violence in South-East Asia perpetrated by right-wing violent extremists have been very infrequent compared with violence by those adhering to more regionally dominant extremist ideologies, such as those associated with ISIL/Da'esh and Al-Qaida, or by left-wing violent extremist groups like the New People's Army (NPA) in the Philippines.[310] Most South-East Asian governments have therefore focused more on these latter threats.[311] Right-wing extremists in the region operate, including as vigilantes,[312] either in support of or in parallel with the established authority, against real or exaggerated threats from left-wing or ISIL/Da'esh- or Al-Qaida-inspired violent extremist groups. This ideological or operational alignment may contribute to a perception among some South-East Asian governments that right-wing extremism may not pose a significant threat to national or regional security.

Abuse of digital technologies

The presence of right-wing extremism is probably most visible online, where nascent Austronesian supremacist networks have socialised and attempted to spread their message on mainstream platforms like X, Facebook, Instagram and TikTok.[313] These networks are believed to be composed of

307 "Detention of Singaporean youth who intended to attack Muslims on the anniversary of Christchurch attacks in New Zealand", *Ministry of Home Affairs,* 27 January 2021, archived from the original at: https://web.archive.org/web/20210131130757/https://www.mha.gov.sg/newsroom/press-release/news/detention-of-singaporean-youth-who-intended-to-attack-muslims-on-the-anniversary-of-christchurch-attacks-in-new-zealand; "Singapore boy held for Christchurch-inspired mosque attack plot", *BBC News*, 28 January 2021, available at: https://www.bbc.co.uk/news/world-asia-55836774.

308 "How a Sec 4 student who planned to attack mosques in S'pore was radicalised within months", *The Straits Times,* 30 January 2021, available at: https://www.straitstimes.com/singapore/how-a-sec-4-student-who-planned-to-attack-mosques-in-spore-was-radicalised-within-months.

309 "Singapore Terrorism Threat Assessment Report 2024", *Internal Security Department, Ministry of Home Affairs,* available at: https://www.mha.gov.sg/docs/default-source/default-document-library/sttar-2024.pdf.

310 Ben Schonveld and Robert Templer, "Assuming the Worst: Narratives and their impacts on violent extremism in southeast Asia", *United Nations Development Programme,* 2020, available at: https://www.undp.org/sites/g/files/zskgke326/files/publications/UNDP-RBAP-Violent-Extremism-in-SE-Asia-case-study-Assuming-the-Worst-2020.pdf; "Terrorism and counterterrorism in southeast Asia", *The Soufan Center,* June 2021, available at: https://thesoufancenter.org/wp-content/uploads/2021/06/TSC-Report_Terrorism-and-Counterterrorism-in-Southeast-Asia_June-2021.pdf; "The communist insurgency in the Philippines", *ACLED,* 13 July 2023, available at: https://acleddata.com/2023/07/13/the-communist-insurgency-in-the-philippines-a-protracted-peoples-war-continues/.

311 Interview with Munira Mustaffa, Chasseur Group, 13 June 2024.

312 "Failure to act against vigilante groups encourages mob justice, says LFL", *Free Malaysia Today,* 23 March 2024, available at: https://www.freemalaysiatoday.com/category/nation/2024/03/23/failure-to-act-against-vigilante-groups-encourages-mob-justice-says-lfl/; Interview with Munira Mustaffa, Chasseur Group, 13 June 2024.

313 Saddiq Basha, "The Creeping Influence of the Extreme Right's Meme Subculture in Southeast Asia's TikTok Community", *Global Network on Extremism and Technology,* 8 April 2024, available at: https://gnet-research.org/2024/04/08/the-creeping-influence-of-the-extreme-rights-meme-subculture-in-southeast-asias-tiktok-community/; Jonathan Suseno Sarwono, "'Yup, another far-right classic': the propagation of far-right content on TikTok in Malaysia, Indonesia, and the Philippines", *Global Network on Extremism and Technology,* 8 November 2023, available at: https://gnet-research.org/2023/11/08/yup-another-far-right-classic-the-propagation-of-far-right-content-on-tiktok-in-malaysia-indonesia-and-the-philippines/; Interview with Nicole Matejic, Charles Sturt University, 12 June 2024.

young people, based on their lexicon and choice of platform.[314] Research conducted into them in the past three years has shown their adoption of narratives and tactics utilised by white supremacists operating in Europe, North America or Australasia, repurposing them for their own regional context.[315]

On TikTok, for example, South-East Asian right-wing extremists have been observed to co-opt the racist slogan of "Total N****r Death (TND)", converting it into regionally-specific memes such as "Total Rohingya Death" (#TRD), "Total Chinese Death" (#TCD) or "Total Arab Death" (#TAD). In a sign that these accounts are subjected to suspension by TikTok, these acronyms have been disguised as more innocuous phrases, such as "totally cheerful day" or "totally amazing day".[316] Other accounts, which describe themselves as "nationalist", share memes supporting mass deportations or the ethnic cleansing of immigrants.

Figure 15. Examples of images shared on TikTok by South-East Asian right-wing extremist accounts, captured in July 2024.

There are also signs that right-wing extremists in South-East Asia are communicating in more private spaces, including messaging apps with varying degrees of encryption. An investigation carried out in preparation for this report in June 2024 found instances of Indonesian-speaking Telegram users expressing neo-Nazi views, including in discussions of *Mein Kampf* and the manifesto produced by the Christchurch attacker. The group also included several links to affiliated WhatsApp groups. Experts interviewed as part of this research told us that there are communities of South-East Asian right-wing extremists on Discord, a gaming-adjacent platform used primarily for messaging and content sharing within communities.[317]

314 Interview with Benjamin Mok and Saddiq Basha, RSIS, 6 June 2024.

315 Interview with Benjamin Mok and Saddiq Basha, RSIS, 6 June 2024.

316 Jonathan Suseno Sarwono, "Tracing Austronesian Supremacy Rhetoric on Social Media: Its Impact on the Fate of Rohingya Refugees", *Global Network on Extremism & Technology,* 28 May 2024, available at: https://gnet-research.org/2024/05/28/tracing-austronesian-supremacy-rhetoric-on-social-media-its-impact-on-the-fate-of-rohingya-refugees/.

317 Interview with Benjamin Mok and Saddiq Basha, RSIS, 6 June 2024; Jakub Guhl, "Discord & Extremism", *Institute for Strategic Dialogue,* available at: https://www.isdglobal.org/explainers/discord-extremism/.

South-East Asian right-wing extremist networks also engage in more offensive digital tactics, such as trolling or doxxing their perceived opponents.[318] Thousands of right-wing Malaysian trolls reportedly targeted *Jewish News*, a British newspaper, with Nazi imagery and abusive comments on Facebook in January 2019. The paper had been covering the decision by an international sporting event to withdraw its upcoming championships in Malaysia after the government there had reportedly banned Israeli athletes from competing.[319]

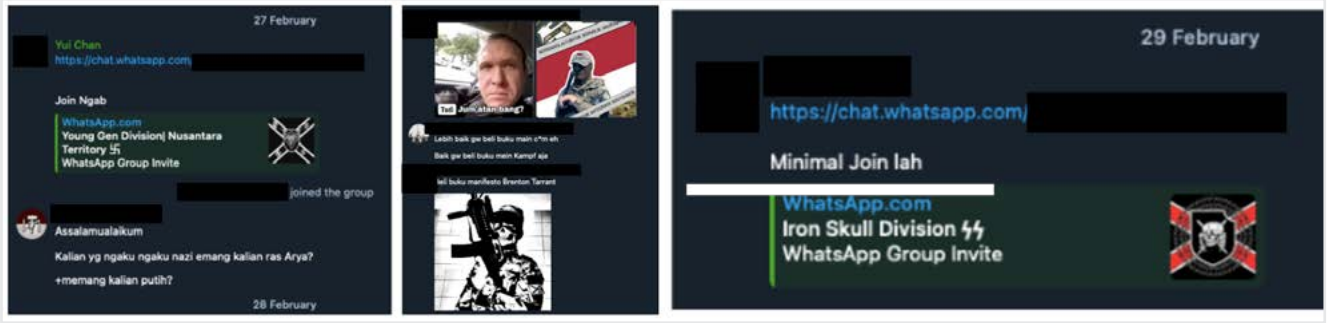

Figure 16. Screengrabs of Indonesian right-wing extremist Telegram chats, captured in June 2024.

Right-wing extremists in South-East Asia mostly do not appear to have the intent or the capability to mount more technical cyber-attacks, although several pro-government hacktivist groups do operate there. A 2016 press report cited an increase in nationalist hackers in Myanmar, for example, who were reportedly targeting the digital assets of both foreign states and domestic critics of the government, including the Rohingya minority.[320] In another example, DragonForce Malaysia is a hacktivist group that has long targeted Indian websites in DDoS and web defacement attacks.[321] It has operated, in particular, in support of Palestinians since the Hamas terror attack on Israel in October 2023.[322] At the time of writing it had an active deep web forum with more than 26,000 members.

318 Interview with Munira Mustaffa, Chasseur Group, 13 June 2024.

319 Jack Mendel, "Thousands of Malaysian trolls target Jewish News", *Jewish News,* 28 January 2019, available at: https://www.jewishnews.co.uk/thousands-of-malaysian-trolls-target-jewish-news/; Colin Drury, "Malaysia stripped of international swimming tournament after banning Israel over treatment of Palestinians", *The Independent,* 27 January 2019, available at: https://www.independent.co.uk/news/world/asia/malaysia-world-para-swimming-championships-israel-ban-palestine-middle-east-controversy-a8749381.html.

320 "New wave of Myanmese hackers claim to have targeted Thai government websites", South China Morning Post, 25 February 2016, available at: https://www.scmp.com/news/asia/southeast-asia/article/1916549/new-wave-myanmese-hackers-claim-have-targeted-thai.

321 "DragonForce Malaysia", *Radware,* available at: https://www.radware.com/security/ddos-knowledge-center/ddospedia/dragonforce-malaysia/.

322 Nate Nelson, "DragonForce Gang Unleash Hacks Against Govt. of India", *ThreatPost,* 15 June 2022, available at: https://threatpost.com/hackers-india-government/179968/.

{ CONCLUSION }

This report aims to provide insights into manifestations of right- and left-wing violent extremism in the Global South, and their exploitation of digital technologies, via case studies in South America, Africa and Asia. While these case studies are distinct from one another, and represent different forms of violent extremism that have arisen out of particular national or regional contexts, several key trends can be identified that warrant further attention and should guide further programmatic and research activities.

First, this study demonstrates the inherently interconnected nature of the online and offline activities of violent extremist groups, networks and movements. The use of digital technologies by violent extremist actors, as by the general population, is an integral part of day-to-day communication and productivity, which means that neither online nor offline spaces can be studied in isolation from the other.

Second, while violent extremism is a term used predominantly to apply to non-state actors, several of the case studies here show varying degrees of connection between violent extremists and state-backed actors. This includes ideological proximity, pro-government vigilantism, state-backed cyber activities, and evidence of potential operational cooperation between diverse threat actors. Such convergences make effective responses to these issues more difficult, including from the perspectives of domestic politics, content moderation and international diplomacy.

Third, some of the ideological movements covered in this report may not have as sophisticated or widespread online presence as other violent extremist movements, and there is minimal evidence to suggest that they have engaged in destructive cyber-attacks to any significant degree. A common theme, however, is that these movements operate across multiple online services, and demonstrate a relatively advanced understanding of how to exploit digital technologies to further their objectives. Especially in some of the regional case studies discussed here, these movements are able to exploit apparent gaps in technology responses to violent extremism, and thereby maintaining a relatively stable and open presence on mainstream platforms.

Finally, it must be acknowledged that right- and left-wing narratives have often appeared in mainstream political discourse – including thanks to political figures and mainstream press outlets who (intentionally or unintentionally) repeat extremist narratives, possibly influenced by extremist information operations online. It is therefore essential that nonpartisan definitions of terms such as “extremism” and “violent extremism” should be agreed, referred to, and upheld.

The below recommendations serve as general guidelines for Member States and should be adapted to each country’s specific circumstances and realities. Although these recommendations are not exhaustive, they strive to provide foundations to foster fruitful conversations among relevant stakeholders and promote effective collaboration.

Recommendations

* **Those professionally engaged in countering violent extremism should move away from conceptualising "online" and "offline" spaces as being fundamentally separate.** Digital platforms are increasingly playing an essential role in the everyday lives of people and organisations, and distinctions as to when an interaction happens "online" versus "offline" are becoming increasingly blurred. Technology companies have a responsibility to counter the use of their services for illegal purposes and it is right that they should be subjected to the scrutiny and accountability requirements they often are constrained by. Demonising digital platforms as the sole cause of issues such as violent extremism can fail to recognise that violent extremism is fundamentally a people and societal problem, albeit often enabled or accelerated by digital technologies. Overly focusing on the digital aspects carries the risk of underplaying the inherently human drivers of violent extremism and, thereby, potentially hindering effective, holistic responses to it.

* **Counter-terrorism (CT) and Preventing or Countering Violent Extremism (PCVE) approaches should avoid considering violent extremism online as an isolated phenomenon**. Evidence presented in this report suggests that manifestations of right- and left-wing violent extremism in South America, Africa and Asia, as well as globally, are increasingly overlapping with other issues relating to online harms, including dis- and misinformation, Child Sexual Abuse Material (CSAM), cybercrime, and mainstream authoritarian or radical politics. Responses to these threats should not operate in isolation from one another; work should be done to improve the sharing of information between sectors across the industry.

* **The public and private sectors should leverage existing CT and PCVE initiatives and mechanisms in the Global South to address also the challenges posed by violent extremism in the digital realm**, with the ultimate aim of preventing and countering the abuse of digital technologies by violent extremist actors. South-South and Triangular Cooperation (SSTC) should be promoted as a means of facilitating international cooperation, complementarily to North-South cooperation. Further work should be done to establish more effective partnerships and coordination between technology companies and Member States in the Global South, engaging in cross-jurisdictional collaboration on the issue of terrorist- and violent extremist-operated websites. In this context, the relevant UN agencies should invest in facilitating policy dialogues in a multi-stakeholder format to address concrete issues, such as the technology sector's apparent under-investment in moderating content in the Global South compared with that in the Global North.

* **Engagement with local communities, through collaboration with civil society organisations, should be embedded in efforts to address violent extremist content online.** This type of engagement should aim at fostering media and information literacy in users and dismantling information systems that rely on hateful narratives, borderline content and mis- or disinformation campaigns. National and local capacities should be developed in order to produce innovative and practical solutions, leveraging the active participation of young people to promote local ownership of sustainable activities. Led by young people, Hedayah's program, Tech2Protect, incorporates this approach and showcases successful initiatives aimed at addressing the terrorist use of the Internet in Tunisia. Such a model should be adapted to other situations, taking into account domestic contexts and the threats posed by both non-state and state-backed actors. Additionally, Member States and technology companies should seek advice on cultural and linguistic factors from civil society and community-based organisations, to ensure context-responsive strategies and measures. These organisations should be empowered to lead the creation and promotion of grassroots efforts to counteract decentralised violent movements and widespread violent extremist narratives.

Recommendations to Member States

- **Member States should dedicate further resources to investigating and disrupting violent extremism and other criminal exploitation of the dark web and encrypted communication platforms**. While the dark web forms part of a broader online violent extremist ecosystem that is also active on the surface and deep web, it continues to pose serious challenges to law enforcement investigations and the removal of illegal content. Member States should look to leverage technical, investigative or legislative tools, such as those (previously cited) used by Australian and Dutch law enforcement,[323] to find and disrupt violent extremist and criminal networks on the dark web and encrypted communication platforms.

- **Member States should review the strength of their cybersecurity in the face of a growing threat posed by cybercriminals, state-backed actors, and non-state actors with non-financial motivations**. Member States should devote particular attention to boosting and strengthening cybersecurity in those Member States with less knowledge or fewer resources in the realm of cybersecurity, especially in the Global South. This should include workshops, knowledge sharing and capacity-building activities.

Recommendations for Research

- **More research is needed into manifestations of right- and left-wing violent extremism in the Global South, and these actors' exploitation of digital platforms.** Research continues to be strongly focused on how these ideologies manifest in the Global North context, despite their long-standing manifestations elsewhere in the world. Donors should allocate funds for projects that involve researchers and organisations based in these regions. Research should aim in particular to understand better how local or domestic movements are interacting with or being influenced by international dynamics via digital technologies, especially via gaming and adjacent platforms – an increasingly worrying trend in South America, Africa and Asia.

- **Further research should be undertaken into the radicalising pathways to ideologies or movements affiliated with violent extremism potentially followed by hacktiv-**

323 The Hon. Karen Andrews MP, "New powers to combat crime on the dark web", Home Affairs, Australian Government, 25 August 2021, available at: https://minister.homeaffairs.gov.au/KarenAndrews/Pages/new-powers-to-combat-crime-on-the-dark-web.aspx; Andy Greenberg, "Operation Bayonet: Inside the sting that hijacked an entire dark web drug market", Wired, 8 March 2018, available at: https://www.wired.com/story/hansa-dutch-police-sting-operation/https://www.wired.com/story/hansa-dutch-police-sting-operation/.

ists. While significant research has been undertaken to date into the radicalisation processes of individuals into physical violence, significantly less research has been conducted into the radicalisation of individuals into extremist hacking, and the extent to which established understandings of radicalisation may be applied to actors whose involvement in extremism is confined to offensive digital activities. Such research should aim to inform, and ultimately be complemented by, prevention activities.

Recommendations to the Technology Sector

- **More work should be done on developing approaches to supplementing content removal**. The removal of violent extremist accounts and content serves an important purpose in the broader toolkit for countering the violent extremist exploitation of digital platforms, but it is not a long-term solution. While it may contribute to reducing the overall audience of violative actors on particular platforms, they have been shown to return quickly elsewhere online or to engage in sophisticated tactics to evade content moderation. Complementary solutions should include demonetisation, education and review for users attempting to post potentially violative content; fact-checking or community notes; and contextual labelling of specific accounts or material by technology platforms.[324] Progress has been made in this area by some of the larger companies, but such approaches need to be further developed across the industry and applied globally. In addition, a more widespread adoption of red team threat modelling by technology companies could enhance their understanding of how violent extremist actors take advantage of the companies' services and products online.

- **The technology sector should continue its efforts to build and maintain effective collaboration and communication between companies to counter and prevent the increasingly cross-platform nature of violent extremist ecosystems.** Industry initiatives like the Global Internet Forum to Counter Terrorism (GIFCT) should be supported in expanding their membership to encompass a greater proportion of the wider Internet industry. Strengthened communication frameworks and expanded collaboration spaces should aim to mitigate the risk that companies' moderation efforts might be focused exclusively on their own services. Companies should work to share information more effectively with other platforms, to support smaller or less-resourced companies proactively, and to mutualise tactics, techniques and procedures in order to prevent and counter terrorist and violent extremist content online, bearing in mind the differences between the functionalities and settings of different companies' products and services.

324 Erin Saltman, Micalie Hunt, "Borderline Content. Understanding the Gray Zone", GIFCT, 2023, available at: https://gifct.org/wp-content/uploads/2023/06/GIFCT-23WG-Borderline-1.1.pdf.

Recommendations to International Inter-governmental Organizations

- **International inter-governmental organisations, such as the United Nations, should foster strategic sessions among Member States to address definitions of contentious issues like violent extremism.** The increasingly fragmented nature of definitions with regard to such issues is making it more and more difficult for companies that are invested in moderating such material globally to do so consistently, especially when confronted with conflicting legislative regimes and broad or hard-to-agree-on definitions. Decisions on these issues should not be the exclusive preserve of private, unelected companies, nor should they be the sole responsibility of national governments, especially when those companies or governments are based in different jurisdictions from those where these policies or laws are enforced. Relevant international inter-governmental organisations should foster multi-stakeholder dialogue to promote a harmonised international approach to definitional challenges. Established guidance frameworks, under the Digital Services Act (DSA) or Terrorist Content Online (TCO) legislation in the European Union, for instance, could be leveraged when working towards voluntary guidelines on a more international level. In addition, democratic governments should provide diplomatic support for technology companies when the latter are facing pressure, from repressive governments, to act in violation of international human rights law.

- **Relevant international inter-governmental organisations should step up their responsibilities to maintain international peace in the realm of cyberspace.** In this regard, the UN system could consider holding a briefing, ideally at a regular cadence, to review the evolving cyber threat landscape in terms of the existing mandate and agenda of the Security Council. Developing assessments and strategies to deal with the evolving cyber threat landscape by incorporating comprehensive insights from the UN system, the private sector, civil society and academia would help to ensure that the Council remained abreast of new developments and their implications for international peace and security. Specific briefings should focus on interconnected threats, terrorism, violent extremism, cybercrime and cybersecurity, to draw Member States' attention to threats that might not otherwise be present, or sufficiently recognised, in their countries, but are growing internationally. The briefings should also aim to foster greater collaboration between Member States.