Ponder the Improbable since 1996

CENS EXPERT SURVEY ON EXTREMISM REPORT

CURRENT AND EMERGING THREATS

Policy Report

July 2021

Joseph Franco

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Policy Report

CENS EXPERT SURVEY ON EXTREMISM REPORT

CURRENT AND EMERGING THREATS

Joseph Franco

July 2021

TABLE OF CONTENTS

Executive Summary

The CENS Expert Survey assessed prevailing sentiment among various violent extremism (VE) stakeholders. Among Southeast Asia experts, “Salafi-Jihadi terrorism and recruitment” was considered the most relevant issue. In the offline space, family connections were cited as the “most important” conduit for recruitment. Outside Southeast Asia, “far-right terrorism and recruitment” ranked a close second to Jihadi threats. It was also observed that VE groups in other regions were 15 per cent more likely to use online tools. Perceptions on whether VE groups exploited the COVID-19 pandemic were virtually the same across regions. COVID-19 was not as important a driver for inciting attacks in Southeast Asia or beyond. As societies spend more time online, VE groups have adjusted their recruitment and organisational activities.

Introduction

The COVID-19 pandemic overlays increased uncertainty upon the threat posed by violent extremist (VE) groups. The Centre of Excellence for National Security (CENS) designed an online expert survey, primarily to assess the pandemic's impact on the current state of play among VE groups. The survey also examines how preventing and countering VE (P/CVE) initiatives fared. This is the first of two RSIS Policy Reports presenting key findings from the two month-long "*Expert Survey on Violent Extremism and its Prevention"* or the CENS Expert Survey (CES). This report is on "Current and Emerging Threats" and will be subsequently followed by a Policy Report on the assessment of P/CVE trends.

The CENS Expert Survey

Between January to March 2021, CENS conducted an expert survey to assess the prevailing sentiment among various VE stakeholders based on a survey instrument created in 2020. A list of potential respondents was collated, and initially comprised notable academic researchers, practitioners, and policymakers who work on P/CVE related issues. Most respondents listed were previously speakers or participants in CENS-organised international workshops and seminars. Other researchers have used the same expert survey sampling method in a study focused on "what role does technology, particularly computer mediated communications, play in violent extremism?"[1]

As the CES was administered, other experts and stakeholders were invited to answer the online survey form. In total, CENS elicited 65 anonymised responses. Respondents were contacted from seven regions: Australasia, Southeast Asia, South Asia, Middle East and North Africa (MENA), Sub-Saharan Africa, Europe, and the Americas. A majority or 34 of the respondents indicated that their geographical area of focus is Southeast Asia. Europe and the Americas were the second and third most selected geographical areas.

The CES comprised 17 questions, which included multiple-choice, ranked choice, and open-ended questions.[2] Six questions were specifically designed to investigate the impact of COVID-19 on VE phenomena. Respondents were asked to assess whether the pandemic has affected activities of VE groups. The survey also prompted respondents to assess how governments, non-government organisations, and civil society organisations have adapted.

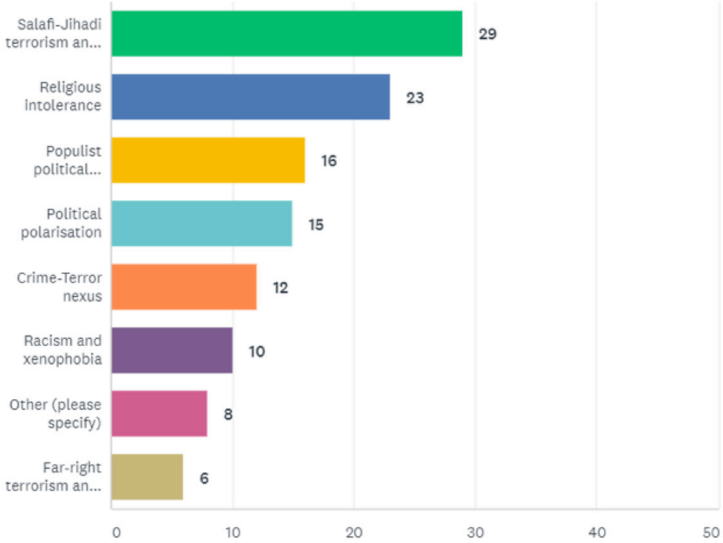
[1] Khalil, Lydia. "GNET Survey on the Role of Technology in Violent Extremism and the State of Research Community – Tech Industry Engagement." *Lowy Institute,* May 5, 2021, pp. 5, 15. www.lowyinstitute.org/publications/gnet-survey-role-technology-violent-extremism-and-state-research-community-tech-0

[2] See Annex.

Perceptions Among Southeast Asia Specialists

Reflecting CENS's location and primary research focus in Southeast Asia, 53 per cent of the respondents identified themselves as geographically focused on Southeast Asia. Among them, 85 per cent considered "Salafi-Jihadi terrorism and recruitment" the most relevant issue (See Figure 1). The second issue of concern was "religious intolerance" in Southeast Asia. Nearly tied at third place were the emergence of "populist political parties or movements" and "political polarisation". Coming in last was "far-right terrorism and recruitment".[3]

Figure 1: Most relevant issues for Southeast Asia specialists



Experts observed that from 2019–2021, Southeast Asian VE groups tended to slightly favour online over offline recruitment methods. Respondents were asked to rate on a scale how much VE groups recruited using "fully online" (0 points) or "fully offline" (100 points) methods. The average rating was 46, which signifies how VE recruitment was slightly skewed to online methods.

[3] The CES used a broad definition of "far right" VE in its questionnaire to cover organised VE groups espousing fascist, ethnocentric, and sectarian narratives.

When asked to elaborate, all the Southeast Asia experts shared that "private messaging apps" functioned as the primary online recruitment tool. Telegram was mentioned as the preferred choice due to its reputation as a "more secure" app. Other messaging apps mentioned by the respondents were Viber and WhatsApp. Coming second was "social media platforms", with 97 per cent respondents citing it. Facebook was the platform of choice for VE groups in Southeast Asia. One respondent pointed out that Facebook provides wide reach, especially through its Groups function. Facebook's built-in Messenger app allowed VE group recruiters to directly message a specific individual scouted for recruitment.

In the offline space, family connections were cited as the "most important" conduit for recruitment. It was almost tied with "friends and/or friend group" that received just a 3 per cent lower rating. This suggests that involvement in VE groups was often facilitated through a person that a prospective recruit already knows. The two succeeding offline venues were "prisons" and "activist/charitable associations". Occupying the lowest rung in the ratings were "study groups, sport clubs, gyms".

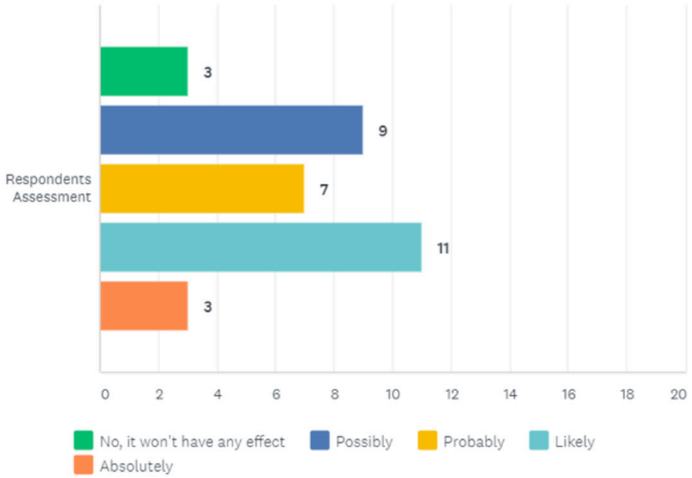
CES respondents were also asked which evolving technologies were used by VE groups in Southeast Asia. "Encrypted communications" was used the most according to 79 per cent of the respondents, which validates earlier findings on how VE groups depend heavily on messaging apps. The second-ranked technology, at 64 per cent, was the use of "improvised explosive devices" (IEDs). Coming third, at 46 per cent, was "unconventional/indirect fund transfer methods", such as the use of in-game currencies. Surprisingly, the use of cryptocurrencies ranked lower as a form of illicit fund transfer. Among the technology categories used in the CES, deployment of ransomware and malware, and unconventional munitions (i.e., chemical, biological, radiological weapons) ranked last.

Regarding the COVID-19 pandemic, Southeast Asia experts felt that VE groups exploited the prevailing public health emergency. On a scale marked 0 for "not exploited" to 100 for "fully exploited", the average response was 64 points or "slightly exploited". In a follow up question, it was determined that VE groups exploited the pandemic by "undermining trust in the state". This was followed by the promotion of narratives to provoke "societal divisions". Coming in third were actions not focused on narratives, but to "consolidate" existing levels of membership.

These courses of action by VE groups were indirectly caused by second-order effects created by the pandemic. Ranking at the top of COVID-associated factors was the "socio-economic disruption" caused by the pandemic. The second most relevant factor was the divisive nature of the "online information space". Ranking as "least relevant" in terms of dynamics unleashed by the pandemic was the notion of "distracted security agencies", especially security personnel involved in COVID-19 mitigation and response, becoming targets for VE groups.

In conclusion, a third of Southeast Asia experts deemed it "likely" that the pandemic would lead to more extremist violence in coming years (Figure 2).

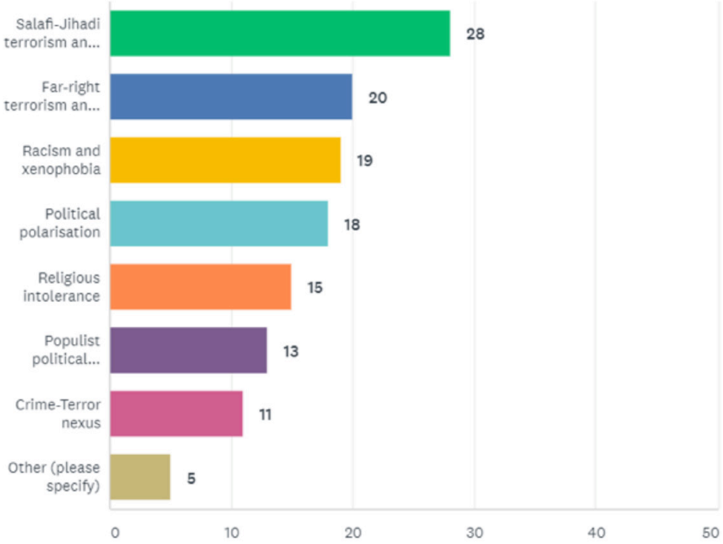
Figure 2: Assessment whether the pandemic would lead to increased extremist violence in Southeast Asia



Perceptions Outside Southeast Asia

Experts on areas outside of Southeast Asia observed that Salafi-Jihadi terrorism was the "most relevant" issue to their region. The second and third ranked issues are "far-right terrorism and recruitment" and "racism and xenophobia", respectively (Figure 3). This ranking suggests how far-right terrorism is more relevant outside of Southeast Asia.

Figure 3: Most relevant issues outside Southeast Asia



Compared to observations made about Southeast Asia, VE groups in other regions were 15 per cent more likely to use online tools for recruitment. When asked what specific online tools were used, both private messaging apps and social media platforms were ranked at the top. Respondents emphasised the prevalence of Facebook and Telegram usage among VE groups. What differs in the non-Southeast Asian context was the greater importance of websites, specifically online forums. In the offline space, respondents ranked "friends and/or friend groups" as the most important sources for recruitment. This was followed by "family and kin networks" and "prisons". Schools and universities came in last as sites for VE recruitment.

Like Southeast Asia, VE groups in other regions used encrypted communications and IEDs. What distinguishes regions outside Southeast Asia is the wider adoption of cryptocurrencies by VE groups. However, respondents did not state the type of cryptocurrency in use. There was also no information on whether the underlying blockchain technology that powers cryptocurrency was exploited by VE groups. Another contrast to Southeast Asia was the higher ranking assigned to the use of "coordinated inauthentic online behaviour" such as sock puppets to sway public opinion.[4]

Respondents also reported more instances of tactical or strategic convergence between VE groups on the one hand and non-ideological groups such as organised crime on the other. In one example, certain violent Islamist groups in the Caucasus region extended their protection racket to cover crime gangs. Another example given was how VE groups initially linked up with illicit arms dealers. Weapons-related transactions would pave the way for further interactions and transactions with members of organised crime syndicates. Among the far-right VE groups, connections were made with subcultures like "motorcycle gangs" in the United States.

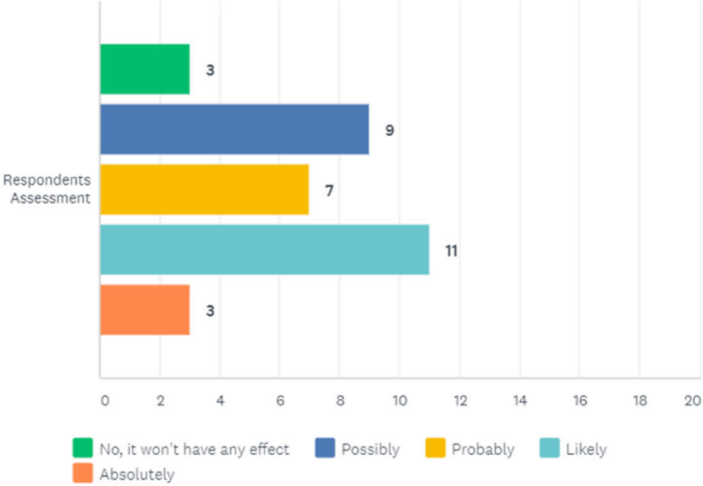
Perceptions on whether VE groups exploited the COVID-19 pandemic were virtually the same, which was rated at 63 per cent, just one percentage point lower than the reported figure by Southeast Asia-focused respondents. Similar responses were also seen when respondents were asked how VE groups outside Southeast Asia exploited the pandemic. Groups took advantage indirectly by treating the pandemic as an opportunity to undermine trust in the state. The other VE group initiatives that can be attributed to the pandemic are efforts to provoke "societal divisions" and "consolidating support". Again, conducting attacks was considered the least probable VE group course of action for the respondents.

When asked to determine which aspects of the pandemic and pandemic recovery would lead to heightened VE activity, respondents pointed to the divisive nature of the "online information space". Coming in second is the "socio-economic disruption" created by the pandemic. "Increased internet and/or social media usage" due to community quarantines and lockdowns was cited as the third most important factor. CES respondents who focus in areas other than Southeast Asia appeared more optimistic.

[4] Sock puppets are defined as online identities used in "undesired behaviour by deceiving others or manipulating discussions". See Srijan Kumar et al., "An Army of Me: Sockpuppets in Online Discussion Communities." Paper presented at the 26th International World Wide Web Conference, April 2017. DOI:10.1145/3038912.3052677.

In conclusion, most (45 per cent) assessed that it is “possible” that the pandemic would lead to more VE group violence in coming years (Figure 4).

Figure 4: Assessment whether the pandemic would lead to increased extremist violence outside Southeast Asia



Convergence and Divergence

The pandemic has underscored what would likely be a more complex threat environment or perhaps a "universal recognition [among experts] that other forms of extremism have proliferated."[5] Based on the CES it is reasonable to believe that while Southeast Asia reflects global VE trends, important distinctions must be made.

The Salafi-Jihadi terrorist threat remains the most relevant threat across all regions. The biggest divergence is how other regions view far-right VE groups. Southeast Asia remains largely unperturbed by this strain of political violence. Looking more closely at the responses, experts covering the Americas and Europe placed far-right extremism on an almost equal footing with the jihadist threat. Far-right extremism was deemed relevant by 74 per cent of the respondents, while jihadist threat was deemed relevant by 78 per cent.

It is unclear whether this is due to Southeast Asia's preoccupation with religious and/or ethnonationalist-driven VE, or a lack of appreciation over what constitutes far-right extremism; or a combination of both. Speakers at a recent CENS Online Workshop co-organised with the Global Network on Extremism and Technology (GNET), argued that increasing intolerance and violence in India and Myanmar could be considered as far-right extremism, perhaps with Asian characteristics.[6] Recruitment and involvement into VE groups in Southeast Asia appears to utilise family and kinship-driven networks. This is in contrast to the greater reliance on friends and peer groups in other regions.

It was also clear from the CES that online tools are exploited by VE groups globally. This is similar to trends reported by a GNET report on how "internet enabled communication and online activities" enabled "real world harm".[7] In fact, the United Nations has pointed to "increased recruitment online" and "increased spread of disinformation, conspiracy theories, and propaganda" as "new challenges" in P/CVE.[8] According to the CES, Facebook and Telegram are far ahead of other platforms and apps for recruitment purposes.

[5] Clarke, Colin P. "From COVID to the Caliphate: A Look at Violent Extremism Heading into 2021." *United States Institute of Peace,* December 15, 2020. www.usip.org/publications/2020/12/covid-caliphate-look-violent-extremism-heading-2021

[6] Sumpter, Cameron, et. al. "GNET-CENS Online Workshop on Right Wing Extremism: East and West", Centre of Excellence for *National Security,* May 7, 2021. https://www.rsis.edu.sg/rsis-publication/cens/gnet-cens-online-workshop-on-right-wing-extremism-east-and-west/

[7] Khalil, Lydia. "GNET Survey on the Role of Technology in Violent Extremism and the State of Research Community – Tech Industry Engagement." *Lowy Institute,* May 5, 2021, p. 18. www.lowyinstitute.org/publications/gnet-survey-role-technology-violent-extremism-and-state-research-community-tech-0

However, in Southeast Asia, trust in online tools appeared constrained to the areas of propaganda and mass outreach. Terrorist financing reflects continuity, with the widespread use of cash and the very limited use of non-digital assets such as cryptocurrencies. Slower technology adoption in Southeast Asia can be attributed to multiple factors. It can simply be an issue of limited internet access or connectivity. Related to this is the relative costs in using online tools for operational activities versus offline tools (i.e., use of human couriers for communications and financial transfers), or it can be a fundamental issue of trust. Family networks can be deemed more trustworthy in planning and executing attacks, versus trusting online interlocutors, who may be under government surveillance.

[8] United Nations Institute for Training and Research. “Impact of COVID-19 on Violent Extremism and Terrorism.” Accessed June 14, 2021. www.unitar.org/sites/default/files/media/file/COVID-19%20and%20Its%20Impact%20on%20Violent%20Extremism%20and%20Terrorism%20Factsheet_0.pdf

On COVID-19 and Violent Extremism

According to CES respondents, COVID-19 was not as important a driver for inciting VE group attacks in Southeast Asia or beyond. Rather than directly triggering attacks, the pandemic provided VE groups with additional angles to underscore the lack of or weakness of governance in contested areas. VE groups may differ in ideology but all of them persist due to dysfunctional governance, whether in specific geographical areas or thematic issue areas. This CES finding is consistent to observations made by experts over "how violent extremist groups have sought to exploit economic grievances relating to loss of employment by offering financial support to affected individuals … perceiving this as an opportunity to indoctrinate or recruit them."[9]

This should serve as a cautionary note for policymakers who may inadvertently conflate P/CVE initiatives with pandemic response or mitigation measures. Public health measures are neither intrinsically against nor favourable to P/CVE. A minimalist position would have P/CVE in its own lane, with pandemic response insulated from the discourse of securitisation. A more maximalist response would integrate P/CVE intended outcomes into the COVID-19 response.

The online space has gained even more importance for VE groups during the pandemic. Greater reliance on the online space will likely continue in the near-term as populations grow more accustomed to digital tools. This dynamic is unleashed by factors beyond the control of VE groups themselves, and more attributable to external factors. These factors can be intrinsically benign, such as populations having more time for online activities or internet use. It can also reflect how online tools open new avenues for populations to express disagreement or even dissent against governments.

[9] UN Security Council – Counter-Terrorism Committee. "CTED Paper - The impact of the COVID-19 pandemic on counter-terrorism and countering violent extremism." June 2020. www.un.org/securitycouncil/ctc/content/cted-paper%E2%80%93-impact-covid-19-pandemic-counter-terrorism-and-countering-violent-extremism

Conclusion

The CENS Expert Survey was designed to provide a broad scan of P/CVE trends across regions. The primacy of Salafi-Jihadi ideology as the “most relevant” threat was unsurprising. However, outside of Southeast Asia, the rise of the far-right has become an equal source of concern. Fortunately, the effect of the pandemic on VE group activities are indirect. But as societies spend more time online, VE groups have adjusted their recruitment and organisational activities. Their reliance on “encrypted communications” means that more effort is needed by governments on PVE rather than CVE. The next Policy Report will examine the trends in P/CVE, as shared by the CES respondents.

About the Author

Joseph Franco specialises in countering violent extremism (CVE) and counterinsurgency. As Research Fellow with the Centre of Excellence for National Security (CENS) at RSIS, Joseph examines terrorist networks in maritime Southeast Asia and best practices in CVE. He obtained his MSc in International Relations at RSIS through an ASEAN Graduate Scholarship. He is a frequent resource person for international media such as the BBC, Channel News Asia, Deutsche Welle, and TIME.

Joseph previously worked for the Chief of Staff, Armed Forces of the Philippines (AFP), and the J3, AFP. He provided consulting services for the enhancement of internal security operations; deployment of peacekeeping forces; and the employment of special operations forces. Joseph was also the lead writer of the AFP Peace and Development Team Manual—a novel, community-based approach to counterinsurgency.

About the Centre of Excellence for National Security (CENS)

The **S. Rajaratnam School of International Studies (RSIS)**) is a global think tank and professional graduate school of international affairs at the Nanyang Technological University, Singapore. An autonomous school, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. With the core functions of research, graduate education, and networking, it produces research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, Cybersecurity, Maritime Security and Terrorism Studies.

CENS is a research unit of RSIS at the Nanyang Technological University, Singapore. Established on 1 April 2006, CENS raison d'être is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues. CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs.

For more details, please visit www.rsis.edu.sg and www.rsis.edu.sg/cens. Join us at our social media channels at www.rsis.edu.sg/rsis-social-media-channels or scan the QR code.

Annex — CES Questions

Q1: Which is/are your geographical area(s) of focus?

Q2: What are issues most/relevant in your country/region of focus?

Q3: Which aspects of counter-terrorism policy in your country/region should be prioritised?

Q4: Over the past two years, have violent extremists in your country/region of focus prioritised online or offline methods of recruitment?

Q5: Which of the following media tools do violent extremists use for recruitment in your country/region of focus?

Q6: Based on the online media you selected, which should be given most attention, and why?

Q7: Which offline venues are the most important sources of violent extremist recruitment in your country/region of focus?

Q8: Which areas of P/CVE policy and practice should be prioritised in your country/region of focus?

Q9: Who should be the key stakeholders in P/CVE initiatives in your region/country of focus?

Q10: Which new/emerging technologies are violent extremists using in your country/region of focus?

Q11: Are you seeing evidence of tactical/strategic convergence between ideological and non-ideological violent organisations in your country/region of focus? If so, please elaborate.

Q12: Have violent extremists in your country/region of expertise sought to exploit the COVID-19 pandemic?

Q13: Are violent extremists in your country/region of expertise seeking to exploit the COVID-19 pandemic?

Q14: Which COVID-19 associated dynamics have violent extremists sought to exploit in your country/area of focus?

Q15: Will the COVID-19 pandemic lead to more extremist violence in coming years?

Q16: What form/type of violence? (Please expand on Q16)

Q17: What aspect of the pandemic and recovery period will potentially generate more violent extremist activity?

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Nanyang Technological University, Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg