

How a Full-Spectrum Approach Will Address Critical Gaps in Countering and Preventing Extremist and Terrorist Threats

By the Strategies Against Violent Extremism (SAVE) team of the 1st NAEF

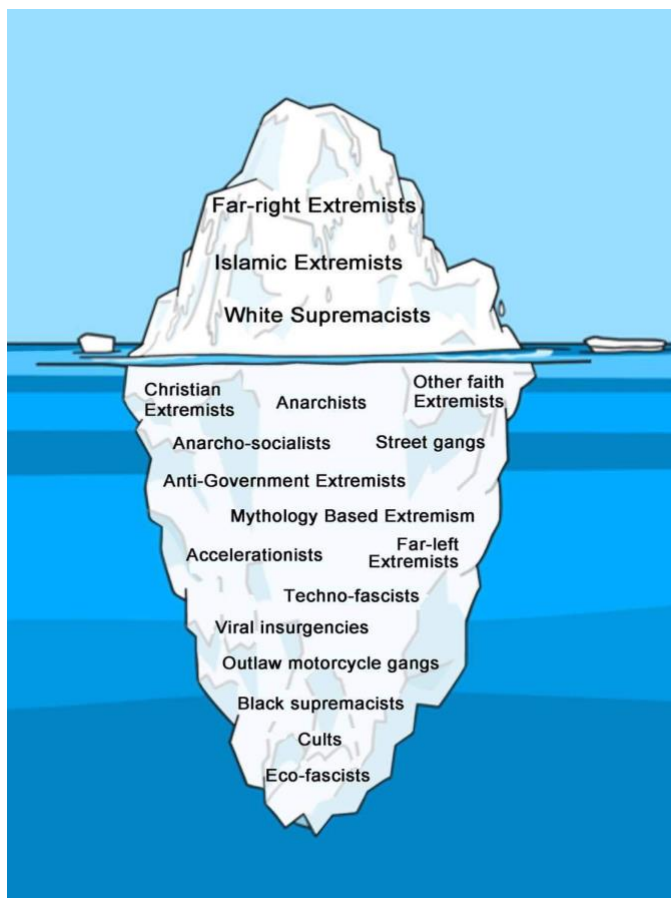




TABLE OF CONTENTS

Executive Summary	p.3
Introduction	p.5
Situation	p.6
Problem	p.11
Recommendations	p.14
Conclusion	p.18
About	p.19
References	p.20



EXECUTIVE SUMMARY

Global Peace and Security is Being Harmed by Not Considering All Extremist and Terrorist Threats

This whitepaper by the *Strategies Against Violent Extremism (SAVE)* team of the 1st NAEF calls for urgent change to the **counter and preventative extremism and terrorism industry** across the Five Eyes alliance. It highlights problems and complexity in the landscape, identifies critical and dangerous gaps and blind spots, and proposes a Full-Spectrum approach to enhance practice and operational effectiveness.

A PROBLEMATIC AND COMPLEX LANDSCAPE

It is becoming increasingly problematic for industry leaders and practitioners to fight extremist and terrorist threats. Technological advancements have enhanced the awareness of observable threats, and extended the reach of nefarious actors seeking to manipulate vulnerable people. Complexity has been further increased by the large number of communications platforms and technologies; many different categories of practitioners and intersecting fields of practice; and a large and diverse range of threats and actors.

CRITICAL GAPS AND BLIND SPOTS

Our industry faces significant challenges in addressing these threats. Existing systems lagging behind advances and adaptations made by extremists and terrorists due to critical gaps and blind spots. The most significant blind spot is a **highly saturated focus on a narrow spectrum of threats and manifestations** – particularly Islamic or right-wing extremism – to the detriment of considering other new or evolving threats. Secondly, operational effectiveness suffers from an undefined industry architecture and lack of best practices – there are no common definitions, standards, or methodologies. Finally, there are difficulties in addressing youth extremism: inappropriate programming; and a focus on mainly child soldiers, to the detriment of at-risk youth in non-conflict and domestic spaces.

A FULL-SPECTRUM APPROACH TO THREATS

This paper proposes a **'Full-Spectrum approach'** to considerations, frameworks, and analytics for countering and preventing extremism and terrorism, in order to address critical gaps. We must expand the scope of consideration and analytics beyond Islamic or right-wing extremists and terrorists, and child soldiers, to better observe emerging and other threats. We need to map the ecosystem, and establish industry definitions, standards, and best practice methodologies. We have to develop youth-centric programs. Finally, we need to create a dedicated central coordinating body and industry forum to develop and implement recommendations, and enhance collaborations.

KEY BENEFITS

A Full-Spectrum approach will bring considerable benefits for the industry, including a more integrated and cohesive coordination between leaders, policy-makers, decision-makers, and practitioners. Improved strategies will enhance industry practices and reduce critical blind spots, ensuring that initiatives will be of operational utility and effectiveness. We will be able to respond faster to forming, emerging, adapting, and shifting threats. The approach will also enhance our ability to implement preventative measures



before violent thresholds are crossed. A more robust scope of domain awareness, analysis, and understanding will reduce extremist threats and unintended consequences. Refined and agreed upon definitions for classification and attribution will improve industry practice.

Call to Action

Urgent action is required to address the critical and dangerous gaps noted in this paper. It will require strong engagement from industry leaders, particularly government departments and state agencies – for appropriate funding, participation, and support – to develop and implement each Five Eyes members Full-Spectrum approach.

We need to act now, especially in light of recent events in the US, and the lack of consensus of what may or may not be considered an extremist or terrorist act or threat. A Full-Spectrum approach will help our industry keep pace with actual and potential extremist and terrorist threats in our world today and in the future.



INTRODUCTION

Domestic and Transnational Extremism and Terrorism are Becoming Increasingly Problematic to Fight

“The global extremism landscape has evolved significantly in the last decade. Policymakers must ensure they have a clear, strategic sense of direction to address the threats of today and those on the horizon.” – Tony Blair Institute for Global Change¹

Technological advancements have enabled extremists and terrorists to become more effective in influencing and manipulating vulnerable people to their causes. In contrast, many parts of the counter and preventative industry lag behind, with strategies and practices that are outdated, slow, and/or suffering from a narrow or limited scope. This has rendered them not fit-for-purpose for addressing the *complete* spectrum of threats to peace, stability, and the common security interests of Five Eyes members.

Pathways into radicalization, extremism, and terrorism are increasingly diffused, and the balance between the role of terrorist ideologies and broader socio-economic factors remains under-developed. The terrorism and extremism landscape is continually transforming, and policymakers and practitioners “cannot afford to be complacent when facing an ever-changing and ever-evolving threat”.²

Urgent action is now required to address critical and dangerous gaps in fighting extremist and terrorist threats. This paper by the 1st NAEF’s *Strategies Against Violent Extremism (SAVE)* team aims to show how a comprehensive Full-Spectrum approach will help industry leaders, policy-makers, decision-makers, practitioners, and other stakeholders to develop strategies and practices for more effectively analyzing, preventing, and countering extremism and terrorism.

In this paper, we:

- Assess the current situation and state-of-play in the industry
- Identify critical gaps and blind spots
- Propose a Full-Spectrum approach to considerations, frameworks, and analytics for countering and preventing extremist and terrorist threats

A Full-Spectrum approach will provide a stronger platform for Five Eyes engagement and partnerships to more effectively fight extremism and terrorism in the UK, US, Canada, Australia, and New Zealand, as well as globally.

Note: This paper is Five Eyes-centric because the SAVE team have combined experience in these domains, and it is based on their expert insights. However, observations and recommendations also apply to international partners in countering and preventing radicalization, extremism, and terrorism.



THE SITUATION

Increased Challenges and Complexity in Fighting Threats

Many leaders and practitioners in the counter and preventative extremism and terrorism industry today recognize that the fight against threats is becoming increasingly problematic, due to a number of inter-related factors.

Technological advancements in communications devices, messaging services, and platforms have made it easier for extremists, terrorists, radicals, and others to reach and manipulate larger numbers of vulnerable people to their causes. Threats have become more observable due to these technological advancements and to an ever-increasing global connectivity. There has also been an increase in complexity, due to the large number of communications platforms and technologies, many different categories of practitioners and intersecting fields of practice, and diverse range of threats and actors.

The range of stakeholders contributing to counter and prevention efforts has also compounded a common conflation between counter terrorism and community integration, thereby increasing the confusion associated with identifying successful practices. Youth extremism is also creating separate challenges for those working to prevent or counter extremism and terrorism.

Extremists and Terrorists Becoming More Effective

Domestic and transnational extremism and terrorism appear to be on the rise, with major incidents, recruitment, and proliferation becoming more widespread and more complex in the rapidly evolving digital world.

Extremism and terrorism hasn't fundamentally changed in the 21st century. There have always been extremists and terrorists. They still use similar tactics, techniques, and procedures, applied in ways that leverage modern systems for their means.

The major difference now is that extremism and terrorism are more observable, and can reach a wider audience much more easily. Fringe movements, once limited to local communities, can now become global through the use of technology. The most notable elements that extremists and terrorists have leveraged are the advancements and proliferation of communications technologies, social media channels, online forums, and gaming platforms. These allow them to better target, recruit, and retain members, while affecting influence upon sympathizers and detractors alike.

Figure 1 shows many of the devices and platforms that allow modern extremists and terrorists to communicate securely or broadcast widely. The numbers of subscribers, members, or users of the messaging, social media, online, and gaming platforms presents nefarious actors with **audiences of billions of people**. All of these advances have come to fruition in the last 30 years, with the majority in the last decade.



Figure 1: Communications Technologies and Platforms Available to Modern Extremists and Terrorists



Source: 1st NAEF, 2021

Industry Leaders Lagging Behind

In contrast, and despite some successes, international counter and prevention programming suffers from critical gaps and often a lack of coordination. Extremist activities are becoming increasingly problematic for Five Eyes members, and also more complex to assess completely, because existing criteria, systems, and processes are not fit-for-purpose for analyzing all major threats. This is exacerbated by social instability, increasing polarization, and the rapid emergence and growth of terrorist threats across the spectrum.

Industry practitioners have achieved mixed results with efforts to reach at-risk audiences, with success being framed by way of superficial metrics rather than meaningful interventions that can contribute to broader counter terrorism approaches. For example, a recent 1st NAEF-supported doctoral research study, on initiatives to reduce radicalization and extremism, found that many practitioners were measuring program success based on participant attendance rather than changes in their perception and outlook.³

There are also blind spots in understanding (identifying, acknowledging and addressing) new extremist and terrorist manifestations within a given space. Complete and effective domain awareness suffers from limitations, including scoping, grouping analysis, identification, and attribution of new or previously out-of-scope threats.

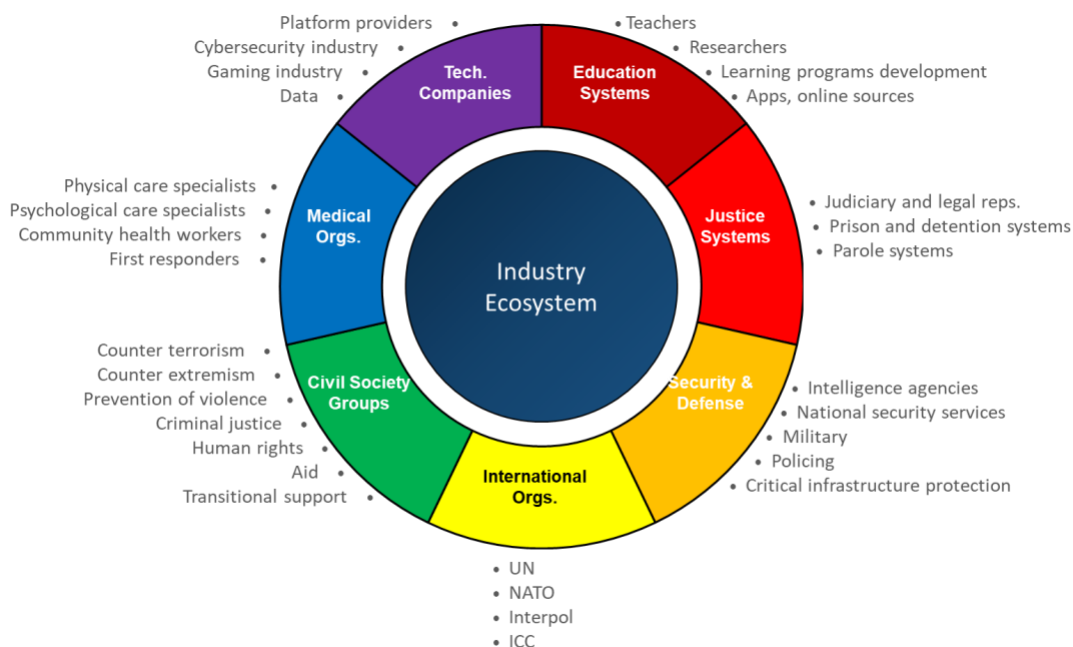


Multiple Categories of Practitioners and Intersecting Fields

The complexity of modern extremism and terrorism is also aggravated by the myriad of preventative and counter practitioners across a multitude of fields of practice. This industry architecture has not been clearly mapped and remains ambiguous.

Figure 2 is an illustrative and not exhaustive list of categories of practitioners and intersecting fields for the counter and preventative extremism and terrorism industry in the Five Eyes alliance:

Figure 2: Intersecting Fields and Specialties for Counter and Preventative Extremism and Terrorism Industry



Source: 1st NAEF, 2021

Many Categories of Threats

The complexity of threats is further exacerbated by the different categories of extremists and terrorists (active or potential) being applied by industry practitioners. Each Five Eyes member has its own unique threat actors, as well as shared transnational concerns, that manifest across a dynamic domain of threats.

The industry considers various types and categories of threat, with different thresholds, which are often classified based on different threat consideration perspectives – threat to public safety, threat to community cohesion, or threat to national interest. Until certain thresholds are crossed, various radical behaviors are considered potential and probable rather than actual threats – for example, a person can be radical, radical extremist, or extremist, but not yet have crossed the threshold to ‘terrorism’, i.e. becoming a national security threat.



Figure 3 is an illustrative and not exhaustive list of active, emerging, or historical forms of extremism present across the Five Eyes network:

Figure 3: Spectrum of Modern Extremist and Terrorist Threats



Source: 1st NAEF, 2021



We also need to focus more on the mixing of ideologies as pathways to extremism and terrorism, which is becoming increasingly prevalent. A new 'Mixed, Unstable, or Unclear Ideology' category was added in 2018 to the UK government's reporting on its Channel safeguarding program.⁴ This category describes cases in which the ideology the individual is presenting cannot easily be described as one of the existing categories, such as Islamist or right-wing extremism. This reflects how practitioners work to support individuals with wide-ranging and sometimes extensive vulnerabilities. For example, an individual may present a range of risks and vulnerabilities including, but not limited to, the risk of radicalization. In cases such as these, the individual may not have a coherent or single ideology, but may still pose a terrorism risk.

A whitepaper on 'memetic warfare' noted that law enforcement and intelligence agencies had begun to map how social media can rapidly radicalize individuals to commit acts of domestic terror. However, the agencies faced a challenge in understanding how social media empowers entirely new groups to self-organize radicalized militant cells and incite violence. The ability of extremist groups to self-organize created a new and poorly understood theater for emerging threats in the cyber domain.

Youth Extremism Creating Separate Challenges for the Industry

"Countries around the world are grappling with a surge in radicalization and violent extremism, which disproportionately affects young people." – UN Office on Drugs and Crime⁵

Children are under increased threat from being recruited and manipulated by extremists and terrorists. However, there are additional complications associated to youth extremism – i.e. how children and youth are vulnerable and currently affected – which raise the need for programs and initiatives that are specifically developed for children and youth, rather than simply repackaging adult-oriented frameworks and models. We also need to consider the unprecedented level of online engagement that exacerbates youth vulnerability to digital forms of extremist manipulations.

There is a potential source of conflict here, with the relatively new counter and preventative industry encroaching upon existing statutory functions to safeguard and protect children from a range of harmful behavior. Our efforts must synthesize with existing safeguarding functions.



THE PROBLEM

Dangerous and Critical Gaps in Fighting Extremism and Terrorism

Initiatives and programs suffer from critical gaps and blind spots that contribute greatly to our ability to effectively counter and prevent with extremist and terrorist threats. Many existing systems and processes are out-of-date – the extremism and terrorism landscape has evolved rapidly, but many practitioners have not managed to keep pace.

We face many challenges in countering and preventing extremism and terrorism across the Five Eyes today, particularly in regards to considerations, frameworks, and analytics:

Critical Gap 1 – Limited Scope of Consideration

There is an over-saturation, combined with a narrow or limited focus, in counter and prevention programming. Most efforts are still heavily focused on ‘traditional’ threats, specifically Islamic terrorism and right-wing extremism. For example, Tech Against Terrorism’s *Terrorist Content Application Platform (TCAP)* – which claims to be “the world’s largest database of verified terrorist content collected in real-time from verified terrorist channels on messaging platforms and apps”⁶ – only includes content created by the following designated terrorist groups in its initial scope:

- IS (including official provinces)
- Al-Qaeda (including official affiliates)
- Designated far-right terrorist organizations

The current narrow focus limits consideration of other rising or evolving threats. However, TCAP has recognized the narrow scope of its threat analytics and aims to expand updates in the future to include:⁷

- Expanding scope to include proscribed terrorist groups from other ideological strands
- Increasing the remit of Islamist and far-right terrorist groups in line with updated designations as well as our own, and external, ongoing analysis
- Including supporter-generated material as well as official centrally-communicated content

Political and academic research cycles contribute to this critical gap. Each new government has its own political interests and considerations, resulting in inconsistencies in focus of counter and preventative extremism and terrorism programs. However, radicalization and exploitation exists across the whole of society, not just those deemed most politically or socially expedient, or popular (i.e. the current spectrum of analysis). Anyone is vulnerable if extremists’ messaging aligns to their own identity group.

Critical Gap 2 – Narrow Spectrum

We’ve been focusing too long on *longitudinal* threat analysis, and we have missed how groups pose *latitudinal* threats.

National agencies, by nature of capacity and necessity, tend to have a wider spectrum of threat consideration than others within the umbrella of countering and preventing extremism and terrorism. Private organizations, academic institutions, think-tanks, and non-profits most often focus on a narrow scope of longitudinal threat analysis, i.e. how differently ideologically-motivated groups interact with one another and exist in “reciprocal” relationships. For example:



A. Increased right-wing extremism across western countries in response to rising Islamic extremism.

By focusing largely on these threats, we fail to address the aggregated threat environment and Full-Spectrum of manifestations, such as:

B. Increased left-wing extremism in response to rising right-wing extremism; and

C. Increased anarchist extremism in response to instabilities created, in part, by A. and B.

It is important to consider that not all manifestations will be traditionally organized, and that not all manifestations will engage in the same types of threat actions. These manifestations can pose different kinds of 'latitudinal' threats, falling broadly into three areas:

- i. *Public order threats:* Groups who engage in street fights or nuisance actions that impact on the orderly function of an area within a community.
- ii. *Community cohesion threats:* Groups or others whose actions cause inter/intra community tensions and damage stability of entire communities by fostering, inciting, or otherwise influencing destabilization or violent acts.
- iii. *Terrorist threats:* Groups or individuals who commit bombings, attacks against critical infrastructure, public beheadings, shooting rampages, or other similar violent actions that are committed for political, ideological, or mythological purposes, that result in direct impact on national interest.

Critical Gap 3 – Undefined Industry Architecture

The industry architecture is largely undefined, resulting in differences in practice between different practitioners, across the following areas:

- *Ecosystem:* There is no comprehensive mapping of practitioners working within the different intersections that make up the industry, meaning that the roles and responsibilities of any practitioner outside of national security and defense agencies are unclear at best and undefined at worst. The USAID and FHI 360's *CVE Reference Guide for Local Organizations* notes that the violent extremism ecosystem is complex, with different groups holding diverse interests and stakes in terms of counter and prevention programming.⁸
- *Definitions:* There is a lack of agreed upon or common industry definitions, terminology, and taxonomy across practitioners and intersecting fields of practice. There is no consensus when it comes to defining 'extremism' or 'terrorism'. Scholars, organizations and government agencies across the world have created more than 260 definitions of 'terrorism'. There is also no universal consensus regarding what exactly constitutes 'countering' or 'preventing' extremism, nor what forms these should take (McCants and Watts).⁹
- *Standards:* There are no industry standards for analytics, prevention strategies, or counter measures.
- *Measurement:* It is difficult to measure the performance or effectiveness of programs due to a lack of best practice Measurement & Evaluation programs. "A UN Special Rapporteur on the protection of human rights while countering terrorism concluded that "the lack of semantic and conceptual clarity that surrounds violent extremism remains an obstacle to any in-depth examination of the impact of strategies and policies to counter violent extremism on human rights as well as on their effectiveness in reducing the threat of terrorism".¹⁰



- **Critical Gap 4 – Lack of Best Practice Methodology**

There is a lack of industry best practice in methodologies and programing. The risk here, particularly in relation to international development efforts, is that the counter and preventative extremism industry is often seen as reinventing the wheel compared with long-standing counter-terrorism practitioners. Additionally, the profile of some organizations today is also more akin to activists who focus on specific variants of terrorism, to the detriment of developing data-driven methodologies and contributing to holistic threat assessments.

- **Critical Gap 5 – Speed**

"Technology is one of the strategic factors driving the increasing use of the Internet by terrorist organizations and their supporters for a wide range of purposes, including recruitment, financing, propaganda, training, incitement to commit acts of terrorism, and the gathering and dissemination of information for terrorist purposes." – UN Office on Drugs and Crime¹¹

Existing systems and processes for analyzing extremism and terrorism have not evolved or adapted with the speed of technological and communications advances leveraged by extremists and terrorists. Firstly, more and more nefarious actors have access to cell-phones, VPNs, encrypted communications, digital forums, and online platforms, making it easier for them to target and radicalize vulnerable people. Secondly, industry practitioners are finding it hard to keep abreast of forming and emerging threats that have a high probability to cross, or have already crossed, the threshold from radicalization to extremism or terrorism.

- **Critical Gap 6 – Difficulties Pertaining to Children and Youth**

Strategies to prevent or counter youth extremism are inappropriate for children and limited in scope. There two main issues to address:

- *Inappropriate programming:* The gaps in addressing youth extremism effectively are further aggravated by the focus of analytics and programs being primarily developed for adults. However, children differ from adults in many different ways, including differences in cognitive development, coping mechanisms, freedom, needs, emotional maturity, identity, worldviews, state intervention, and safeguarding requirements.
- *Limited scope:* Intersections relating to youth are becoming an increasing focal point for prevention and counter initiatives, but this focus has mostly only been applied to children in conflict and post-conflict areas - i.e. 'child soldiers'. The 1st NAEF has previously reported that we often fail to recognize the complete spectrum of children used and exploited by organized criminal groups, extremists, and ideological supremacists. This is especially so for children in domestic spaces – where if they were located in a conflict zone, under the same conditions they live now, they too would be considered 'child soldiers.'¹²

- **Critical Gap 7 – Lack of Industry Cohesion**

Finally, there is a lack of industry cohesion. There is no integrated approach, and poor communication or liaison, between industry leaders and practitioners, making it hard to coordinate counter and preventative extremism and terrorism efforts.

RECOMMENDATIONS

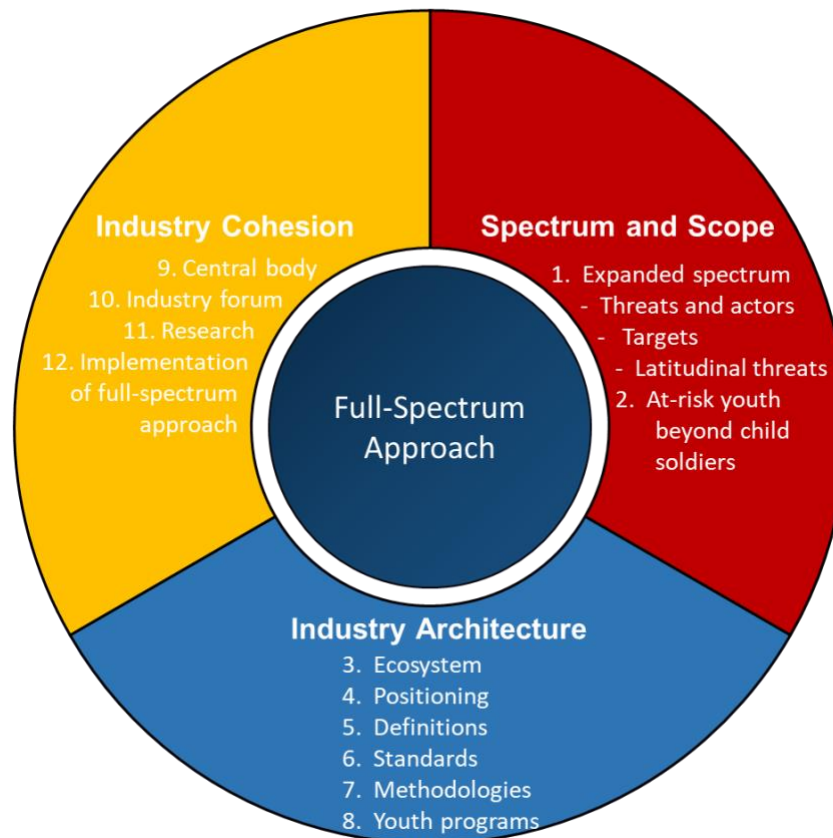


A Full-Spectrum Approach Will Address Critical Gaps and Blind Spots

We propose **the development and adoption of an industry-wide Full-Spectrum approach** to address critical gaps and blind spots noted in this paper. 'Full-Spectrum' is an umbrella term for a broader and more comprehensive approach, rather than an established industry framework or model. Our aim is to gradually and eventually make it the industry norm for extremism and terrorism considerations, frameworks, and analytics across the Five Eyes network.

Figure 4 highlights key objectives and recommendations of the proposed Full-Spectrum approach:

Figure 4: Key Elements of Full-Spectrum Approach to Counter and Preventative Extremism and Terrorism Programming



Source: 1st NAEF, 2021



The Full-Spectrum approach includes the following strategic objectives and key recommendations:

STRATEGIC OBJECTIVE: INCREASING THE SPECTRUM AND SCOPE OF THREAT ANALYTICS

Recommendation 1 – Increasing the spectrum of analytics beyond current over-saturated and limited scope

This will have three key areas of consideration:

- A. Expanding the range of threats actors across a broad spectrum, and also across new and emerging technologies and communications platforms. This increase in scope could include violent manifestations such as destruction of property, illegal or unregulated carrying of weapons, hate crimes, street fighting, riots, inciting and directing violence, assault, and participation in violent crime networks.
- B. Increasing the range of vulnerable people targeted for influence and manipulation by extremists, particularly: in-group/out-group members, those socially isolated and seeking to belong, those socially isolated and feeling victimized, those socially active in communities of repeated rejection, and those socially active in communities that demand group-think for association. We must also consider what conditions and scenarios are known to increase vulnerability and susceptibility.
- C. Adding latitudinal threat analysis to longitudinal threat analysis. This will provide for complete domain awareness of threats in and across each Five Eyes member state.

Recommendation 2 – Increasing the scope of youth extremism beyond ‘child soldiers’

New considerations and frameworks must fully reflect the reality of children targeted by extremists as they exist in different forms around the world today. Whilst our industry recognizes the concept of ‘child soldiers’ in conflict zones, we need to consider the Full-Spectrum, including the acknowledgement, identification, and protection of children recruited and manipulated by extremists in non-conflict or domestic spaces.

STRATEGIC OBJECTIVE: IMPROVING INDUSTRY ARCHITECTURE AND PROGRAMMING

Recommendation 3 – Mapping and documenting a common industry architecture (ecosystem).

This should include roles and responsibilities for all practitioners across intersecting prevention and counter fields.

Recommendation 4 – Developing an understanding of the positioning of counter and preventative extremism and terrorism

This should be with respect to counter terrorism and community integration, and also international development efforts.

Recommendation 5 – Developing and adopting commonly understood industry definitions

This should include an agreed taxonomy and glossary of key terms and definitions.

Recommendation 6 – Setting and implementing industry standards for common analytics and practice

This should be applied evenly across forming, emerging, evolving, shifting, and rising extremist and terrorist threats.



Recommendation 7 – Developing and establishing best practice methodologies

This will include developing and agreeing common measurement and evaluation programs.

Recommendation 8 – Developing more comprehensive youth-centric programs and methodologies

This will increase operational effectiveness in tackling child and youth extremism. The recommendation will take into account the differences between adult extremists and those children targeted and manipulated by extremists.

STRATEGIC OBJECTIVE: ENHANCING INDUSTRY COHESION AND COORDINATION

Recommendation 9 – Creating a central, collective body of thought leaders and industry experts

The main function of the body will be to coordinate prevention and counter extremism and terrorism programming.

Recommendation 10 – Establishing a dedicated industry forum

The key aim will be to improve networking, collaborations, and sharing of best practice for the Full-Spectrum approach.

Recommendation 11 – Investigating critical gaps and solutions development further

This should include gaining funding for detailed research looking at new and evolving extremist threats across the entire spectrum.

Recommendation 12 – Considering how to develop, introduce, and implement a Full-Spectrum methodology across the Five Eyes network

This will pertain to the monitoring, analysis, countering, and prevention of extremism and terrorism in and across these domains.

Key Benefits from the Approach

Our recommendations hold significant benefits for the industry, and also for the intelligence-sharing capability, across the Five Eyes and globally. The Five Eyes intelligence-sharing alliance and agreement is well-detailed and well-structured, with formalized definitions, structures, frameworks, and partnerships. Five Eyes members already benefit from the work done in the counter and preventative extremism and terrorism fields. They would receive greater benefits from formalized and agreed upon definitions, architecture, standards, methodologies, and collaborations, including:

- A more integrated and cohesive approach between industry leaders and practitioners
- A stronger platform for Five Eyes engagement and partnerships in more effectively fighting extremism
- Improved strategies in Five Eyes member countries and also UN/NATO member states to enhance practice and reduce critical blind spots
- A faster response to forming, emerging, adapting, and shifting extremist and terrorist threats
- An enhanced ability to implement preventative measures before extremism violence thresholds are crossed
- Reduced extremist threats and unintended consequences from increased scope of analytics and focus



A Full-Spectrum Approach to Countering and Preventing Extremist and Terrorist Threats

- Refined and new definitions for classification and attribution

Key Success Factors

Our success in developing and implementing a Full-Spectrum approach will be dependent on more industry leaders, policymakers, and practitioners joining our efforts and supporting our cause. We also require increased systemic support and funding for Full-Spectrum counter and prevention efforts.

Page | 17



CONCLUSION

Closing Thoughts

It is becoming increasingly problematic for agencies and practitioners to fight new and evolving extremist and terrorist threats across the Five Eyes member countries and globally. There are many critical gaps and blind spots that affect the industry and practices, and which need to be addressed.

The *Strategies Against Violent Extremism* team believes that a Full-Spectrum approach to considerations, frameworks, and analytics for counter and preventative extremism and terrorism programming is urgently required. It is imperative that we expand spectrum of analytics to better observe new, emerging, and evolving threats. Our industry also needs to develop and establish clear and commonly understood architecture, definitions, standards and best practice methodologies. We must establish youth-centric programs to more effectively address child and youth extremism. We also need a dedicated central coordinating body to develop and implement recommendations and enhance collaborations.

The proposed approach will bring considerable benefits for the counter and preventative extremism and terrorism industry across the Five Eyes network. There will be a more integrated approach between industry leaders and practitioners; improved strategies and programming; faster response to new and evolving threats; preventing extremism before a violence threshold is crossed; reducing extremist threats and unintended consequences; and refined and new definitions for classification and attribution.

Many of us working in this space recognize the need for urgent change and improvement. This paper is intended as a wake-up call, to alert industry leaders – those with deep pockets and influence – to critical gaps and blind spots. Together, we must develop and implement the changes necessary for our industry to keep pace with actual and potential extremist and terrorist threats in our world today and in the future.

Call to Action

A Full-Spectrum approach requires high-level buy-in and strong engagement from industry leaders, particularly Five Eyes government departments and state agencies, for appropriate state-level funding, partnerships, participation, and support. We look forward to discussing and collaborating with other industry leaders to pioneer 21st century solutions for a more secure and stable world.



ABOUT

About the Authors



Ian Bradbury is CEO of *the 1st NAEF*, and also heads its *Strategies Against Violent Extremism (SAVE)* program. He has an extensive 22-year career including military, national security, educational, and international roles. He has been a TEDx speaker on youth male victims of extremism, and is an accomplished leader in stability programming, including acting as a subject matter expert to the NATO Stability Policing Center of Excellence.

For more information: primary@1naef.com



Dr. Craig McCann is Director of *SPECTRUM Universal Ltd.*, a specialist consultancy providing services, tools, and expertise to prevent individuals from being drawn into terrorism. He was formerly a police officer in the Metropolitan Police Service in London for 14 years, including working in counter terrorism. Craig also writes, advises and lectures on the UK PREVENT strategy and on state responses to right-wing extremism.

For more information: <https://www.linkedin.com/company/s-p-e-c-t-r-u-m-universal-ltd>



Peta Lowe is Principal Consultant at *Phronesis Consulting & Training*, which provides assessment, consultancy, and training services to community, justice, and security sectors working to counter violent extremism. She was formerly Director of Countering Violent Extremism for Juvenile Justice in the NSW Department of Justice. Peta has over 15 years' experience working with young people involved with the justice system, and has worked with individuals, families and communities to address offending behaviors and criminogenic risks.

For more information: www.phronesisconsultingandtraining.com.au



Khalid Irshad is Strategy Director at *the 1st NAEF*. He has multi-sector experience across for-profit and non-profit organizations in Europe, the Middle East, and North America. Khalid specializes in developing decision support insights, business strategies, plans, and proposals to enhance corporate strategy, programming, concept development, and executive decision-making.

For more information: strategy@1naef.com

Contributors

We would like to thank Whitman Davis and Pauline Zerla for their contributions to this paper.

About the 1st NAEF and the SAVE Program



The 1st NAEF is an independent international 21st century non-profit NGO focused on developing modern and innovative solutions to address critical gaps in stability operations, peace support, and humanitarian aid to protect vulnerable populations.

The organization's **Strategies Against Violent Extremism (SAVE)** program provides advisory, research, and solutions focused on countering and preventing violent extremism.

For more information: <https://1naef.org> or <https://1naef.org/save>.



REFERENCES

- ¹ Tony Blair Institute for Global Change
2020: Challenges in Counter-Extremism
www.institute.global/policy/2020-challenges-counter-extremism
- ² Tony Blair Institute for Global Change
2020: Forward: Recalibrating the Response to Global Extremism
www.institute.global/policy/foreword-recalibrating-response-global-extremism
- ³ McConnell, Lisa: Colorado Technical University
2019 (PDF) Investigating Specific Strategies Required To Neutralize And Successfully Reduce Radicalization And Extremism
www.researchgate.net/publication/337099692_Global_Leaders_Speak_Investigating_Specific_Strategies_Required_To_Neutralize_And_Successfully_Reduce_Radicalization_And_Extremism
- ⁴ UK Home Office
2020: Individuals referred to and supported through the prevent program.
www.gov.uk/government/statistics/individuals-referred-to-and-supported-through-the-prevent-programme-april-2019-to-march-2020
- ⁵ United Nations Office on Drugs and Crime:
www.unodc.org/dohadeclaration/en/news/2020/07/guide-on-preventing-violent-extremism-through-sport.html
- ⁶ Terrorism Content Analytics Platform
www.terrorismanalytics.org/group-inclusion-policy
- ⁷ Terrorism Content Analytics Platform:
www.terrorismanalytics.org/group-inclusion-policy
- ⁸ USAID: CVE Reference Guide for Local Organizations:
www.cverefereceguide.org/stakeholder-engagement
- ⁹ United Nations Office on Drugs and Crime
www.unodc.org/e4j/en/terrorism/module-2/key-issues/preventing-and-countering-violent-extremism.html
- ¹⁰ (General Assembly, Human Rights Council report A/HRC/31/65, para. 55)
www.unodc.org/e4j/en/terrorism/module-2/key-issues/preventing-and-countering-violent-extremism.html
- ¹¹ United Nations Office on Drugs and Crime:
www.unodc.org/unodc/en/terrorism/news-and-events/use-of-the-internet.html
- ¹² Homeland Security Today:
www.hstoday.us/subject-matter-areas/counterterrorism/why-red-hand-day-2020-must-help-drive-better-understanding-and-protection-of-child-soldiers-today/