Heliyon 7 (2021) e07121

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

# Countering violent extremism using social media and preventing implementable strategies for Bangladesh

Sajid Amit [a], Lumbini Barua [a], Abdulla - Al Kafy [b,c,*,1]

[a] Center for Enterprise and Society, University of Liberal Arts Bangladesh (ULAB), Dhanmondi, Dhaka 1209, Bangladesh
[b] ICLEI South Asia, Rajshahi City Corporation, Rajshahi 6200, Bangladesh
[c] Department of Urban & Regional Planning, Rajshahi University of Engineering & Technology, Rajshahi 6203, Bangladesh

ARTICLE INFO

*Keywords:*
Social media
Violent extremism
Disruptive technology
Digital technology

ABSTRACT

Globally, more than 85% of youth use social media daily in the medium of Facebook, Youtube, Twitter, etc., which is more than 70% for Bangladesh. The young population of Bangladesh is rapidly embracing social media through the internet and afflicted with the malaise of countering violent extremism (CVE), often through Facebook. Given the increasing connectedness that the internet and social media offer, it is crucial that the fight against CVE shift to the digital space. Extremists are increasingly adopting novel ways and means based on technology to draw unsuspecting youth to their cause. It is essential to establish effective implementable strategies to stop the CVE activities using social media in Bangladesh. This study aims to identify existing initiatives globally in the space of disruptive online technologies that have yielded some success in preventing CVE. Various publications such as journal and news articles, TV news, and blogs have been used as data sources for this study. Also, fifteen expert interviews have been conducted to identify the most effective strategies for CVE in Bangladesh. Through the content analysis, the study highlights successful efforts and explores technology-based initiatives that can be deployed in Bangladesh to minimize the impact of VE activities through online technology. Finally, recommendations for strategies to restrict VE activities through technologies have been suggested that can be potentially implemented by the Bangladesh government by coordinating with international donor agencies and CVE practitioners. The research output recommends that Bangladesh and other less developed countries can concurrently deal with CVE by successfully using cutting-edge online/digital technologies.

## 1. Introduction

Violent assaults by individuals and groups labelled "extremist" have occurred in most countries, and violent extremism (VE) is now widely regarded as a significant threat to global peace and development (Patel and Koushik, 2017; Ambrozik, 2018). VE is a process by which an individual or a group comes to take up a violent form of action which directly linked to an extremist ideology that contests the established order at the political, social or cultural level (Heydemann, 2014; Frazer and Nünlist, 2015). In 2001, the world was given the most chilling reminder imaginable to VE's potency – the coordinated attacks on the Twin Towers in New York City. Since then, the threat has been gaining momentum through a series of attacks in countries across the globe. Today, VE is widely recognised as one of the most withering threats to peace and development at both national and global levels (Thiessen, 2019). This impedance gained further traction through a series of terrorist attacks in Europe, including suicide bombings and gun attacks in Paris, Brussels, Bastille, and Munich in 2015 and 2016 (Macnair and Frank, 2017; Patel and Koushik, 2017). With the realisation that VE, by many groups, is a coordinated and well-planned strategy rather than mere affiliation with random individual extremists, the concept of "Countering Violent Extremism (CVE)" was established as an official political jargon in 2015 (Frazer and Nünlist, 2015) and a popular term used by governments, academics, and NGOs to refer non-coercive attempts to reduce involvement in terrorism. CVE is universally recognised as activities designed to reduce the phenomenon of VE and provide sustainable counterterrorism plan and policies designed to enable them (Frazer and Nünlist, 2015).

Bangladesh is not an exception to encountering the daunting threats of VE and radicalisation. The country experienced a chapter of violence between 1999 to 2005 influenced by extremism from militant

* Corresponding author.
*E-mail address:* abdulla-al.kafy@localpathways.org (A.A. Kafy).
[1] Website: https://www.abdullaalkafy.xyz/.

https://doi.org/10.1016/j.heliyon.2021.e07121
Received 8 December 2020; Received in revised form 6 March 2021; Accepted 18 May 2021

organisations like Jamayat-ul-Mujahedin Bangladesh (JMB), Hizbut Tahrir, and violent extremist organisations associated with al Qaeda in the Indian subcontinent (Bashar, 2017; Husain, 2017). This upsurge in domestic terrorism inspired nationwide concern, most notably witnessed following a series of 63 coordinated bomb blasts throughout Bangladesh in 2005 by JMB. The current phase of VE in Bangladesh started in 2013, announcing its emergence through serial murders of a number of secular bloggers, liberal academics, LGBT activists, and religious or other minorities (BIPSS, 2017; CEP, 2019). The most prominent incident, the infamous "Holey Artisan Bakery Assault," occurred in 2016 and achieved global attention for the 22 dead at an upscale bakery in Dhaka (BIPSS, 2017; Ambrozik, 2018; Kundnani and Hayes, 2018).

In recent times, extremists have been looking into VE activities through the use of social networking sites, such as Facebook and Twitter, with additional inroads into YouTube – all of which are used for propaganda, recruitment, and fundraising (Alam, 2015; Waldman and Verga, 2016). Using social media as a weapon, through the internet, the extremists luring in people who are susceptible to their contents, recruiting individuals in their extremist groups and missions, and finally planning and executing terror attacks in different parts of the world (Gielen, 2017; Stewart, 2017). Countries including the United States, Spain, Russia, and the United Kingdom have discovered that the violent attacks they have faced were facilitated by extremists who had been radicalised online with the help of the internet and social media (Fernandez et al., 2018; Kundnani and Hayes, 2018). The perpetrators responsible for the horrifying 2019 Easter suicide bombing in Sri Lanka communicated and planned the attack through the internet and social media, as well (van der Vegt et al., 2019; Weine and Kansal, 2019).

From all appearances, the weaponization of the internet and social media by extremist groups is perceived as a significant concern as the internet and social media users are increasing every day. According to the Global Digital 2019 Report, the world is currently home to about 4.39 billion Internet users and 3.48 billion social media users (Idris, 2019). Realising the advantages of these mass-communication networks, extremist groups utilise them to instil and disseminate their agendas and ideologies towards people irrespective of countries, backgrounds, and other differences. Governments, non-governmental organisations, tech companies, and other global stakeholders are increasingly focusing on CVE efforts online under these circumstances. The social media platforms are also facing constant pressure from governments for augmenting their endeavors in combating the spread of VE online (Cleveland et al., 2020).

Correspondingly with the rest of the world, Bangladesh, with about 90 million Internet users (Hassan et al., 2020) and about 30 million social media users (Sayeed et al., 2020) are vulnerable to the influence of radicalisation online. International VE organisations like the Islamic State and their local disciples have already started exploiting this opportunity. Evidence of mass dissemination of extremist content and recruitment of individuals through the internet and social media channels are regularly coming to attention (CEP, 2018; Millar et al., 2018). Realising the imminent threat of VE online, the Bangladeshi government has announced zero-tolerance for terrorism and VE, and different government bodies and non-government stakeholders have been undertaking a diverse set of CVE initiatives to tackle the situation at hand. While it is clearly impossible and undesirable to either eliminate or survey the entire internet and social media landscape for VE recruitment activity, a potentially more productive approach need to be taken in using social media and the internet to support pro-social, anti-VE activities, which can be supported through offline and community-based awareness activities.

Very little research has addressed the role of social media in violent radicalisation. Although a large number of articles deal with terrorists' e-strategies and uses of the Internet and social media online for recruitment, there are very few empirical studies that describe the effective strategies to reduce them. In this context, the objective of this study is intended to identify effective CVE strategies for Bangladesh in minimising the VE activities induced by social media and the Internet. The strategies will be developed based on the experiences of the successful global online/offline/digital based CVE practices and analysing the current local interventions to identify what holds the most promise in Bangladesh's context. This research performed a content analysis of selected documents to fulfill the objective. The selected documents consist of the published journal and news articles, TV news, and blogs that considered existing initiatives globally and yielded some success in preventing and countering violent extremism (P/CVE) accelerated by social media technologies. Experts interviews also performed to identify the most effective strategies from the existing ones, which can reduce the VE activities in Bangladesh. Information obtained from content analysis and expert interviews, the paper highlights those successful efforts and explores technology-based initiatives deployed in Bangladesh. Finally, recommendations for strategies to deploy technologies in the CVE for Bangladesh have been suggested that can be potentially implemented by international donor agencies and P/CVE practitioners.

The paper is structured as follows: First, review the extant literature on the VE and CVE initiatives globally and locally. Section 3 then explains the research methods, including the data and its collection and analysis. Next, section 4 presents the results of this study while highlighting some implications, recommendations, and future research avenues in section 5. Finally, Concluding remarks are stated in section 6 based on the result and discussion sections.

## 2. Literature review

This section of the report presents a comprehensive review of the brief conceptualizations of terminologies, notions, and research findings collected from a broad range of literature relevant to CVE. The references include books, journal articles, reports, websites, newspaper articles, and blogs.

### 2.1. Violent extremism (VE)

The "VE" term is currently preferred for describing destructive actions or support for such actions undertaken by groups or individuals formally or informally affiliated with them, in the name of "extreme" political or religious ideals (Frazer and Nünlist, 2015; Cleveland et al., 2020). For years, VE did not have an internationally accepted or agreed-upon definition. Different governments and intergovernmental organizations have defined this concept in varying directions. U.S. Agency for International Development (USAID) defines VE as any action "advocating, engaging in, preparing, or otherwise supporting ideologically motivated or justified violence to further social, economic and political objectives" (USAID, 2011). UNESCO defines VE as "beliefs and actions of people who support or use violence to achieve ideological, religious or political goals" (UNESCO, 2016). The definition provided by the UN General Assembly in their plan of action to prevent VE suggests that VE is a diverse phenomenon that doesn't have any clear definition, and "it is neither new nor exclusive to any region, nationality or system of belief" (UN, 2016). While many experts urge that economic distress, political unrest, and poor educational systems contribute to inspiring terrorism among a nation's people, empirical evidence suggests otherwise (Berger, 2016). For instance, Benmelech & Klor in 2016 explains that foreign fighters' flow to IS determined that people from countries with higher levels of economic development, lower levels of inequality, and more highly developed political institutions are more likely to join IS. In their analysis, the correlation between the numbers of IS foreign fighters from a country has a positive correlation with the country's gross domestic product (GDP) per capita and with their human development index (HDI) score, a not so high correlation with unemployment, and a negative correlation with the economic inequality of the country. In a similar study focused solely on Palestine, there was also found a positive association between higher levels of education and higher standard of living with the tendency of becoming suicide bombers (Berrebi, 2003).

#### 2.1.1. Drivers of violent extremism

There are debates on what drives people towards VE activities. Researchers agree that multiple factors, rather than a single one, are

responsible. The Department of Foreign Affairs and Trade of the Australian Government has divided VE drivers into three levels: macro-level, meso-level, and micro-level drivers. The macro-level drivers include broad socio-economic-political trends of a nation and can also be recognised as push factors. The meso-level drivers can be influenced by the identity groups (e.g., particular groups united by shared ideologies based on religion or ethnicities) which can work as pull or enabling factors. Finally, the micro-level drivers are the individual factors or pull factors that are created from individual vulnerabilities, social isolation, person-to-person interaction or sensitivity to radical narratives (Government, 2017; Ahmed, 2019; Gordon and True, 2019).

Similar explanations of these three levels have been given by another team of researchers from the Open University, UK while highlighting the roots of the radicalisation process, albeit controversially. This team identified the micro-level drivers as the "individual roots" that relate to the self-affecting factors of the individual. The meso-level drivers are labeled as the "community roots" that represent the factors of group identity and social interaction with like-minded people. Finally, the macro-level drivers are recognised as the "global roots" of radicalisation, including the effects of globalisation process and influences of the government and society both at home country and foreign countries (Fernandez et al., 2018).

In a study commissioned by Morse, a European Union initiative in 2016, researchers have come up with a set of definitions of the "push factors" and "pull factors" of VE. In this study, the "push factors" have been interpreted as structural conditions responsible for fueling a sense of injustice in individuals. That sense eventually leads them towards accepting violent extremist ideas. On the other hand, the appeals of the ideas, persuasions preached by the extremist groups and different incentives promised by them have been identified as the "pull factors" (Morse, 2016).

UNDP's conceptual framework for preventing VE outlines eight drivers of radicalisation and resulting action of VE. The drivers are the role and impact of global politics, economic exclusion and limited opportunities for upward mobility, political exclusion and shrinking civic space, inequality, injustice, corruption and the violation of human rights, disenchantment with socio-economic and political systems, rejection of growing diversity in society, weak state capacity and failing security, changing global culture and banalisation of violence in media and entertainment (UNDP, 2016).

Besides these drivers, UNDP also suggests that individuals can get pulled into VE through a manipulation and socialisation process that involves media, educational institutions, family, religious and cultural institutions (UNDP, 2016). Elsewhere from a solely political aspect, USAID, in their research piece on drivers of VE, highlighted seven political drivers, including denial of fundamental political rights and civil liberties, harsh and brutal rules entailing gross violations of human rights, widespread corruption, and perceived impunity for well-connected elites, poorly governed and ungoverned areas, protracted, violent local conflicts, repressive regimes viewed as illegitimate and bankrupt, government's previous support to extremist groups to serve their political or strategic interests (USAID, 2011).

Considering and categorising these drivers of radicalisation and VE, Dr. Randy Borum suggested that four observable stages can be viewed as a model for explaining the process of ideological development of a VE. These four stages are context, comparison, attribution, and reaction. The first stage, the context indicates the social and economic deprivation of the individual. This sense of deprivation gives birth to the urge for comparison and results in the realisation of perceived inequality and resentment. After that, the individual progresses towards the third stage, which is attribution, and tries to blame people or a system for his/her adverse situation. Finally, in the last stage of reaction, the individual becomes dehumanised and aggressive (Borum, 2003).

#### 2.1.2. Online radicalization and descent to VE

Spreading radicalisation and VE online via the internet and social media is one of the most growing concerns of recent times. The internet has enabled easy availability of and unlimited access to content and rendered communication effortless through social media like Facebook, Twitter, YouTube, WhatsApp, and so on. At the same time, these characteristics of the internet have also equipped extremist individuals and organisations with the ability to mass disseminate their objectives and values without directly revealing their faces. Research shows the internet works as a channel for radicalisation in three of the following ways (Denoeux and Carter, 2009; Hassan et al., 2020):

i. **Illustrate and reinforce:** Use of the Internet in illustrating and reinforcing extremist ideologies via messages and narratives
ii. **Join and integrate:** Use of the Internet in creating an easy pathway for like-minded individuals to join together and form networks for integrating more people
iii. **Normalise unacceptable views and behavior:** Use of the Internet in creating a virtual echo chamber' of extreme views and ideas through which unacceptable behaviors become normalised

A study by UNESCO delivers similar findings by stating that social media channels are used for creating interactive platforms, disseminating violent content, identifying potential participants, producing false information, fostering one-to-one dialogue, and even for forming offline ties with individuals with the aim of recruitment (Alava et al., 2017).

According to Davies et al., a single item promoting extremist propaganda will never guarantee the radicalisation stimulation towards an individual's VE. Usually, radicalisation happens through people getting submerged in extremist content and ideologies for a long duration (Davies et al., 2016). This occurs quite easily due to the unique feature of social media, which customises a user's feeds with content appealing to their interests and connects them with like-minded individuals. Such "echo chambers" enable heavy exposure to a consistent barrage of extremist ideas and thus make it conducive to radicalisation – and in the long run, it helps them justify their violent behaviors (Mleagrou-Hitchens and Kaderbhai, 2017).

### 2.2. Countering violent extremism (CVE)

The concept of CVE was introduced for the first time after the extremist attacks in Madrid and London in 2014 (Frazer and Nünlist, 2015). Till this date, no standalone and universally accepted definition of CVE had been established. According to Ms. Humera Khan, CVE is the "use of non-coercive means to dissuade individuals or groups from mobilising towards violence and to mitigate recruitment, support, facilitation or engagement in ideologically motivated terrorism by non-state actors in furtherance of political objectives" (Khan, 2015).

The European Union (EU) claims that CVE ``constitutes all actions that strengthen the resilience of individuals and communities to the appeal of radicalisation and extremism" (EU, 2015). On a more comprehensive note, the National Counter Terrorism Centre of the United States views CVE as "programs and policies intended both to prevent individuals and groups from radicalising and mobilising to commit violence and to disengage individuals and groups who are planning to commit, or who have already engaged in extremist violence" (Elshimi, 2017).

Therefore, the conceptualisation of CVE circumvents a broad area that spans from preventing people from absorbing extremist values to impeding their active participation in violent acts. According to a number

of researchers, ambiguity regarding the concept of CVE among different nations and organisations leads to discrepancy in designing, delivering, coordinating, and evaluating CVE interventions across nations (Lakhani, 2012; Berger, 2016; Elshimi, 2017). Moreover, a vague realisation of CVE parameters poses challenges in CVE research; due to this, the policy and practice in this area lack a robust knowledge-based platform (Morse, 2016).

#### 2.2.1. CVE online

CVE online can be delineated as a broad field. This field may include different sets of actions or programs, and those programs can be divided into different typologies considering different aspects. Online CVE programs are most commonly split into two categories: positive and negative (Hussain and Saltman, 2014). Positive measures include strategies that "seek to challenge extremist narratives and propaganda by producing counter-content." Negative measures contain strategies that are intended to "block, filter, take-down or censor extremist content."

On the other hand, Saltman and Russell (2014) put forward a typology that divides CVE programs into three categories such as negative measure (blocking, censoring, filtering, or removing Internet content), positive measure (counter-messaging, which may be specific or general) and monitoring (identifying and analysing extremist contents) (Saltman and Russell, 2014).

This typology contains a component of "monitoring" in addition to those labeled under positive and negative measures. In this typology, 'monitoring' involves leaving the extremist contents uncensored while analysing them to provide assistance to the counter-extremism interventions (Saltman and Russell, 2014). Meanwhile, solely focusing on the negative CVE measures online, Denoeux & Carter divided the most commonly utilised strategies into three categories: removing extremist contents from the web, controlling and filtering the information exchanges and users' access, and hiding the radical content through manipulating the search engine results (Denoeux and Carter, 2009).

Another interesting classification of online CVE is advanced by Briggs and Feve (2013) in which they described the whole set of activities as a 'Counter Messaging Spectrum'. This spectrum includes government strategic communications to disseminate a positive message about government actions, alternative narratives to address extremist narratives by affirming social values, and counter-narratives to deconstruct extremist messaging. In this typology, the government is held responsible solely for strategic communications, and the responsibilities of counter-narrative-related activities fall entirely on civil society. Both of them are accountable for promoting alternative narratives (Briggs and Feve, 2013).

#### 2.2.2. Disruptive online technologies for CVE

Professor Clayton M. Christensen, a renowned academician from Harvard Business School, first used the terms "disruptive technology" and "disruptive innovations" in his book "The Innovator's Dilemma," published in 1997. According to him, disruptive innovations are unique and new innovations that are usually simpler than the previous ones and are initially more valued to an emerging market rather than to the mainstream. However, disruptive technologies are intended to replace existing technologies and approaches that are already established and thus bring revolution while creating an entirely new industry (Christenson, 1997; Meleagrou-Hitchens and Kaderbhai, 2017).

However, from a wider viewpoint, disruption can be defined as an outcome that can be measured based on both process and results. For a new technology or process to be considered as a disruptive one, it has to fulfill any of the following criteria (Millar et al., 2018):

i. **Cost:** Available at a cheaper cost than the older ones
ii. **Quality:** Be of better quality than the older ones
iii. **Customers:** Make notable changes in customer preferences
iv. **Regulation:** Be appropriate according to the new laws or regulations
v. **Resources:** Can be acquired using resources that are readily available

Therefore, in CVE, innovative technologies or processes that significantly reduce the appeal of the previously deployed ones can be recognised as disruptive technologies. With the increasing use of the internet, social media channels, different computer science technologies like artificial intelligence, machine learning, digital apps, and many others, a number of new and innovative technologies have been introduced in the field of CVE that are more effective considering from the perspectives of cost, impact and audience reach.

### 2.3. Existing online-based CVE research and interventions

According to Berger, the current CVE interventions are mostly chasing two goals without realising the distinction between them. One of the goals is "disengagement", which seeks to prevent people from participating in violent extremist movements. The other goal is "de-radicalisation/counter-radicalisation," which seeks to dis-engage people from taking on extremist ideologies (Berger, 2016). He also claims that disengaging the people who have been targeted by the extremist groups already is a more practical and accomplishable goal for CVE rather than de-radicalisation. As a rationale for such a statement, he claimed that, by ignoring the approaches that are intended to prevent extremism or radicalisation, CVE could gain a narrow focus solely focusing on disrupting the radical or violent activities and extremist recruitment process (Berger, 2016). However, there is no scope for ignoring the PVE[2] approaches as CVE is useful only for tackling the problem's outcomes while PVE strategies can uproot the problem itself.

In a review of six online CVE programs (Against VE; Exit White Power; Think Again, Turn away; Muflehun; Don't be a Puppet; and Open letter to our sons and daughters in Syria and Iraq) implemented mainly in western countries, including Australia, Canada and the United States, researchers concluded that the interventions had barely sufficient focus on the contextual factors. That implies, the online CVE interventions mostly adopted a slender approach in conceptualising the programs and targeted specific ideology or specific VE groups only. The actual roots of the problem in hand, the contributing factors of radicalisation, were hardly considered. It was also criticised that none of the interventions integrated social psychological aspects like identity, recognition, history, conspiracy, etc., responsible for radicalising individuals in many cases. Lastly, the reviewed programs lacked suggestions for replacing the so-called "benefits" of extremism (Davies et al., 2016).

A trend identified among individual governments' online CVE approaches is to restrict extremist content on the internet. This approach has been criticised by several researchers, media observers, and terrorism analysts, pointing out several limitations (Davies et al., 2016). The most major limitation suggested by the experts is that if one content or site is blocked, it will likely pop up on some other site (Macnair and Frank, 2017). The other limitations are that these are actually arduous as well as expensive processes; and, last but not least, there may not be a clear understanding about what exactly can be labeled as "extremist content" among certain groups (Davies et al., 2016). According to Briggs and Feve (2013), only a small portion of the extremist content can be marked as illegal, and thus the dilemma remains as the content promulgating extremist ideologies do not necessarily need to be illegal (Briggs and Feve, 2013).

Stevens and Neumann (2009) also argue that removing radicalised contents is not practical, claiming that in a liberal democratic context, the social and political costs caused by this approach would surpass the

[1] PVE can be interpreted as a broad spectrum of strategies that deal with the auxiliary factors of radicalization and violent extremism with the aim to prevent radicalization from ever occurring and thus involve a long term goal to tackle violent extremism.

benefits yielded. Here, the term "social and political costs" may imply that a fair number of legally expressed social or political opinions can be affected as well (Stevens and Neumann, 2009). Stevens and Neumann further urge that any online radicalisation countering strategy's core objective should be to create an environment where production and sharing of radical content become unacceptable. Based on such view they presented an alternative solution which suggests raising awareness among the people against violent and hateful content on the internet and prosecuting a number of representative guilty individuals to set an example of appropriate boundaries (Stevens and Neumann, 2009).

On the other hand, plenty of evidence proves the success and utility of blocking and suspending extremist content or other online activities. They suggest that the suspension of extremist sites or extremist groups' social media accounts and even suppressing the shared extremist contents diminishes followers and limits the frequency of content sharing to some extent (Berger, 2016). However, an important concern remains about the suppression of freedom of speech due to restricting extremist messages (ODIHR, 2014).

One of the most commonly deployed online CVE interventions is counter-narratives or counter-messaging (Briggs and Feve, 2013). While a fair number of analytical studies acknowledge counter-narratives as a significant CVE effort (Ashour, 2010), debates exist about the usefulness of this strategy, asserting that the potential adverse effects of counter-narrative campaigns supersede their expected rewards (Gielen, 2017; Weine et al., 2017). Evaluating three counter-narrative initiatives by the Danish government, the Danish Institute for International Studies disclosed that there is a lack of evidence proving the minimising effect of counter-narratives on violent extremism or radicalisation. They explain that the counter-narratives, which are reactive or confrontational in nature engender the risks of recognising or ridiculing the extremist messages in reality and thus get rejected by the target audiences (Mandaville and Nozell, 2017; Mirchandani, 2017).

On the contrary, another set of researchers expressed different findings after reviewing three online counter-narrative campaigns named *Average Mohamed* targeting Somalia youth, *ExistUSA* targeting far-right extremist groups, and *Harakut-ut-Taleem* targeting Taliban extremist narratives promoted in Pakistan. They conclude that sharing counter-narratives online can foster conversations online, antagonistic or otherwise, and provide a better understanding of the target audiences' reactions towards the counter-messages. The researchers further assert that if these conversations are sustained, both already radicalised people and at-risk individuals get exposure to alternative viewpoints that can insert a "seed of doubt" in their minds (Silverman et al., 2016). However, according to Berger (2016), the absence of an internationally-accepted ideology that can be an alternative to the extremist ones may create confusion and obstacles while adopting this approach (Berger, 2016). In such contexts, experts suggest that when countering extremist messages are not sufficient to tackle radicalisation or extremism, and it has to be complemented by creating positive alternative messages for the people who are predicted to fall victim (Berger, 2016). The Center for Strategic & International Studies conducted an online survey on CVE in the U.S., U.K., France, India, China, Turkey, Egypt and Indonesia covering 8000 people. When asked about the imagery they consider more effective in counter messaging campaigns, 47.0% of the respondents claimed that positive messages explaining the benefits of religious peace and harmony work best. Only 38.0% of the respondents rooted for displaying the violence caused by the extremists to work effectively. Such findings from the survey indicate that there may be a common perception among several people that alternative messaging has significant potential in countering extremist ideas (Green and Proctor, 2016). However, no empirical evidence have been generated to claim this perception as truth.

As social media channels are being widely used for sharing extremist content and recruiting among extremist groups, more and more agencies and governments are increasingly focusing their CVE interventions on social media as well. A research report (Waldman and Verga, 2016) focusing on CVE interventions and strategies deployed in social media has categorized the reviewed CVE interventions into two groups: (a) what appears not to work and (b) what holds promise. According to this review, taking down VE content, suspending accounts, analysing geo-spatial data for tracking extremists' locations, denouncing specific communities, and government-led counter messaging interventions are proven to be less than useful. However, social media monitoring, social network analysis, sponsoring evidence-based counter-narratives, pairing CVE with face-to-face interventions, developing alternative resources, enhancing Internet literacy, and strategic government messaging are claimed to hold promise in this field (Waldman and Verga, 2016).

### 2.4. CVE scenario in Bangladesh

Research indicates that there is a perception among the people of Bangladesh which recognises poverty as a major source of radicalisation and violent extremism (Bashar, 2017). In addition, there used to be a particular perception existing in the country associating madrasahs with militancy most commonly (Idris, 2019). However, the infamous Holey Artisan Bakery incident on July 1, 2016 depicts a different scenario. Among the five militants involved in this terrorist attack, two were undergraduates, and one was a college student, and all three of them were from affluent families with top English medium school background (Bashar, 2017; Hassan et al., 2020). In addition, a recent study conducted by the Anti-Terrorism Unit of Bangladesh reveals that most of the individuals involved in extremist activities come from a general education background rather than coming from a madrasah background. Among 250 militants surveyed for this study, about 56.0% respondents were from general education background and only 22.0% had madrasah education. The other 22.0% were either from English-medium background or uneducated. The study further asserts that the militants belonged to different socio-economic backgrounds (The_Daily_Star, 2019).

The government-led CVE approaches in Bangladesh are predominantly kinetic in nature which means that the existing strategies follow a counterterrorism (CT) approach through military solutions and police interdictions (Ahmed, 2019; The_Daily_Star, 2019). In operational CT cases through intelligence-led operations, Bangladesh has a number of success stories (The_Daily_Star, 2019). However, in cases of adopting a holistic measure for CVE which includes non-coercive methods, Bangladesh faces a significant number of limitations.

Along with many other countries around the world, Bangladesh faces the imminent threat of the spread of radicalisation and VE via the internet and social media (Alam, 2015). A survey among 250 arrested militants revealed that about 82.0% of them were radicalised via social media (Corraya, 2017). Despite such circumstances, research suggests that Bangladesh is yet to establish a fixed and strong online monitoring mechanism for disrupting the dissemination of extremist ideologies through the internet and social media. Moreover, appropriate hardware and software, institutional strength, technical expertise, and last but not least, policy issues for countering violent extremism online are absent (Alam, 2015; Bashar, 2017; Husain, 2017; Gordon and True, 2019; Hassan et al., 2020).

In conclusion, it should be acknowledged that with the increasing menace of VE globally, in-depth research and counter-strategies are gaining greater momentum every day. However, a number of gaps still remain in the existing literature. From a geographical perspective, the global agenda regarding CVE scarcely has covered Asian contexts and experiences (Klein, 2017). There is also a need for longitudinal studies drawn on extensive data gathered from the field for evaluating the potentialities and impact of the CVE initiatives. Particularly in Bangladesh's case, there is an absence of empirical research on appropriate CVE strategies and evaluation of existing ones. In this context, mapping of prospective online CVE strategies suitable for Bangladesh is needed. Also, identifying successful worldwide online interventions is needed for implementing CVE strategies in Bangladesh.

**Table 1.** Overview of data collection sources.

| Data Source type | No. of documents | Collection sites | Searching Keyword |
|---|---|---|---|
| Journal Articles | 48 | Google Scholar | Impact of social media/internet on VE activities, strategies to reduce the VE using social media, and successful global strategies for controlling CVE. |
| Newspaper articles | 23 | Google Search | |
| Reports | 14 | Google Search | |
| Blogs | 19 | Google Search | |
| Video Clips | 8 | Facebook and Youtube | VE incidents |

## 3. Methodology

### 3.1. Research setting

This study has a global setting, so it is not focused on any particular region. It considers events, incidences, and decisions associated with CVE activities around the world. This study is explorative with a qualitative approach. The data collection focuses on capturing the state of the CVE scenario influenced by social media based on secondary data sources, which are widely used for high-quality research. Indeed, secondary data is perhaps more appropriate for this study because first-hand data could not provide comprehensive knowledge about the impact of disruptive technology on CVE. Secondary data has been widely used in a range of disciplines, including strategic orientation (Shortell and Zajac, 1990), microfinancing (Cobb et al., 2016), and policy establishment (Lichtenberger et al., 2014; Stewart, 2017), and it has several benefits for academic studies (Houston et al., 2006). It shows the real decisions being made by real decision-makers, having been collected in a less obstructive manner and not influenced by the biases of self-reporting. The biases related to the vital informant sampling approach can therefore be avoided. Recent studies based on online comments to a newspaper article present a vivid exemplification of the importance of such data for studies (Cheng and Foley, 2018).

### 3.2. Data collection

The main data sources comprise newspaper and popular press articles, blog posts, published journal articles, and video clips. Through a comprehensive search, we collected as much information as possible about social media impacts on CVE activities. When searching for relevant articles, we used the keywords shown in Table 1. We only included documents written in English that clearly discuss social media technology and CVE relationship. The searches took place during July and August of 2020. Whenever we found an appropriate document, we added its title and a web link to a spreadsheet. After completing the collection process, we sorted the documents listed in the spreadsheet to see if any had been recorded twice. We found several such documents, so duplicates were removed from the list. We do not claim to cover all the relevant documents available on the internet. Still, we feel that our list is comprehensive enough to provide an insightful academic contribution about social media impact on VE activities and effective recommendations to minimize it. The final body of documents comprised 104 written documents and 8 videos, with the latter being viewed carefully and their main information being written down. For implementing the appropriate online-based CVE strategies in Bangladesh, information collected worldwide was validated and further enriched from 15 in-depth interviews with experts (including academics, activists, journalists, and researchers) in this field (Annex 01).

### 3.3. Data analysis

All documents were downloaded as PDFs and saved in a temporary folder. Subsequently, these were combined into a single PDF document that was 894 pages long. We applied content analysis

and organized the diverse data, including coding information, into different categories (Neuendorf & Kumar, 2015; Soldatenko and Backer, 2019). Content analysis can contribute a new depth of understanding for a phenomenon that has received limited attention (Vaismoradi et al., 2016). The combined document was uploaded to Qualitative Data Analysis (QDA) Miner Lite, an effective qualitative data analysis program. A free basic version was used, which is sufficient for coding and data analysis purposes. We used a range of preselected codes and additional codes through open coding. The preselected codes included worldwide CVE interventions, apps to reduce it, and effective strategies. We read each document line by line and coded it accordingly. After completing the iterative coding process, we merged several codes into one to reduce the number of coding categories to a more reasonable level. Once the coding process was completed, we extracted the coded texts into Excel files and synthesized the findings for implementable online-based strategies to minimize the CVE effect. The results of this study are described briefly in the following section.

## 4. Result

This section portrays the global landscape of online-based/digital CVE interventions thematically and summarizes them (Table 2), including innovative ideas, and identifies ones that have brought about disruption in technology-based CVE strategies deemed successful by the experts. This section also depicts successful intervention stories, deployment methods, success rates, and significant reviews provided by experts in this area.

### 4.1. Successful online-based digital CVE strategies by category

#### 4.1.1. Redirect method (RM)

The RM is one of the highlighted online CVE interventions of the present time. This method targets audience members who actively look for IS content and redirect them towards curated YouTube videos disproving extremist ideologies or themes. This is a joint initiative of the partnership among Jigsaw, a Google technology incubator, Moonshot CVE, a UK based startup, Quantum Communications, a policy and strategic communications advisory firm, and a group of researchers (Table 2). The RM campaign launched its pilot project in 2015. From the campaign's brochure, "The Redirect Method: A Blueprint for Bypassing Extremism", a clear overview of their deployed strategy can be obtained. Firstly, through extensive research, interviewing IS defectors, and mapping major IS narratives, they identified 5 recruitment narratives used by IS. They considered those under the following categories:

i. **Good Governance**: Showcasing their bureaucratic structure and implementation of sharia law.
ii. **Military might**: Portraying themselves as an unstoppable force destined to achieve victory over their enemies
iii. **Religious legitimacy**: Depicting their own interpretation of Islam as the only correct one
iv. **Call to Jihad**: Calling out individuals to do their part in attacking the enemies in the name of IS and rise as heroes
v. **Victimhood of the umma**[2]: Portraying a scenario where the rest of the world is subjugating Muslims around the world

[2] 'The Umma' is expression used to refer to an imagined global community of Muslims.

**Table 2.** Summary table of the major CVE interventions globally.

| CVE Intervention | Pros | Cons | Programmatic lessons |
|---|---|---|---|
| Redirect Method | • Utilises empirical evidences<br>• Prevents the possible echo chamber from forming<br>• Shares alternative narratives rather than counter-narratives<br>• Reaches the target audiences simply using targeted advertising techniques<br>• Easily replicable by other companies<br>• Identifies the at-risk individuals | • Doesn't remove any extremist contents from the web leaving scopes for those to be found anyway<br>• Solely focused on IS, ignoring other sorts of extremism<br>• Lacks provision for direct human interaction | • This approach can effectively hinder echo chambers' creation in social media without necessarily violating freedom of speech. The drawback regarding the persistence of extremist contents on the web can be addressed by creating a database of the extremist contents for investigation by the suitable authorities<br>• A follow-up intervention needs to be included in the process for facilitating the at-risk individuals with human interaction and counseling |
| eGLYPH Technology | • Prevents the once removed contents from resurfacing in the web<br>• Carries out thorough research for identifying generally used extremism associated keywords<br>• Maintains a database of hashes which is shareable with the other companies working for the same agenda | • Separating extremist contents from permissible public opinions can be troublesome | • The hashing technology can successfully solve the predicament caused by the resurfacing of the contents after removing. The issue of identifying extremist contents from the legitimate public opinions, a whitelist can be developed with the help of experts. Moreover, every content can be flagged down first and be removed only after being reviewed by a team of human specialists |
| AI Technology | • Identifies and removes extremist contents fast and accurately<br>• Can handle an enormous amount of data<br>• Shareable | • AI technology can always make false identification which may hinder people's freedom of expressing political and social grievance | • The impediments of using AI technology can also be solved quite effectively using the same procedures mentioned in the eGLYPH technology |

Secondly, they created a playlist of 116 videos from YouTube, either in English or Arabic. While curating these YouTube videos to debunk the extremist messages, they carefully selected those that offer credible and authentic counter arguments using:

i. Citizen journalism and documentary footage depicting IS's brutality towards civilians and unsuccessful governance efforts
ii. Religious debate featuring well known religious figures disproving IS's religious legitimacy
iii. IS defectors testimonies revealing the flaws and hypocrisies of IS

Finally, they placed the playlist alongside the results for the predetermined keywords and phrases that the potential IS recruits search for. Thus, they were re-routed to the curated video playlist, undermining the echo chamber walls (D'Onfro, 2016). The counter-narrative videos reached the potential IS disciples by deploying this strategy, just like any other targeted advertising campaign reaches prospective customers (Mirchandani, 2017; Patel and Koushik, 2017).

Although measuring the success of a CVE intervention in dissuading IS followers or recruits is not that simple, Jigsaw claims to find that the campaign at least succeeded to grab the searcher's attention (Green and Proctor, 2016). Throughout its pilot phase of 8 weeks, the RM campaign reached about 320,906 individuals and successfully led them to watch a total of about half a million minutes of videos (Lichtenberger et al., 2014). The most effective or popular ones received as much as 8 min and 20 s average viewing time. The Click-Through-Rate (CTR)[3] was 76% higher for the English ads and 79% higher for the Arabic ads than other ads against similar keywords (Lichtenberger et al., 2014).

The RM has attracted much attention from different relevant sectors and has received considerable acclaim. Charlie Winter, an associate fellow at the International Center for Counter-Terrorism at The Hague, expressed his high optimism about the overall campaign highlighting that the RM uses empirical evidence for countering the extremist messages (D'Onfro, 2016).

However, some experts predict that if an individual is looking for extremist content, they might still be determined to find those contents even if they are redirected (Klor and Benmelech, 2016). Ms. Humera Khan, the executive director of the Islamic deradicalisation group called "Muflehun" pointed out that this is only the first step in achieving the goal. Even if the campaign succeeds in making people watch the curated videos, influencing them to come back and watch other similar and new videos could pose challenges (Green and Proctor, 2016). Another criticism of this campaign can be the fact that this is solely focused on the IS, their narratives, and recruits, leaving all other kinds of extremism like white supremacy, far-right extremism, or religious extremism from the followers of other religions than Islam. Nevertheless, Ms. Khan acknowledges that the Redirect method is indeed a "good piece of solution", although not a fully comprehensive one. She stresses that for any PVE/CVE intervention to be successful, the element of human interaction and support from the community is a must. Similar observations can be found from other sources as well. After hooking up the individuals to the curated playlist, the next step can be including human interactions like therapeutic sessions or resources and online counseling to steer them further away from extremism (Kruse, 2016).

Yasmin Green, the director of research and development for Jigsaw, claimed to acknowledge these issues and declared that the campaign has plans to partner with a third-party to follow-up with the people who would like or comment on any of the curated videos and will assist and guide them through the process of deradicalisation (D'Onfro, 2016). In case of addressing other sorts of extremisms, an initiative has already

[3] CTR (click-through rate): A performance metric expressed in percentages that measures the number of times an ad is clicked versus the number of times it has been viewed. https://www.oberlo.com/ecommerce-wiki/click-through-rate-ctr.

been announced to replicate the Redirect Method to counter white supremacy and (other?) jihadist activities online. It will be carried out by the partnership among Moonshot CVE, the Anti-Defamation League, and the Gen Next Foundation in the US. However, there is still a need for further efforts from relevant organisations to counter the different VE arrays being promoted online.

#### 4.1.2. The eGLYPH technology

"eGLYPH" is a robust multimedia-based "hashing algorithm technology" developed by Professor Hany Farid, Chair of the Computer Science Department at Dartmouth College, Hanover, New Hampshire, and Senior Advisor to the Counter Extremism Project (CEP). Professor Farid presented research to the European Parliament's Special Committee on Terrorism (TERR) on April 24, 2018, sharing findings on IS and other extremist videos on YouTube, the duration they stay online, and views generated. From his research, it was discovered that between March 8 and April 18, 2018, a six-week period:

i. About 942 IS videos were uploaded to YouTube
ii. Those 942 videos generated 12 views each on average with a total of 134644 views
iii. Those videos were uploaded by 157 different YouTube accounts and some of those accounts uploaded as many as 70 videos prior to being removed by YouTube or deleted by the user.
iv. About 91% of the videos were uploaded more than once and remained in the web for a fair amount of time

These findings reveal that despite the triumph of YouTube in taking down extremist videos uploaded; those removed contents are finding ways to repeatedly resurface again and remaining online while attracting more viewers (Table 2).

To tackle this threat, Dr. Farid put forward eGLYPH as a viable technological solution that he claimed to have the potential to prevent extremist contents or affiliated accounts from resurfacing again. eGLYPH uses a "hashing" technology to assign a unique fingerprint or digital signature called "hash" to different contents like images, audios, and videos that have already been identified and flagged as extremist contents and automatically removes any versions of those from the social networks and websites. Furthermore, it automatically deletes the customised versions of those extremist contents from the web as soon as they are uploaded (Macnair and Frank, 2017; Macdonald, 2018).

According to CEP, eGLYPH can be deployed in the following two ways (CEP, 2018):

a) Deploying eGLYPH on the Internet and social media platforms for detecting and flagging contents to remove
b) Attaching eGLYPH to a web crawler for continuously searching through the internet for content and sending notices to the sharing companies for taking down the flagged contents

CEP created a database of hashes composed of 229 full-length IS videos, clips, and other visual propaganda. They also identified 183 keywords which are associated with IS content, provinces, media outlets, and propagandists or demonstrate sympathies towards IS. eGLYPH has a web crawler attached with it that is responsible for conducting searches using YouTube's API (Application Programming Interface) every 20 min throughout the day looking for audio or video or image uploads that match with the hashes or keywords of the database. Therefore, as soon as any content's signature or hash is recognised and added to the database, it becomes virtually impossible to re-upload that content ever again to any web platform.

The eGLYPH technology was developed using the model of the PhotoDNA algorithm, which was created by Dr. Farid targeted to prevent child pornography. PhotoDNA works through recognising images even in the case they are altered or customised, but eGLYPH works on a more advanced level as it can also process and analyse audio and video files making it more impactful in countering all sorts of extremist contents (Meleagrou-Hitchens and Kaderbhai, 2017; CEP, 2018).

Not unlike any other P/CVE interventions, eGLYPH has been appreciated and criticised at the same time from different angles. Mark Wallace, the CEO of the CEP and a former ambassador to the UN denominated eGLYPH as a "game-changer" and expressed his belief that this technology will successfully disrupt the online promotional activities of the terrorist groups. He further argued that when the extremists realise that their online posts will be removed long before becoming viral, they will become reluctant to upload the content at all.

While the experts agree that the automation element of eGLYPH can be useful in restricting the reach of IS and other extremist groups on social media, questions remain here, as well. For instance, Dr. John Hogan, Professor of Psychology at Georgia State University, who is also an expert on IS and other terrorist groups, acknowledges the potential of the tool to play a significant role in curtailing the extremist groups' digital footprint and acting as a frustrating move in strategic and psychological senses. However, he also pointed out the earlier question of how to determine what content may or may not constitute extremist or problematic ones.

Nevertheless, civil libertarians assert that the use of automated tools like eGYLPH are bound to supersede their prior design intention, which was fighting against child pornography. Dr. Farid proposed a solution to address the issue of non-extremist contents getting removed. He suggested creating a "whitelist" for pre-approved publishers licensed to circumvent the algorithm. In this way, the companies using eGLYPH or similar technologies can decide if they want to remove a flagged item or not (Klor and Benmelech, 2016).

CEP also acknowledges that automation can always produce false positives and realises that human verification is necessary while tackling extremist content online. They believe that if eGLYPH is coupled with human reviewers, where human researchers and content moderators will have the final decision-making authority, the whole system will work much more effectively and will be able to avoid controversies. This is why they suggest all the companies that wish to make use of eGLYPH technologies be entirely sufficient with trained human reviewers (CEP, 2018).

#### 4.1.3. Artificial intelligence (AI)

Artificial Intelligence (AI) is an invention of computer science and technology that can work, process, and analyse like humans. It can demonstrate many dispositions associated with human intelligence, including planning, learning, reasoning, problem-solving, knowledge representation, and social intelligence. At present, AI is mostly being deployed as algorithms that are familiar with certain datasets to recognise patterns and make automated decisions (Vaismoradi et al., 2016; Giscard d'Estaing, 2017). Web browsers like Google and social media channels like Facebook have been using AI to sort search preferences among their users and to carry out targeted advertising of different products. Similarly, Netflix and Amazon have been using AI algorithms to understand their customers' preferences to suggest future purchases (Cleveland et al., 2020; Parker and Lindekilde, 2020).

In the present time, extremist groups like IS have used the Internet and social media platforms like Facebook, Twitter, WhatsApp, and many others to radicalize individuals and promote VE. They use targeted branding to influence their target population's preferences and decision analysis to disseminate their ideology (Macdonald, 2018; Parker and Lindekilde, 2020). Furthermore, there have been occurrences of planning, communicating, and carrying out violent attacks around the world using the internet and social media channels as tools. As a result, governments of the nations already victimised or otherwise have urged the online platforms to address this crisis. In response, the web organisations,

particularly social media companies, expanded and intensified the use of AI to help tackle online promotion of VE content by identifying and removing it from the websites at a faster pace with increased accuracy (Millar et al., 2018).

As the internet is becoming cheaper and providing easier access every day, people of all ages across the globe are being more and more active on social media channels. In every single minute, on average, 510,000 comments and 136,000 photos are shared on Facebook, 350,000 tweets are posted on Twitter, and 300 h of video are uploaded to YouTube (Hossain et al., 2019; Sayeed et al., 2020; Sundarasen et al., 2020). As a result, while handling such huge amounts of data, social media companies are now depending on AI broadly (Hassan et al., 2020). In June 2017, Google, Facebook, Microsoft, Twitter, and YouTube announced the news of forming a collaborative platform named the Global Internet Forum to Counter Terrorism (GIFCT) to combat the spread of extremist propaganda online (Heller, 2020). Gradually, LinkedIn, Instagram, Dropbox, Ask. fm, Cloudinary, JustPaste.it, Verizon Media, Reddit, Snap, and Yellow joined, as well.

Adopting and deploying AI technology, only within the first quarter of 2018, Facebook took down 837 million spam contents, 2.5 million content promoting hate speech, and disabled 583 million Facebook accounts globally (Dahlberg, 2018; Hossain et al., 2019; Sayeed et al., 2020). In 23 months, starting from August 2015, Twitter suspended about a million accounts for promoting violence (Fernandez et al., 2018; Singh et al., 2018). In the latter half of 2017, YouTube deleted 150,000 videos spreading violence and extremism and about half of these videos were removed within 2 h of being uploaded (Macdonald, 2018; Macdonald et al., 2019).

The GIFCT member companies are also putting effort into addressing the issue of resurfacing a flagged or removed content on another website. They have developed a shared industry database of "hashes." Whenever one company identifies any extremist content, they share the hash of that content with other companies so that the AI technology of all the companies can include that hash in their database and proceed with removing it from their websites (Macdonald, 2018). Within 2018, GIFCT successfully added 100k hashes in the database which current number is 200K (Waldman and Verga, 2016; Aggarwal, 2019; Metsky et al., 2019).

While AI is applauded extensively for bringing about a disruption in the technology industry combating extremism online, many experts express certain concerns about the possible negative consequences of using AI for CVE. Particularly, terrorists adopting more encrypted sites (which are harder for AI to access) and limiting people's freedom to express political and social grievances are the two most major concerns. After all, AI technology can always make false identification (Ahmed, 2019; Westerlund, 2019; Winter et al., 2020).

However, GIFCT members claim to be well aware of this issue and partner with organisations that can provide them with human reviewer support and research organisations to better understand the latest trends of online terrorist propaganda. For example, Google has created a network of eight think tanks worldwide to develop better ethics of content moderation and planned to add 50 expert NGOs to their current list of 63 organisations for content flagging and moderation (D'Onfro, 2016). In 2017, Facebook employed 75,000 content reviewers and increased the number since then (Sayeed et al., 2020).

Experts and researchers of this field suggest building an effective hybrid system integrating human and AI or machine learning to solve the issues regarding contextual ambiguity and decision-making about the grey-zone or borderline contents (van der Vegt et al., 2019). After all, machine learning or AI is not foolproof partly because the humans who design it are not either (Polonaki, 2018).

#### 4.1.4. Mobile apps

With the advancement of technology in the area of CVE, governments, international organisations, and tech companies have joined hands to develop and deploy mobile apps aimed at countering the spread of VE using diversified approaches (Table 3). The following is the portrayal of some major mobile apps that have already been launched globally:

*4.1.4.1. UNDP Africa: Tackling Extremist Narratives.* With the concept of capturing local voices in developing counter narratives for tackling the extremist ones, UNDP in partnership with Albany Associates, a communications company developed a mobile app titled "UNDP Africa Toolkit: Tackling Extremist Narratives' ' (UNDP, 2018). This app has been designed to act as a toolkit for Civil Society Organization (CSOs) to plan and implement campaigns to combat extremist narratives. The developers of this app believe that alternative narratives work better than the counter-narratives as the first one is about "what we are" and the latter one is about "what we are against." They encourage creating alternative narratives that portray or involve positive and inclusive messages which are rooted in a community's history and traditions. For serving this purpose, this app contains a framework, step-by-step guideline on strategic and communication elements starting from primary concepts of narratives to planning a campaign. It also contains various sections containing information, checklists, online resources, tips, case studies, procedures, and protocols. All these elements have been aimed to help develop interventions like alternate narratives to counter the extremist narratives.

CSO delegates and other practitioners have overwhelmingly endorsed the UNDP Africa Toolkit. Mr. Mohamed Ibn Chambas, Head of the United Nations Office for West Africa and Sahel, expressed his optimism about this app and emphasised that this app will help groups across the regions to better fight the threats of VE. At the launch of the app, representatives from over 12 sub-Saharan countries discussed the contextual gaps between the national and international interventions and local crises and acknowledged that UNDP Africa Toolkit might succeed in closing this gap. Some of this app's unique features are that it is free of cost, readily available for download in Apple, Google play store or the web; and once downloaded, doesn't need any Internet connection. This app is available in English and French.

*4.1.4.2. GCTF – lifecycle toolkit.* In 2015, the Global Counterterrorism Forum (GCTF) launched the "Initiative to Address the Life Cycle of Radicalization to Violence". This initiative was co-led by Turkey and the United States and aimed to assist policymakers and practitioners with conceptual tools applicable at various stages of life cycle of radicalisation to violence. In 2017, as the next step of the web-based version of the toolkit, a mobile application for iOS and Android was created.

This GCTF Lifecycle Initiative Toolkit highlights good practices for countering violent extremism at any stage of the life cycle of radicalisation to violent extremism to the policymakers and the implementers. According to the GCTF website[4], these good practices are on the following stages:

i. **Prevention**: This section includes the push and pull-factors of violent extremism, locally relevant initiatives, educational initiatives, roles of families, and roadmap of initiatives.
ii. **Detection and Intervention**: This section delineates a human rights-compliant approach, alternatives to prosecution and incarceration and risk assessment tools.
iii. **Rehabilitation and Reintegration**: This section highlights the rehabilitative measures, legal frameworks, additional guidance and tailored approaches.

This app also enables its users to access the latest research from several international organisations and esteemed global experts on the counter-extremism field. This app is available in Arabic, English and French.

[4] https://toolkit.thegctf.org/en/About.

**Table 3.** Summary of the CVE focused Mobile Apps.

| Mobile Apps | Developer | Country | Approach |
|---|---|---|---|
| UNDP Africa: Tackling Extremist Narratives<br>Language: English & French | UNDP in Africa & Albany Associates | Ghana | • Makes use of positive and alternative messages focusing on community's history and roots<br>• Shares knowledge and case study based evidence<br>• Facilitates to close the contextual gap between national and international interventions<br>• Includes step by step guidelines and components for designing interventions<br>• Enables any user or group to plan and develop CVE intervention |
| GCTF – Lifecycle Toolkit<br>Language: English, French & Arabic | GCTF | Global | • Addresses different stages of radicalisation<br>• Identifies the pull factors of VE<br>• Conveys the good practices and contemporary research findings |
| Hedayah – MASAR App<br>Language: English | Hedayah & Royal United Services Institute (RUSI) | Global | • Provides the P/CVE projects with MM&E frameworks, including tutorials, guidelines, and resources<br>• Enables the P/CVE practitioners to connect through a common platform for knowledge sharing and collaboration |
| Against Violent Extremism (AVE)<br>Language: English | Institute of Strategic Dialogue (ISD) | Global | • Shares real-life experiences of the former extremists which can be perceived as credible to the people<br>• Provides the current extremists who want to come back to everyday life a place to seek help |
| YPSA-CVE Initiative App<br>Language: Bangla | Young Power in Social Action (YPSA) | Bangladesh | • Uses the local language, which can reach people from any educational background<br>• Uses community engagement approach |
| Hello CT App<br>Language: English & Bangla | CTTC Unit, Dhaka Metropolitan Police | Bangladesh | • Maintains anonymity of the informants<br>• Shares contemporary best practices and interventions<br>• Uses local language (Bangla) |

*4.1.4.3. Hedayah- masar app.* "Masar" means "path" or "trajectory" in Arabic. Hedayah, the International Center of Excellence for Countering Violent Extremism, in collaboration with the Royal United Services Institute (RUSI) launched a digital platform named the "MASAR App", in September 2018. The developers of this app claim that the MASAR app will assist the designers of P/CVE projects in staying on the right path for achieving desired outcomes and visible impact.

This app's objective was to make an interactive tool for the practitioners of P/CVE who are engaged in designing better frameworks for MM&E (monitoring, measuring & evaluating) for their CVE programs. This app can provide them with a customised step-by-step guideline on planning a CVE project with accompanying MM&E.

According to the webpage of the MASAR app[5], it contains the following content:

i. Step-by-step tutorial on developing your P/CVE project and MM&E
ii. Support developing a Theory of Change statement
iii. Guidance setting goals and objectives, indicators and activities
iv. Smart guidance on terminology related to MM&E through a glossary
v. A Library of resources related to MM&E and P/CVE
vi. Case studies of actual P/CVE projects and results

Furthermore, the MASAR app includes some unique features like creating a platform for the users to chat within a project, projecting the impacts of an intervention, and providing recommendations of existing research links. The app is also free to download and use for any practitioner.

The Executive Director of Hedayah, H.E. Maqsoud Kruse has described the app as a breakthrough in the field of impact measurement of P/CVE programs, which can improve implementation, develop policy, and generate empirical knowledge. Emily Winterbotham, Senior Research Fellow at RUSI, claims that the MASAR app will significantly evaluate the effectiveness of the P/CVE programs being designed in different countries. Her claim has been validated by several participants of the app testing event. They have assured that the app successfully provides directions regarding the steps to be taken, questions to

[5] https://play.google.com/store/apps/details?id=com.hedayah.masar&hl=en.

be asked, and resources to look for (Ahmed, 2019; Gerspacher and Weine, 2019).

*4.1.4.4. Against violent extremism (AVE).* The AVE is a network created by the Institute for Strategic Dialogue (ISD) in 2011 and launched in 2012 to tackle VE in the present world. This intervention's unique feature is that it has created a network among the former violent extremists and survivors of VE and enabled them to work together to combat the threats posed by the extremist groups. By connecting the former extremists from different histories and backgrounds, this network facilitated sharing by decoding first-hand experiences and leveraging the lessons. Their major focus is to push back the extremist propaganda or narratives and prevent the recruitment of "at-risk" youth.

To fight this battle against extremism, AVE uses technology to connect, exchange, disseminate, and influence violent extremism in all the forms existing, including the far right, the far left, Al Qaeda and the violent gangs in South America. For this purpose, they have launched a mobile app in 2017 along with the AVE website, so that the formers and survivors can join the network and contribute to ongoing CVE projects. ISD asserts that the AVE network has played a crucial role in their counter-narrative programs and other initiatives. According to the RAN issue paper (2016) regarding the AVE, the network seeks to serve the following primary functions:

i. Connecting credible messengers to one another so they can learn best practices and share ideas
ii. Matching credible messengers to private resources, skills and support
iii. Advocating the role of the former extremist and survivors in pushing back extremist narratives to governments and international bodies.

From the AVE network[6] website and mobile app, it was found that they have already reached 2641 connections, including 310 formers and 164 survivors, and together, they have been engaged in about 81 projects. The AVE app enables the downloaders to connect and communicate with the members of the network, discover AVE events and initiatives near them and collaborate with them. ISD has reported that the AVE network has played an integral role in the success of their several initiatives, including "Extreme dialogue counter-extremism education program" and "One to one direct intervention". The insights and experiences drawn from the former extremists helped the initiatives' designs and strategies to reach maximum efficiency.

### 4.2. Existing online-based/digital CVE interventions in Bangladesh

This section depicts the existing situation about the deployment of online/digital CVE interventions in Bangladesh. It also delineated the unique features of the present interventions and received acclamations.

#### 4.2.1. YPSA – CVE initiative

A non-government organisation in Bangladesh named "Young Power in Social Action (YPSA)" has launched a mobile app titled "YPSA CVE Initiative" (Table 3). This app is a component of their ongoing project on "Community Engagement in Countering Violent Extremism in Cox's Bazar (CEVEC)"[7]. This app aims to combat VE through community engagement in Cox's Bazar district, Bangladesh. This app contains flipcharts and leaflets, highlighting students' and youth cohorts' roles and responsibilities towards CVE. It also includes sessions on family and society, extremism and violence, the negative sides of extremism, and the victims of extremism with the aim of knowledge sharing regarding these issues[8]. This app is entirely in Bangla, which makes it convenient to use for the local population. This app is also free to download and use. However, this app doesn't have any national version that will influence people from other localities to use it.

#### 4.2.2. Hello CT

In July 2016, the Counter-Terrorism and Transnational Crime (CTTC) unit of Dhaka Metropolitan Police (DMP) launched an anti-militancy mobile app named "Hello CT"[9]. This app aims to create a bridge between countrymen and the CTTC unit through which citizens can forward and report on information regarding crimes or suspicious activities around them (Table 3). Using this app, people can share information regarding extremism/militancy, cybercrime/cyber terrorism, bombs/explosives/arms/narcotics, and terrorist financing/smuggling/fake currency. According to the app description, the informant's identity is not revealed, nor is it mandatory to provide. The informants can also share pictures and audio/video clips through this app. This app also contains a section titled "News Feed," where local news, slogans, best practices, and campaigns are shared for awareness building among this app's users. The "Hello CT" app is free to download and use, and the instructions inside are provided both in English and Bangla[10].

#### 4.2.3. Bangladesh peace observatory (BPO)

The Centre for Genocide Studies launched the Bangladesh Peace Observatory (BPO) in the University of Dhaka as a component of UNDP's project on "Partnership for a Tolerant, Inclusive Bangladesh (PTIB)" in 2017[12]. The BPO is a research facility with a website that provides free and easy access to data, mapping trends, and various research outputs to create a better understanding of the present state of different sorts of violence in the country among the citizens and other stakeholders[11].

The major goal of BPO is advancing the understanding of peace and tolerance through data insights. It uses mapping and data analytics technology to create a virtual platform that shares knowledge about the state of political, ethnic, communal, criminal, gender-based, and extremist violence. This website contains different sources of publicly available data and visualises those in a useful and interactive way so that the consumers or interested stakeholders like policymakers, civil society, and media can easily understand and procreate accordingly[12].

The UNDP Bangladesh Country Director, Mr. Sudipto Mukherjee, expressed his anticipation about the BPO stating that this initiative can help influence effective policy and contribute to countering rumors by providing facts rather than fear[13].

## 5. Discussion

This study gives an overall picture of successful online-based CVE strategies worldwide and identified effective ones in the context of Bangladesh. Even though extremists used every possible way for VE activities, social media and the internet are the most prominent ones. Extremists targeted people of different ages for VE activities, but young people are particularly the most vulnerable. This section discusses the effective online-based interventions to reduce VE activities in Bangladesh and presents a brief portrayal of the experts' opinion regarding the ongoing CVE initiatives already deployed. Based on their suggestions about some digital/tech-based CVE strategies that are deemed to have

[6] http://www.againstviolentextremism.org/.
[7] https://ypsa.org/community-engagement-in-countering-violent-extremism-in-cox-bazar-cevec/.
[8] https://play.google.com/store/apps/details?id=org.ypsa.ypsa&hl=en.
[9] https://www.banglanews24.com/national/article/54277/Anti-militancy-Hello-City-apps-launched.
[10] https://dmp.gov.bd/police-apps-hello-ct/.
[12] http://peaceobservatory-cgs.org/#/
[11] https://rsis-ntsasia.org/event/launching-of-bpo-bangladesh-peace-observatory/.
[13] http://www.bd.undp.org/content/bangladesh/en/home/presscenter/pressreleases/2017/031/13/22111.html.

high potential for success in the Bangladesh context are also discussed in this section. Considering the effective online-based CVE scenarios, this study indicates theoretical implications by extending our knowledge of successful CVE strategies to reduce the VE activities in Bangladesh and other developing countries.

### 5.1. Effective CVE initiatives for Bangladesh

Based on the discussion on globally deployed online/digital interventions, a typology with two major categories emerged among the measures: positive and negative, similar to the classification provided by Hussain and Saltman (2014). Judging from the approach and implementation strategies, the RM can be categorized under positive measures; and the eGLYPH and AI technologies can be categorised under the negative measures. In the case of mobile apps, all of them are intended to share positive messages and influence cooperation among CVE practitioners rather than taking down or censoring extremist contents online; the apps can also be categorised under positive measures. A common drawback of all these apps is that none of these are promoted or advertised enough to the local or global potential customers. Not much reviews or criticism can be found for any of these apps and this scenario indicates that the apps are yet to obtain substantial reach. Without further research, the implications of none of the categories can be overruled, and it is also possible that the combined implementation of both types of measures can be useful in handling the present threat of VE activities. Table 2 highlights the pros and cons and the programmatic lessons of the major CVE interventions globally reviewed in this study.

### 5.2. High potential CVE strategies for Bangladesh based on expert opinions

This section discusses the CVE strategies, which may hold high potential in Bangladesh's context. The experts interviewed laid out their current understandings about the nature and prevalence of VE. From their depictions, the source of VE in Bangladesh can be divided into two major categories. One of them is extremism driven by religious beliefs. The other is violence influenced by political motives and power plays.

In the case of portraying VE from the religious angle, most of the experts defined extremism as religious minorities being oppressed by the larger religious groups, which in Bangladesh's case are the Islamic extremist/fundamentalist groups. Some of them also added that extremism had been around in Bangladesh for a long time, where religious, ethnic, or other types of minorities are oppressed and face different sorts of violence. Interestingly, while talking about Islamic extremist or fundamentalist groups, most of the respondents tended to indicate ordinary people who are generally conservative in nature when it comes to religious and cultural beliefs rather than pointing out specific terrorist groups. This shows that the experts acknowledge the general religious or other intolerance prevailing in society while going deep into VE in Bangladesh.

The other source of violence, the political unrest and fights, was mentioned by the experts during the interviews by referring to the fact that "Jamaat-e-Islami", a recognized Islamist political party, have often been found to be affiliated with extremism and violence. They still operate as a legitimate political party in Bangladesh. The experts stated that allowing such occurrence has enabled religious extremism to be shifted towards politics, and extremist mentality has become more or less prevalent at every level and sector of the country.

Apart from this, several other reasons behind the rise and existence of VE were highlighted in the interviews. One of the major reasons noted is a lack of in-depth knowledge among people regarding their religions and others. Most experts asserted that this knowledge gap emerged over time and ordinary people are susceptible to manipulation by various misleading promotional materials or activities. They further argued that a lack of knowledge drives such mentality and may instill prejudice towards other religions and cultures and justify violence against minorities. Another major reason underscored was the division among educational institutions of Bangladesh: Bangla-medium, English-medium and Madrasah. This situation results in various disturbances, including discrepancies among the content covered by different educational systems, a lack of understanding about the other systems, and, most importantly, discrimination in the workforce. According to them, people generally seem to get certain privileges and face challenges due to their educational background, which can lead to isolation and frustration among the victims. Above all, the experts specified that the fragmentation among the general population through sustaining three different mediums of education could produce more reasons to stereotype and marginalize people socially.

When asked about VE's features that they consider as unique or predominant in Bangladesh, most of the respondents agreed that there is no uniqueness of VE that takes predominance in this country's context. They also pointed out that the common understanding among the general people that held Madrasahs as the major source of radicalization has taken a significant shift due to the recent evidence. However, many respondents put forward concern about the easy and cheap access of the Internet to the country's youth population, which may make them more vulnerable to the threats of radicalization and VE.

Experts believe the P/CVE space in Bangladesh to be underpopulated against the need. Most of the respondents mentioned some of the Bangladesh government-led interventions like the "Hello CT" app, the Digital Security Act of 2018, and other security-led online monitoring and counternarrative campaigns by CTTC, which are a practical approach to reduce the VE activities. However, all agreed that these activities are not well-promoted and are not proportionate to the need. By and large, the government continues to rely on kinetic interventions in the CT space instead of softer P/CVE activities.

A major shortcoming in the interviews is that there are no well-known authorized sources or platforms in Bangladesh to verify fake news and propaganda shared on social media. Bangladesh is yet to gain sufficient technological advancement or dedicated platforms to deal with the constant flow of information when there is no available scope for verification. Another major limitation highlighted was the one-sided focus on the urban population with regard to CVE programmes. Many experts expressed that leaving the rural areas and population behind while planning or implementing a national level CVE initiative may create opportunities for the extremists to be more and more active in those areas by hiding.

During the interviews, the participants were asked to share their understandings regarding the potential for innovative app-based or other digital technologies for P/CVE in Bangladesh. In response, most of the respondents expressed that they preferred offline approaches rather than online ones to counter VE, arguing that technology should mostly be used to monitor suspicious people, groups, activities, and the flow of information consumed by the mass population. However, many respondents agreed that digital platforms need to play a vital role in taking care of a new age technology-based problem.

Following are some technology-based online/digital interventions or strategies that were mentioned by the experts which they perceive to hold high potential:

a) **Online Courses**: They argued that studies specifically indicate that mothers and spouses are able to pick up on early indicators of VE compared to others. They also suggested that teachers can play a vital role in detecting signs of potential radicalization among students. Therefore it was recommended that online courses should be designed and promoted among teachers and parents to train them about the safe use of technology, social media use and online platforms.
b) **Positive Messaging**: Disseminating positive, subliminal messages, for instance, showing lifestyles of various successful people who are happy with their place in life and career through entertainment programs was suggested in the interviews. The respondents opined that showing similarities of life problems, challenges and success among different religious or cultural groups shows people how they are not that much different from each other may contribute in eliminating prejudices towards people from different backgrounds.

c) **Online Religious Platform**: An online platform involving the trained and legitimate religious leaders where they can preach the real messages of religions while providing authentic references to their claims.
d) **Information Verification Platform**: Most of the respondents suggested creating more online platforms or promoting the existing ones where people can visit for evaluating the authenticity of information they have come across through social media or other sources or their doubts about certain matters relating to religions/societal/international issues. They also suggested that such a platform needs to be controlled and monitored by government agencies.
e) **Gaming**: Gaming was suggested as an effective technological tool that could reach a greater audience, and it should be easier to create the demand and ensure that the people are engaging with the software. These games have to be designed as a role playing simulation where the players will choose characters for solving an imitated real-life crisis. Through posing themselves in the good guys' places, the players will be able to stimulate empathy and crisis management skills among themselves.

While discussing these online/digital interventions some specific suggestions were pointed out during the interviews. Following are some of the major suggestions noted:

a) CVE interventions should be implemented by credible sources like the government. The NGOs, private sector and civil society can partner with the government for technological or resources support.
b) When designing content for CVE campaigns, some obvious words like 'radicalization' should not be used.
c) Promoting the positive messages of the generic role models like Buddha, Gandhi, Tagore who represent peace and tolerance.
d) Utilizing heavily trafficked social media platforms for disseminating liberal content or messages.
e) Generating funds from external donors and reaching out to more technologically developed countries for developing apps and digital platforms.
f) Academia can play a significant role in this regard. They can hold conferences for bringing together national and international experts under one roof for sharing knowledge where the government bodies, non-government actors, and private sector can also participate with a vision of developing an integrated plan for CVE

The interview participants also expressed that Government institutions are carrying out some reformative actions in this regard, like redesigning Madrasahs' curriculum with extracurricular activities. NGOs are developing programs where they are engaging the local youths into community work to feel ownership and improve the bonds within the community between different cultural or religious groups. Incubators are developing future plans on awareness building and promotional activities. However, most experts emphasized the lack of an integrated national policy on tackling radicalization and VE at large.

### 5.3. Recommendations for CVE interventions in Bangladesh

Following are some recommendations for potential CVE interventions in Bangladesh based on the global best practices and local context comprehended through this study:

a) The investigative studies in Bangladesh so far have looked into the victims' or militants' economic, educational and social backgrounds but did not concentrate enough on identifying the driving factors that led them to this path. In order to develop an understanding of the driving factors, emphasis needs to be put on conducting empirical research in Bangladesh context. This research should try to investigate the social-psychological aspects, including identity, history and recognition, which might have contributed to the radicalization process of the individuals.
b) An inquiry-based intervention can design focused on the former or identified extremists to understand what drove them towards radicalization and extremism. The insights from this research can be used to address the contextual factors present in the country and identify the at-risk individuals. In the next step, an interactive online course can be developed based on the research findings, particularly for the students and young graduates or professionals. In this app or website, the users will have to go through a number of documentaries, pictures, and videos, and will participate in a series of quizzes, case study analyses, and creative writings. The answers and reactions provided by each participant will be properly documented and preserved. A team of analysts and experts will help determine whether the participants are radicalized or not. A whole campaign can be designed for this course, and the campaign can partner with the educational institutions and offices for influencing the students and the professionals to take this course.
c) This is not an unknown scenario that people's news feed in social media gets bombarded with fake and outraging news or stories regularly. Availability of a credible and trustworthy website or platform for investigating such news's authenticity is the need of the hour in Bangladesh context. This website or platform should be enabled to process the news links shared by any visitor and report back the legitimacy of the news. Such technology will contribute in avoiding mass confusion and triumphs of influencing violence in the community. Although such websites exist in the country, none of them is mass-promoted. An intervention focused on promoting such websites or platforms at the national level would be useful for minimizing this knowledge gap among people.
d) The societal impact of the speeches delivered by the religious preachers is an attention-worthy issue in this field. They have enormous opportunities for influencing the mindset of people from different communities. A targeted campaign can be designed, including religious preachers, which will comprise workshops, seminars, and online courses to build awareness among them and encourage them to share positive messages. This campaign can be organized in partnership with the Ministry of Religious Affairs for ensuring credibility. Another aim of this intervention will be providing the preachers with digital literacy so that they can better check the authenticity of the information they share and communicate with the mass people for counselling and disseminating positive messages. In due course, a platform can be launched, which will connect the country's religious leaders where they will share the constructive messages of religions, and interested people will be able seek valid information and guidance from this platform. While designing these interventions, some crucial components should be taken into consideration. For instance, suggestions for replacing the so-called "benefits" of extremism. In addition, the counter or alternative narratives should be based on empirical evidence. Moreover, initiatives should be taken for developing an internationally-accepted ideology as alternatives to the extremist ones.
e) Another important recommendation for the context of Bangladesh is to establish a strong online monitoring mechanism at the national level for checking extremist activities through the internet and social media.

VE is a global crisis that needs to be addressed at the local level. For this purpose, knowledge sharing among nations is absolutely crucial. Global innovations, interventions need to be contextualized and applied in every country, including Bangladesh. Many CVE interventions like AI Technology require expensive technologies and expert technicians, and Bangladesh being a developing country, can acquire these through partnership and funding from the developed countries. Forming an efficient working committee and network at the national level, including the government ministries, national and

international NGOs, civil society, think tanks, educational institutions and private organizations solely dedicated to countering and preventing VE, will be a milestone for the country. The proper implications of recommended online CVE strategies will help Bangladesh to be a safer place in respect of VE activities.

## 6. Limitations of the study

There are some limitations to this study. The collected resources for this study from different online sources, and even though a large body of documents was analyzed, many documents repeated similar information. Despite comprehensive searching for different online sources, some important documents may have been left out. Experts sometimes give biased answers, which can essentially destroy the value of the collected information. Despite those limitations, this study will give effective insights to understand successful CVE strategies for Bangladesh and will make Bangladesh a safer place to live on.

## 7. Concluding remarks and avenue of future research

Social Media and the Internet offer significant possibilities for supporting the fulfillment of the 2030 Sustainable Development Agenda and advancing all human rights, including access to information, freedom of expression, and privacy. Social media is also responsible for leading vulnerable individuals to perform VE activities. This study aims to identify effective online-based CVE strategies for Bangladesh in minimising the VE activities induced by social media and the Internet. The strategies identified are based on the existing successful global online/offline/digital CVE practices and the most prominent current local interventions in Bangladesh's context. Based on content analysis of selected newspaper articles, blog posts, published journal articles, and video clips, this research's objective is achieved. From the analysis and expert interviews, it was found that VE using social media is a global crisis, and to reduce it, knowledge sharing among nations is absolutely crucial. AI and mobile apps technologies are the most effective online-based CVE strategies to reduce the VE activities in Bangladesh. AI Technology requires expensive equipment and expert technicians and being a developing country Bangladesh, can acquire these through partnership and funding from the developed countries. Bangladesh government is already launching several mobile apps to reduce VE activities, but these initiatives are not well-promoted to the larger audience, especially in the rural areas. Leaving the population of the rural areas behind while planning or implementing a national level CVE initiative may create opportunities for the extremists to be more active in those areas. Experts suggest that positive messages through online courses, online religious platforms and gaming designed for solving real-life crises can play a vital role in CVE activities. Credible sources, like the government of Bangladesh, need to implement CVE interventions with the help of technology or resources support from NGOs, private sectors and civil society. Through implementing effective online CVE strategies, more knowledge sharing, synergy, and multi-stakeholder enterprises, Bangladesh and other less developed countries can concurrently deal with violent extremity by successfully using cutting-edge online/digital technologies. Future research avenues may focus on the effectiveness of existing and recommended online-based CVE interventions by analysing their impacts on the younger population (15–30 years) of city-rural areas in developing countries.

## Declarations

### *Author contribution statement*

**Sajid Amit**: Conceived and designed the experiments.
**Lumbini Barua**: Analyzed and interpreted the data.
**Abdulla - Al Kafy**: Contributed reagents, materials, analysis tools or data; Wrote the paper.

### *Funding statement*

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

### *Data availability statement*

Data will be made available on request.

### *Declaration of interests statement*

The authors declare no conflict of interest.

### *Additional information*

No additional information is available for this paper.

## Acknowledgements

We want to express our heartiest gratitude to all the experts for identifying effective implementable CVE strategies with useful recommendations for Bangladesh. The authors also like to thank Dynamic Institute of Geospatial Observation Network (DIGON) research and

## Annex 01. List of Experts interviewed for the study

| No | Name | Designation | Organization |
|---|---|---|---|
| 1 | Shazzad Hissain Mukit | Chief Executive Officer | Careerki.com |
| 2 | Helal Hossain | Head of Portfolio | Swiss contact South Asia Regional Office, Bangladesh |
| 3 | Inam Uz Zaman | Project Lead | Upskill from Startup Dhaka |
| 4 | Mohammad Shahriar Rahman, Ph.D | Associate Professor and Acting Head. Department of Computer Science and Engineering (CSE) | University of Liberal Arts Bangladesh |
| 5 | Ariful Hoque | Manager, Communications Office | University of Liberal Arts Bangladesh |
| 6 | Asif Uddin Ahmed | Acting Director | EMK Center |
| 7 | Shidartho Goushami | Project Officer | Partnership for a Tolerant, Inclusive Bangladesh (PTIB), Project UNDP, Bangladesh |
| 8 | Adib Sarwar | Head of R&D, | Karrigor.com |
| 9 | Muntasir T. Chowdhury | Executive Director, | Inspira Advisory and Consulting Ltd |
| 10 | Ahmed Saad Ishtiaque | Director (Research), | Creative Research & Consultancy |
| 11 | Afsana Anjum | Lecturer, General Education Department | University of Liberal Arts Bangladesh |

(*continued on next page*)

(*continued*)

| No | Name | Designation | Organization |
|---|---|---|---|
| 12 | Professor Din M. Sumon Rahman, PhD | Department of Media Studies & Journalism & Director, Office of Faculty Research | University of Liberal Arts Bangladesh |
| 13 | Faiz Sobhan | Senior Research Director, | Bangladesh Enterprise Institute |
| 14 | Abantee Harun | Adjunct Faculty, General Education Department | University of Liberal Arts Bangladesh |
| 15 | Oliur Rahman Tarek | Research and Communication Associate, CES | University of Liberal Arts Bangladesh |

consultancy firm experts for proofreading the entire manuscript and doing language editing.

## References


Aggarwal, N.K., 2019. Questioning the current public health approach to countering violent extremism. Global Publ. Health 14, 309–317.

Ahmed, S., 2019. Combating violent extremism cannot Be limited to just security. In: The Daily Star. https://www.thedailystar.net/opinion/perspective/news/combating-violent-extremism-cannot-be-limited-just-security-1741189.

Alam, I., 2015. Social media radicalisation in Bangladesh: a lurking new threat. In: FAIR: Foreign Affairs Insights & Review. https://fairbd.net/social-media-radicalisation-in-bangladesh-a-lurking-new-threat/.

Alava, S., Frau-Meigs, D., Hassan, G., 2017. Youth and Violent Extremism on Social media: Mapping the Research. UNESCO Publishing.

Ambrozik, C., 2018. Countering Violent Extremism Locally.

Ashour, O., 2010. Online de-radicalization? Countering violent extremist narratives: message, messenger and media strategy. Perspect. Terrorism 4, 15–19.

Bashar, I., 2017. Countering violent extremism in Bangladesh. Counter Terrorist Trends and Analyses 9, 17–21.

Berger, J., 2016. Making CVE work, 7. International Centre for Counter-terrorism, The Hague.

Berrebi, C., 2003. Evidence about the Link between Education. Poverty and Terrorism Among Palestinians. nPrinceton University In $ dustrial Relations Section Working Paper, p. 477.

BIPSS, B.I.o.P.a.S.S., 2017. Local Drivers and Dynamics of Youth Radicalisation in Bangladesh. http://bipss.org.bd/pdf/LocalDrivers.pdf.

Borum, R., 2003. Understanding the terrorist mind-set. FBI Law Enforc. Bull. 72, 7.

Briggs, R., Feve, S., 2013. Review of Programs to Counter Narratives of Violent Extremism.

CEP, C.E.P., 2018. CEP recommendations: tackling extremist content online.

CEP, C.E.P., 2019. Bangladesh: extremism & counter-extremism. https://www.counterextremism.com/sites/default/files/country_pdf/BD-06152020.pdf.

Cheng, M., Foley, C., 2018. The sharing economy and digital discrimination: the case of Airbnb. Int. J. Hospit. Manag. 70, 95–98.

Christenson, C., 1997. The Innovator's Dilemma. Harvard Business School Press, Cambridge, Mass.

Cleveland, E., Glaeser, S., Jorgensen, L., Lewi, L.N., Shropshire, A., 2020. Preventing and Countering Violent Extremism: Localization in Kenya, Kosovo, and the Philippines. Workshop in Public Affairs.

Cobb, J.A., Wry, T., Zhao, E.Y., 2016. Funding financial inclusion: institutional logics and the contextual contingency of funding for microfinance organizations. Acad. Manag. J. 59, 2103–2131.

Corraya, T.A., 2017. The School Bag's Weight Influence on the Physical Status of School Going Children. Bangladesh Health Professions Institute, Faculty of Medicine, the University.

D'Onfro, J., 2016. The Subtle Way Google Plans to Use its Greatest Skill to Combat ISIS. Business Insider.

Dahlberg, L., 2018. Facebook's Response to its Democratic Discontents.

Davies, G., Neudecker, C., Ouellet, M., Bouchard, M., Ducol, B., 2016. Toward a framework understanding of online programs for countering violent extremism. J. Deradicalization 51–86.

Denoeux, G., Carter, L., 2009. Guide to the Drivers of Violent Extremism. USAID. February.

Elshimi, M.S., 2017. De-radicalisation in the UK Prevent Strategy: Security, Identity and Religion. Taylor & Francis.

EU, E.U., 2015. Extremism and violent extremism - RUSI. https://rusi.org/sites/default/files/mn0115566enn.pdf.

Fernandez, M., Asif, M., Alani, H., 2018. Understanding the roots of radicalisation on twitter. In: Proceedings of the 10th acm Conference on Web Science, pp. 1–10.

Frazer, O., Nünlist, C., 2015. The Concept of Countering Violent Extremism. CSS Analyses in Security Policy, p. 183.

Gerspacher, N., Weine, S., 2019. Creating Positive Policing Narratives for Countering Violent Extremism. Lulu Press, Inc.

Gielen, A.-J., 2017. Evaluating Countering Violent Extremism. Deradicalisation: Scientific Insights for Policy, pp. 101–118.

Giscard d'Estaing, S., 2017. Engaging women in countering violent extremism: avoiding instrumentalisation and furthering agency. Gend. Dev. 25, 103–118.

Gordon, E., True, J., 2019. Gender stereotyped or gender responsive? Hidden threats and missed opportunities to prevent and counter violent extremism in Indonesia and Bangladesh. Rusi 164, 74–91.

Government, A., 2017. Foreign policy white paper. https://www.dfat.gov.au/sites/default/files/2017-foreign-policy-white-paper.pdf.

Green, S., Proctor, K., 2016. Turning point: A New Comprehensive Strategy for Countering Violent Extremism. Rowman & Littlefield.

Hassan, T., Alam, M.M., Wahab, A., Hawlader, M.D., 2020. Prevalence and associated factors of internet addiction among young adults in Bangladesh. J. Egypt. Publ. Health Assoc. 95, 3.

Heller, B., 2020. Combating Terrorist-Related Content through AI and Information Sharing. Algorithms.

Heydemann, S., 2014. Countering Violent Extremism as a Field of Practice, 1. United states institute of peace insights, pp. 9–11.

Hossain, S.F.A., Nurunnabi, M., Hussain, K., Saha, S.K., 2019. Effects of variety-seeking intention by mobile phone usage on university students' academic performance. Cogent Edu. 6, 1574692.

Houston, D., Meyer, L.H., Paewai, S., 2006. Academic staff workloads and job satisfaction: expectations and values in academe. J. High Educ. Pol. Manag. 28, 17–30.

Husain, T., 2017. Counter terrorism approaches: with reference to Bangladesh. ABC J. Adv. Res. 6, 9–16.

Hussain, G., Saltman, E.M., 2014. Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it. Quilliam.

Idris, I., 2019. Preventing/countering Violent Extremism Programming on Men, Women, Boys and Girls.

Khan, H., 2015. Why Countering Extremism Fails. Foreign Affairs.

Klein, C., 2017. Cold war cosmopolitanism: the Asia foundation and 1950s Korean cinema. J. Kor. Stud. 22, 281–316.

Klor, E., Benmelech, E., 2016. What Explains the Flow of Foreign Fighters to ISIS? NBER Working Paper Series National Bureau of Economic Research.

Kruse, M., 2016. Countering violent extremism strategies in the Muslim world. Ann. Am. Acad. Polit. Soc. Sci. 668, 198–209.

Kundnani, A., Hayes, B., 2018. The Globalisation of Countering Violent Extremism Policies. Undermining Human Rights, Instrumentalising Civil Society. Transnational Institute, Amsterdam.

Lakhani, S., 2012. Preventing violent extremism: perceptions of policy from grassroots and communities. Howard J. Crim. Justice 51, 190–206.

Lichtenberger, E., Witt, M.A., Blankenberger, B., Franklin, D., 2014. Dual credit/dual enrollment and data driven policy implementation. Community Coll. J. 38, 959–979.

Macdonald, S., 2018. How Tech Companies Are Successfully Disrupting Terrorist Social media Activity. The Conversation.

Macdonald, S., Correia, S.G., Watkin, A.-L., 2019. Regulating terrorist content on social media: automation and the rule of law. Int. J. Law Context 15, 183–197.

Macnair, L., Frank, R., 2017. Voices against Extremism: a case study of a community-based CVE counter-narrative campaign. J. Deradicalization 147–174.

Mandaville, P.G., Nozell, M., 2017. Engaging Religion and Religious Actors in Countering Violent Extremism. JSTOR.

Meleagrou-Hitchens, A., Kaderbhai, N., 2017. Research Perspectives on Online Radicalisation: A Literature Review, 2006–2016. International Centre for the Study of Radicalisation, p. 19.

Metsky, H.C., Siddle, K.J., Gladden-Young, A., Qu, J., Yang, D.K., Brehio, P., Goldfarb, A., Piantadosi, A., Wohl, S., Carter, A., 2019. Capturing sequence diversity in metagenomes with comprehensive and scalable probe design. Nat. Biotechnol. 37, 160–168.

Millar, C., Lockett, M., Ladd, T., 2018. Disruption: technology, innovation and society. Technol. Forecast. Soc. Change 129, 254–260.

Mirchandani, M., 2017. Countering Violent Extremism: Lessons for India. Observer Research Foundation.

Morse, C., 2016. Advancing CVE research: the roles of global and regional coordinating bodies. https://ct-morse.eu/wp-content/uploads/2016/07/Report-CVE-Mapping-Research.pdf.

Neuendorf, K.A., Kumar, A., 2015. Content Analysis. The International Encyclopedia of Political Communication, pp. 1–10.

ODIHR, O., 2014. Preventing Terrorism and Countering Violent Extremism and Radicalization that lead to Terrorism: a Community-Policing Approach.

Parker, D., Lindekilde, L., 2020. Preventing extremism with extremists: a double-edged sword? An analysis of the impact of using former extremists in Danish schools. Educ. Sci. 10, 111.

Patel, F., Koushik, M., 2017. Countering Violent Extremism. Brennan Center for Justice at New York University School of Law.

Saltman, E.M., Russell, J., 2014. White Paper–The Role of Prevent in Countering Online Extremism. Quilliam publication.

Sayeed, A., Hassan, M.N., Rahman, M.H., El Hayek, S., Al Banna, M.H., Mallick, T., Hasan, A.-R., Meem, A.E., Kundu, S., 2020. Facebook addiction associated with

internet activity, depression and behavioral factors among university students of Bangladesh: a cross-sectional study. Child. Youth Serv. Rev. 118, 105424.
Shortell, S.M., Zajac, E.J., 1990. Perceptual and archival measures of Miles and Snow's strategic types: a comprehensive assessment of reliability and validity. Acad. Manag. J. 33, 817–832.
Silverman, T., Stewart, C.J., Amanullah, Z., Birdwell, J., 2016. The Impact of Counter Narratives: Insights from a Year-Long Cross-Platform Pilot Study of Counter-narrative Curation, Targeting, Evaluation and Impact. Institute for Strategic Dialogue, p. **52**.
Singh, M., Bansal, D., Sofat, S., 2018. Who is who on twitter–spammer, fake or compromised account? a tool to reveal true identity in real-time. Cybern. Syst. 49, 1–25.
Soldatenko, D., Backer, E., 2019. A content analysis of cross-cultural motivational studies in tourism relating to nationalities. J. Hospit. Tourism Manag. 38, 122–139.
Stevens, T., Neumann, P.R., 2009. Countering online radicalisation: a strategy for action. Int. Centre Study of Radicalisation Political Violence.
Stewart, C.M., 2017. Countering violent extremism policy in the United States: are CVE programs in America effectively mitigating the threat of homegrown violent extremism. In: Naval Postgraduate School Monterey United States.
Sundarasen, S., Chinna, K., Kamaludin, K., Nurunnabi, M., Baloch, G.M., Khoshaim, H.B., Hossain, S.F.A., Sukayt, A., 2020. Psychological impact of COVID-19 and lockdown among university students in Malaysia: implications and policy recommendations. Int. J. Environ. Res. Publ. Health 17, 6206.
The_Daily_Star, 2019. Role of family and religious values in preventing violent extremism. In: The Daily Star. https://www.thedailystar.net/round-tables/news/role-family-and-religious-values-preventing-violent-extremism-1791259.
Thiessen, C., 2019. Preventing Violent Extremism while Promoting Human Rights: toward a Clarified UN Approach.
UN, 2016. Handbook on the Management of Violent Extremist Prisoners and the Prevention of Radicalization to Violence in Prisons. https://www.unodc.org/pdf/criminal_justice/Handbook_on_VEPs.pdf.
UNDP, 2016. Preventing Violent Extremism through Inclusive Development and the Promotion of Tolerance and Respect for Diversity. https://www.undp.org/content/undp/en/home/librarypage/democratic-governance/conflict-prevention/discussion-paper—preventing-violent-extremism-through-inclusiv.html.
UNDP, 2018. UNDP Launches mobile Application to Help Design Campaigns to Prevent Violent Extremism. Available at: (accessed Retrieved 6 17, 2019, from UNDP in Africa: ).
UNESCO, 2016. What Makes a Terrorist?.
USAID, 2011. The Development Response to Violent Extremism and Insurgency Policy. https://www.usaid.gov/sites/default/files/documents/1870/VEI_Policy_Final.pdf.
Vaismoradi, M., Jones, J., Turunen, H., Snelgrove, S., 2016. Theme Development in Qualitative Content Analysis and Thematic Analysis.
van der Vegt, I., Gill, P., Macdonald, S., Kleinberg, B., 2019. Shedding light on terrorist and extremist content removal. Global Research Network on Terrorism and Technology.
Waldman, S., Verga, S., 2016. Countering Violent Extremism on Social media. (Accessed 25 August 2018).
Weine, S., Kansal, S., 2019. What should global mental health do about violent extremism? Global Mental Health 6.
Weine, S., Eisenman, D.P., Kinsler, J., Glik, D.C., Polutnik, C., 2017. Addressing violent extremism as public health policy and practice. J. Sport Tourism 9, 208–221.
Westerlund, M., 2019. The emergence of deepfake technology: a review. Technol. Innovation Manag. Rev. 9.
Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., Fürst, J., 2020. Online extremism: research trends in internet activism, radicalization, and counter-strategies. Int. J. Comput. Vis. 14, 1–20.