TROUBLE AHEAD:

Risk, resilience and the challenge of online violent extremism in Central Asia

June 2021

SecDevAnalytics

Contents

Acknowledgements

This report was prepared by SecDev Group. It draws on field research conducted by analysts between June and December 2020. Ideas were developed and refined during workshops with the Organization for Cooperation and Security and Europe and the RESOLVE Network between March and May 2021. The report was led by the Eurasia team at SecDev Group, including Vadim Dryganov, Kumar Bekbolotov, Kateryna Gazaryan, Behruz Davletov, Temur Davronov. Additional inputs were made by Rafal Rohozinski and Robert Muggah.

SecDev Group was supported throughout by partners from Central Asia. These include the Civic Initiative for Internet Policy (Kyrgyzstan) and its director Tattu Mambetaliva as well as colleagues Marat Torobekov and Asomiddin Atoev. SecDev Group also hosts an annual Central Asia Security Forum that assembles independent researchers, security officials and technology companies to discuss the challenge of digital transformation and violent extremism across the region. SecDev Group is grateful to Facebook for providing support to undertake this assessment.

List of abbreviations

P/CVE	Preventing/countering violent extremism
TO	Terrorist organization
VEO	Violent extremist organization
AD	Hurras al Din
HTS	Hayyat Tahrir al-Sham
IJU	Islamic Jihad Union
IK	Imarat Kavkaz
IS	Islamic State
ISWC	Islamic State Wilayah Caucasus
ISWK	Islamic State Wilayah Khorasan
JA	Jannat Ashugu
JAN	Jamaat Ansarullah
KGT	Katibat al Ghuraba al Turkistan
KIB	Katibat Imam Bukhari
LMA	Liwa al Muhajireen wal Ansar
MT	Malhama Tactical
ND	Nogai Djamaat
TJK	Tavhid va Jihod Katibasi

TROUBLE AHEAD:

Risk, resilience and the challenge of online violent extremism in Central Asia

Executive summary

Central Asia's rapid digital transformation is dual-edged. On the one hand it is expanding online services, powering digital commerce and expanding social connectivity. On the other it is facilitating the social media presence of violent extremists. Whilst Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan are undergoing digitalization at different speeds, they share a common challenge of online harms with destabilizing consequences.

This report by the SecDev Group examines the scope, scale and dynamics of violent extremist threats across the region, focusing on their evolution on social media throughout 2020. After examining the underlying drivers of these phenomena and ways to strengthen digital resilience, the report proposes several recommendations for action.

The explosive growth of digital connectivity across Central Asia is steadily increasing the presence and influence of violent extremist groups. Even before the onset of COVID-19, most Central Asian governments were committed to scaling-up digital transformation, including extending digital services and broadband internet access. The rapid onboarding of citizens, including vulnerable communities, and rising social media use have expanded the potential audience at risk. Without adequate online protective measures and investment in digital resilience - the ability of governments, businesses and civil societies to anticipate, understand, cope with, adapt to and bounce back from digital threats - the diversity and intensity of online harms will likely increase across the region.

> The explosive growth of digital connectivity across Central Asia is steadily increasing the presence and influence of violent extremist groups.

Two popular services - Telegram and Instagram - were vastly more widely used for distributing violent extremist content than Facebook, Twitter, Youtube or Russian-language platforms.

Efforts to disrupt digital threats requires an informed understanding of the challenge. A small number of extremist actors in Central Asia are responsible for a disproportionate share of online extremist content. SecDev Group identified 1,275 active and dormant channels featuring extremist content across 9 social media platforms in the latter half of 2020. At least 716 of these channels are overseen by 13 international and regional jihadist groups. Yet just three violent extremist groups - Islamic State (IS), Hayat Tahrir al-Sham (HTS) and Tavhid va Jihod Katibasi (TJK) - contribute over 77 percent of all active and blocked channels and 70 percent of all channels.

Some social media platforms are more at risk of being abused by violent extremism than others. Throughout 2020, two popular services - Telegram and Instagram - were vastly more widely used for distributing violent extremist content than Facebook, Twitter, Youtube or Russian-language platforms like VKontakte and Odnoklassniki. Roughly 72 percent of all the active and blocked channels and 59 percent of the subscriptions monitored by SecDev Group featuring extremist content were connected to Telegram. Faced with aggressive take-downs and increased surveillance, many violent extremist groups are experimenting with a range of smaller platforms, as well as video-sharing services such as TikTok.

Crucially, violent extremist groups are reaching much wider audiences across Central Asia by engaging third party networks and communities of interest. One of the ways in which the diverse ecosystem of extremist groups are gaining significant exposure is by embedding less objectionable, but nevertheless extremist, content into third party networks and communities of interests. By linking extremist narratives to more moderate channels and posts and making it harder to police offending content, these groups are exhibiting an effective adaptation strategy. In this way, extremist content reached an estimated 5.5 million subscriptions by the end of 2020.

Violent extremist groups have a tendency to “internationalize” their online radicalization efforts. For example, narratives of Muslim oppression in China or France with calls for jihadism are commonplace. Likewise, the glorification of terrorist violence against infidels in conflicts throughout Afghanistan, Iraq and especially Syria are also widespread. More recently, narratives are also leveraging perceived injustices occurring within Central Asia proper. Sources of grievance include allegations of failed democratic governance, the spread of western values, the dubious motives of moderate political and religious leaders, and opposition to Sharia and extending rights to Muslims.

There are multiple risk factors exacerbating the onset, spread and intensity of online harms, including violent extremism. These include:

- the COVID-19 pandemic and lockdown measures;
- digital connectivity and dependence;
- the expansion of addressable online audiences;

- the vulnerabilities of smaller local language groups;
- the limited availability of trusted moderate religious content;
- the lack of free and independent media; and
- weak digital civic engagement and an unchecked social media ecosystem that spreads dangerous content.

More positively, there are several ways in which governments, societies and individuals are protecting themselves from online threats, including by designing-in and reinforcing digital resilience. In this way, they are strengthening their ability to recognize, cope with, adapt to and bounce back from online harms. Most approaches involve some combination of:

- the mobilization of progressive and independent communications;
- enhancing access to more reliable and diverse content;
- and expanding opportunities for inclusive and authentic online participation in decision-making.

As it is, ongoing government and platform-led efforts to take-down violent extremist content are delivering limited results. Across Central Asia, Jihadist-Salafist groups have proven to be highly adaptive to efforts to remove content. While visible profiles and posts of known violent extremists are routinely eliminated, content often re-appears under new identities and across new platforms. There are signs that extremist groups are exceedingly adept at shifting their approaches to reaching audiences in multiple languages even in a context of aggressive crackdowns.

Governments across the region have often taken a hard-line stance against radicalization - both online and offline. Regulatory frameworks typically borrow from international and regional best practices, especially from Russia. Once perpetrators are identified, police and judicial action can be swift. In Kazakhstan, fines may be issued for posting “extremist” content. In Tajikistan, merely liking or sharing a post with terrorist content could recently lead to 15 years in prison. A blanket punitive and deterrence-based approach may not be the most effective, particularly as it is itself fueling frustration and resentment.

At the same time, governments across the region are testing out a wide range of programs to prevent and counter violent extremism. Their action plans often combine operational, preventive and communication measures focusing on the population at large, as well as vulnerable groups such as youth, migrants, prison inmates, former extremists and other categories of the population. Many of these national plans are coming to the end of their life cycles and will likely undergo a process of renewal. This represents an opportunity to rethink strategies based on available data and evidence of where the challenges are, and what works.

> Ongoing government and platform-led efforts to take-down violent extremist content are delivering limited results.

Governments across the region are testing out a wide range of programs to prevent and counter violent extremism.

Governments must start planning the next generation of online harm reduction strategies immediately. New plans and programs must be more focused on current and future challenges. This means shifting from a narrow punitive focus on countering/preventing violent extremism toward addressing a broader spectrum of digital harms. Central Asian governments should develop a diversified portfolio of interventions that promote higher quality digital engagement. They will also need to revisit the consequences of only relying on intermediary liability and extra-judicial blocking regulations on freedom of expression and privacy, not least since this can unintentionally aggravate violent extremist activity.

Social media platforms also need to step up their engagement in Central Asia. There are several ways in which platforms minimize exposure to online violent extremism and reduce the threat of online harms. Priorities include taking coordinated action to improve the durability of take-downs over the long term; investing in behavioral change strategies to improve digital hygiene; and revisiting content personalization algorithms that facilitate the spread of violent extremist content. There are also real opportunities for platforms to assist in pushing out more independent and local language news to help users verify false narratives.

There are also many encouraging opportunities for civil society, media and academic groups to support measures to reduce the risks of online violent extremism and enhance digital resilience. Examples include entering into collaborative efforts at the regional and national level to address high-impact radical narratives. Strengthening the availability and reach of independent media, in coordination with platforms, is another priority. So too are strategies that enhance media and digital literacy, countering misinformation, enhancing digital safety, and strengthening digital inclusion programs that reinforce values of tolerance and diversity, especially in ways that benefit the most vulnerable groups.

Introduction

Central Asia is undergoing rapid digital transformation. Over the past decade, the region's five republics — Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan — have experienced a rapid growth in high-speed fiber connections, mobile phones, and social media, with online services and tech hubs proliferating. Yet the internet and social media are dual-edged: As more Central Asians get online, they are being exposed to sophisticated extremist content in their native languages—and facing risks of a wide array of online harms.

A variety of global and home-grown jihadist movements have secured a foothold in the region. Even in the less digitized past, when extremist ideas spread mostly through CDs, cassettes and books, Central Asian governments struggled to prevent several thousand fighters from the region joining campaigns in war-torn Afghanistan, Iraq, and Syria. Today Central Asians - and extremists networks - have migrated online. Central Asia's new generation of digital extremists are working on fertile soil. They can target huge youthful populations facing dim educational opportunities, limited job prospects, and little social mobility.

What unites Central Asia's ideologically disparate extremist factions is their reliance on social media to reach out to followers and sympathizers. Throughout June-November 2020 SecDev identified almost over 700 separate channels used by 13 extremist organizations on over 9 platforms including Telegram, Facebook, Instagram, Twitter, Youtube and the popular Russian platforms VKontakte and Odnoklassniki. Many of the channels and subscriptions used Russian, the region's lingua franca, but also Uzbek, Tajik and Kyrgyz. Some extremist groups are inevitably more digitally active than others.

Governments, internet providers, and social media companies are struggling to contain this torrent of violent content. The conundrum is familiar: As soon as a social media channel or account is blocked, new ones pop up again—ad infinitum. And the more these efforts at content control are ramped up, the more violent extremist groups discover creative ways to bypass and circumvent them. Years of playing cat-and-mouse with the foreign and domestic governments have turned Central Asia's extremist groups into experienced and agile online operators.

Given these challenges, tackling digital radicalization cannot be achieved through online operations alone. On-the-ground investments by governments, platforms and civil society groups are key. Based on extensive online research, the first section of this report examines the scope and scale of online harms generated by extremist groups in Central Asia. Section two examines the form and dynamics of extremist narratives across the region. The third section reviews the uneven responses to the challenge, while sections four and five consider risk and resilience factors. The final section considers recommendations for governments, social media companies and non-governmental organizations to strengthen digital resilience in the region.

How we map violent extremist content online

SecDev conducts ***open-source research*** *across social media platforms in order to identify content produced and disseminated by known terrorist and violent extremist organizations involved in violating platform community standards. SecDev is particularly interested in (i) threats and acts of violence; (ii) hate speech; (iii) depictions of graphic violence; (iv) calls for terrorist financing and/or recruitment; and (v) terrorist propaganda.*

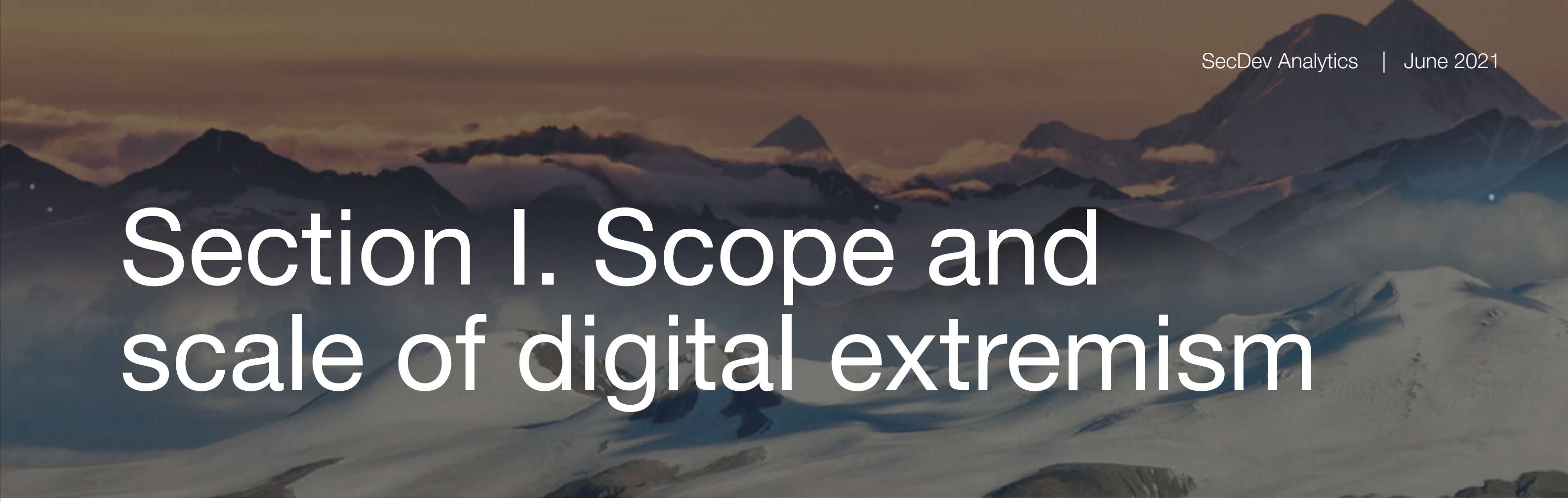
Publicly accessible social media outlets (such as Telegram and Youtube channels, Twitter and Instagram accounts and Facebook pages, profiles and groups) featuring violent extremist content are identified through multilingual keyword searches and analysis. To be included, channels must exhibit a demonstrated connection to Central Asia, by posting content in the region's main languages that is targeted to the digital audiences in and from the region.

Monitoring occurs at two levels:

Channel-level analysis: *Weekly and monthly assessment of social media channels operated by the violent extremist and terrorist organizations, as well as third-party channels with cross-referenced content. Data collection is focused on group affiliation, platform, language, and available data on subscriptions and status (active, inactive, blocked).*

Narrative analysis: *Daily monitoring of the 60 most active channels that involves content classification of all published posts under main categories (violent extremist, extremist and neutral content), sub-categories and linkages to key events and topics of regional importance. For a sub-set of posts, user interaction analysis is conducted, based on available data on views and user reactions.*

SecDev applies a ***public health approach*** *to the collection and analysis of online data. This approach focuses on identifying risk and protective factors associated with violent extremism and prioritizes prevention. It also entails a "do no intentional harm" approach, including the safeguarding of user privacy and safety. For instance, SecDev does not record or retain subscriber account information.*



Section I. Scope and scale of digital extremism

Central Asian social media users are exposed to a modest, but persistent, evolving and adaptive ecosystem of violent extremist content. In the latter half of 2020, SecDev detected 1,275 channels featuring extremist content across 9 social media platforms (Figure 1). Well-known designated violent extremist organizations play a dominant role in disseminating content. At least 716 of these channels are overseen by 13 Jihadist groups.[1] After accounting for takedowns, there were 201 active channels as of December 2020 with some 140,000 subscriptions. Another 320 channels were dormant, albeit accessible, and serving as a kind of "reserve capacity" in the event of takedowns and distributed content repositories for recruitment.

A comparatively small number of organizations are behind the vast majority of violent extremist content on social media. At least 77 percent of all monitored active and blocked channels and 70 percent of subscriptions were operated by just three groups - IS, HTS and TJK (Figure 2). These also happen to be the largest terrorist organizations with interest in the region, and the most well prepared to allocate the necessary resources to ensure an extensive social media profile. These groups can achieve a cross-platform presence in multiple languages, including lesser known sites with lower levels of violent extremist content circulation. Meanwhile, smaller groups such as AD, JAN and KIB are for the most part visible on Telegram.

Figure 1. Channels and subscriptions by violent extremist groups and third-party actors

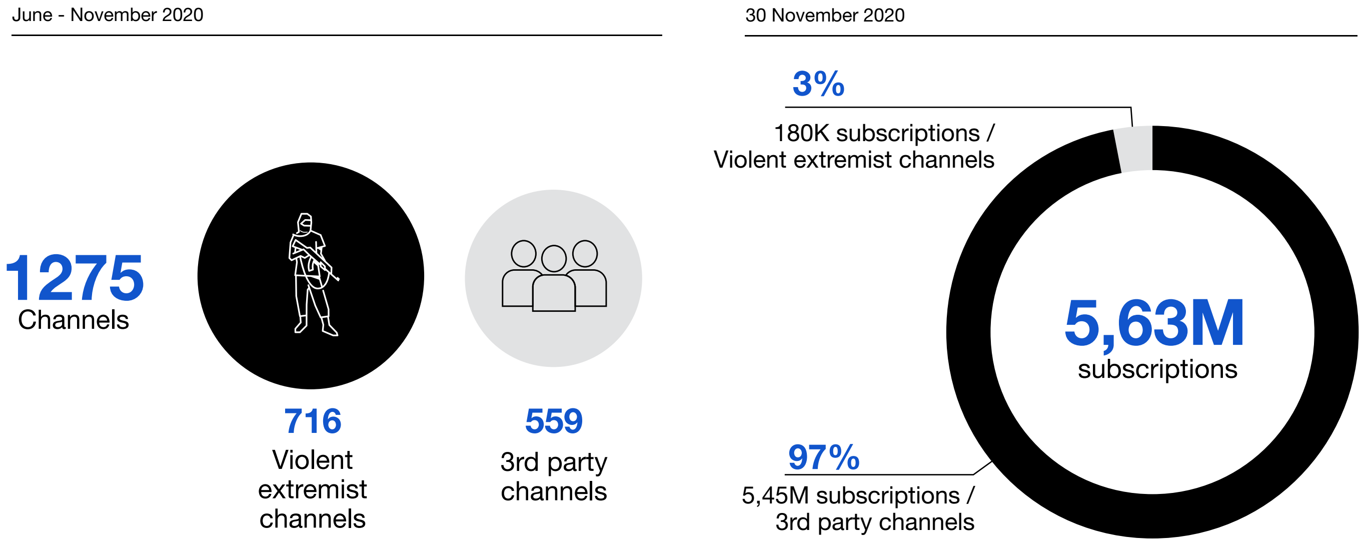
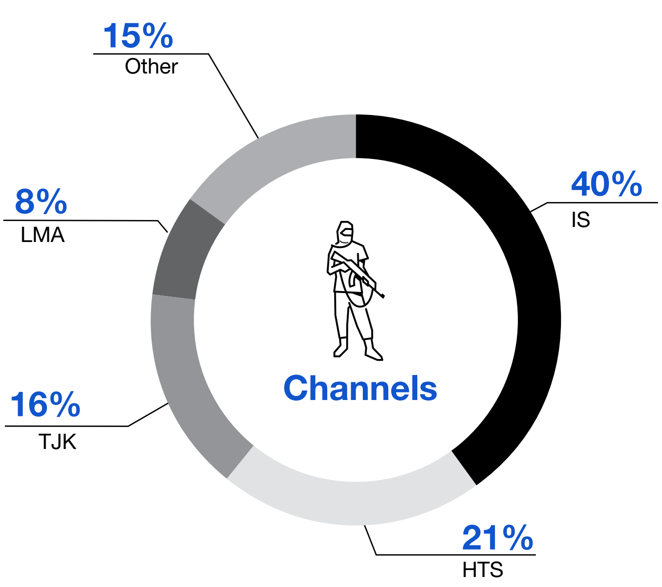
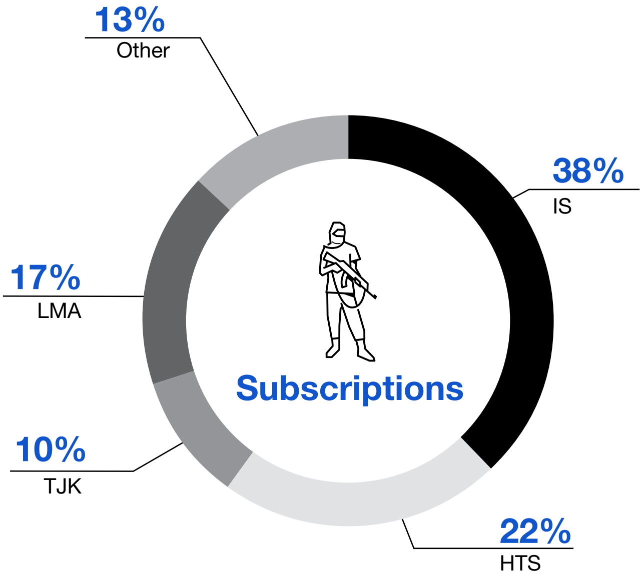


Figure 2. Distribution channels and subscriptions by violent extremist group



396 active and blocked Violent extremist's channels (June-November 2020)

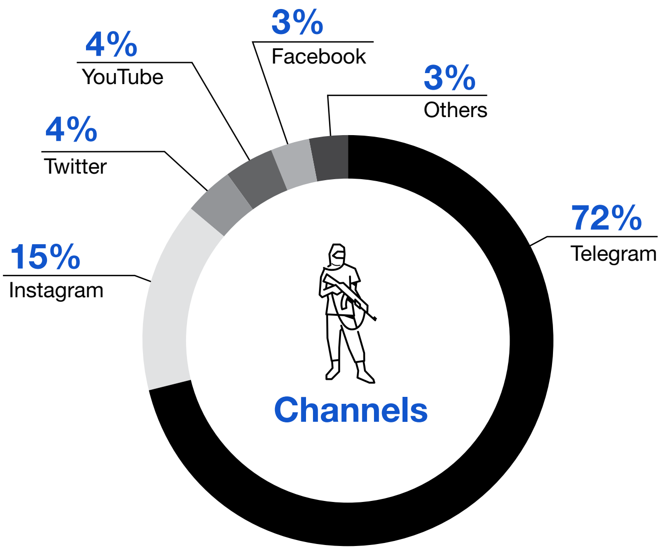


201 active Violent extremist's channels (30 November 2020)

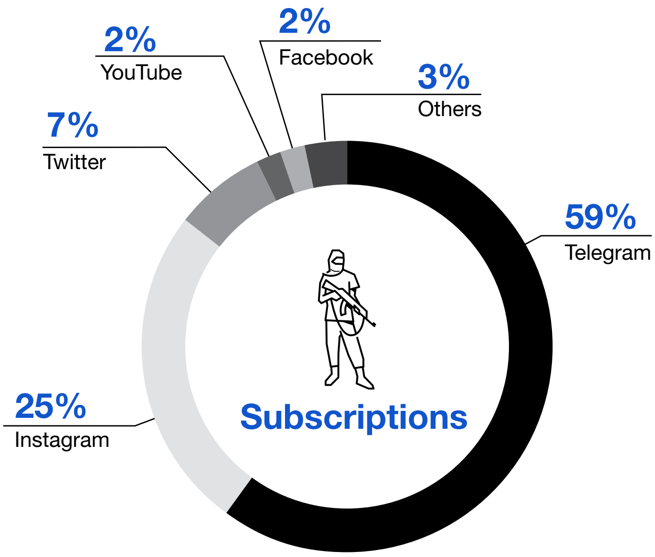
Even more worrisome than online harms spread directly by hardcore radical actors, is the amplification of extremist content by third party channels and communities of interest. Throughout the second half of 2020, SecDev identified 559 third party and community of interest channels reaching a combined audience of 5.5 million subscriptions. By December 2020, SecDev detected 271 active third party channels with 5 million subscriptions and another 254 channels turned dormant. At least 34 third-party channels were taken down during the reporting period. For the most part, it is large groups such as IS, HTS and TJK that are best positioned to penetrate third-party networks. Not only are the effects of such cross-posting dangerous, they are also extremely difficult to police, much less moderate.

Some platforms - especially Telegram and to a lesser extent Instagram - are more popular for distributing extremist content than others. Approximately 72 percent of all the active and blocked channels and 59 percent of the subscriptions monitored by SecDev and featuring extremist content were connected to Telegram (Figures 3 and 4). Telegram is especially popular because of how it affords anonymity and the ease with which users can set-up new channels. Meanwhile, Instagram made up 15 percent of the channels and 25 percent of the subscriptions tracked by SecDev. Other social media platforms are far less popular, accounting for the remaining 13 percent of channels and 16 percent of subscriptions.

Figure 3. Violent extremist channels and subscriptions by platform



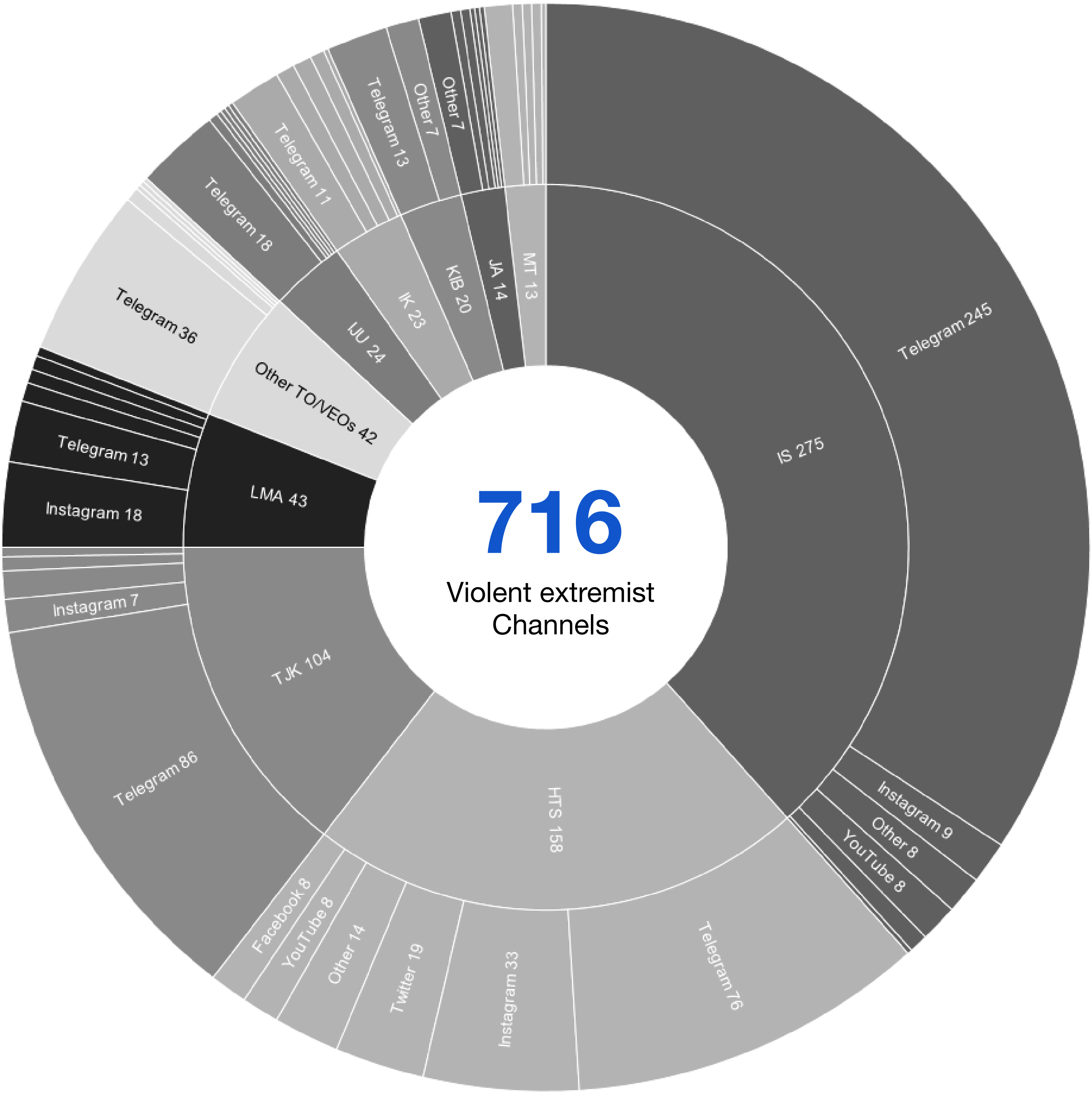
396 active and blocked Violent extremist's channels
(June-November 2020)



201 active Violent extremist's channels
(30 November 2020)

Even so, there is evidence that Jihadist groups are routinely experimenting with newer or alternative platforms, even if their influence is potentially more limited. Platforms such as TamTam, Hoop, SoundCloud, VK and OK account for just 46 channels, the vast majority of which were dormant during 2020.[2] There are also signs that violent extremist groups are expanding their presence on TikTok, a relatively new and increasingly popular arrival to Central Asia. A preliminary assessment of violent extremist activity on this latter platform in late 2020 revealed at least 12 channels associated with known groups such as HTS, IS, TJK, LMA and IK.

Figure 4. Violent extremist ecosystem: channels by group and platform (June-November 2020).

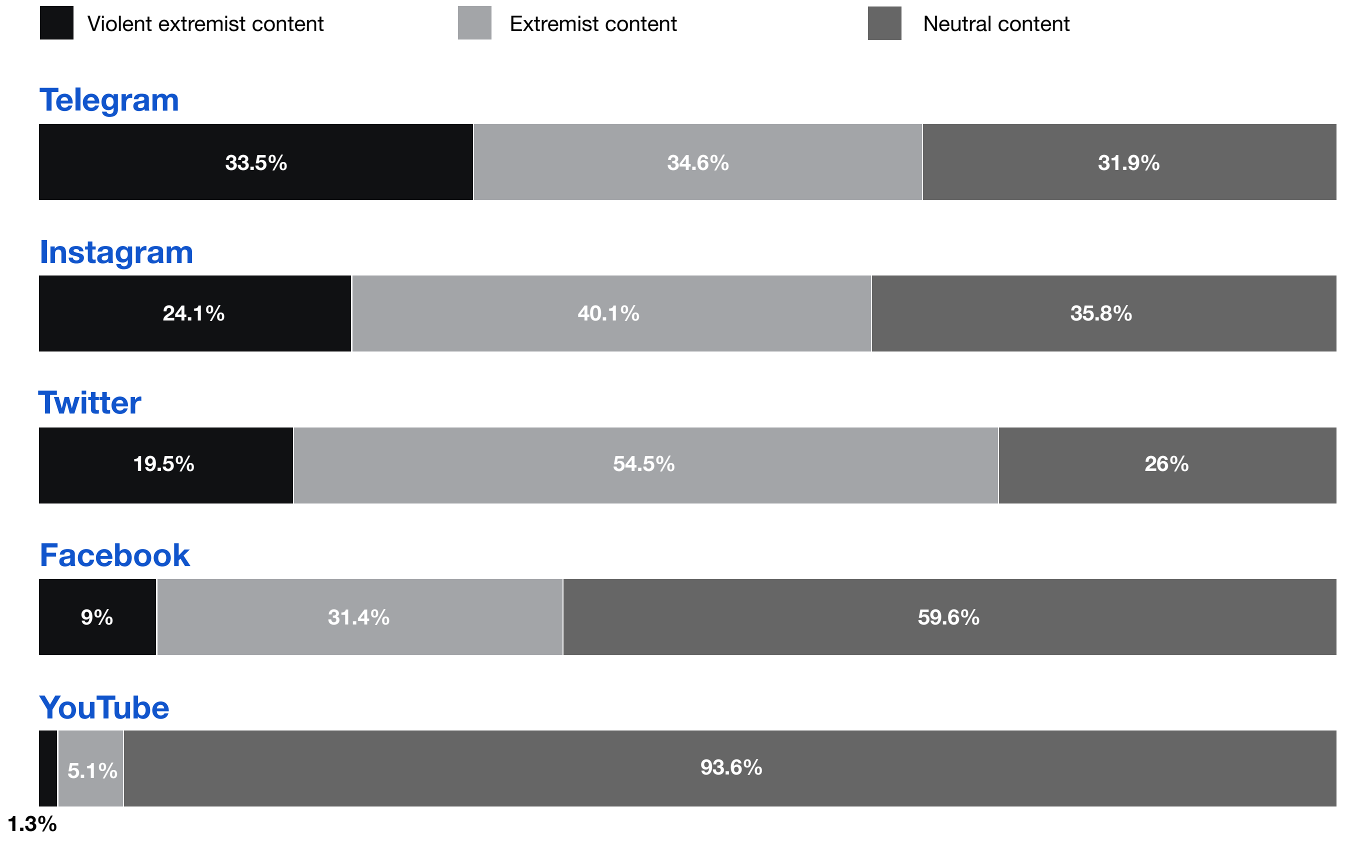


TO/VEO	Platform	Channels
IS 275	Facebook 1	1
IS 275	Instagram 9	9
IS 275	Telegram 245	245
IS 275	Twitter 4	4
IS 275	YouTube 8	8
IS 275	Other 8	8
HTS 158	Facebook 8	8
HTS 158	Instagram 33	33
HTS 158	Telegram 76	76
HTS 158	Twitter 19	19
HTS 158	YouTube 8	8
HTS 158	Other 14	14
TJK 104	Facebook 2	2
TJK 104	Instagram 7	7
TJK 104	Telegram 86	86
TJK 104	YouTube 3	3
TJK 104	Other 6	6
LMA 43	Facebook 3	3
LMA 43	Instagram 18	18
LMA 43	Telegram 13	13
LMA 43	Twitter 4	4
LMA 43	YouTube 2	2
LMA 43	Other 3	3
Other TO/ VEOs 42	Instagram 1	1
Other TO/ VEOs 42	Telegram 36	36
Other TO/ VEOs 42	Twitter 1	1
Other TO/ VEOs 42	YouTube 3	3
Other TO/ VEOs 42	Other 1	1
IK 23	Instagram 4	4
IK 23	Telegram 11	11
IK 23	Twitter 4	4
IK 23	YouTube 3	3
IK 23	Other 1	1
IJU 24	Facebook	1
IJU 24	Instagram	1
IJU 24	Telegram 18	18
IJU 24	Twitter	2
IJU 24	YouTube	1
IJU 24	Other	1
JA 14	Facebook	1
JA 14	Instagram	2
JA 14	Telegram	2
JA 14	Twitter	1
JA 14	YouTube	1
JA 14	Other 7	7
MT 13	Facebook	2
MT 13	Instagram	2
MT 13	Telegram 6	6
MT 13	Twitter	1
MT 13	Other	2
KIB 20	Telegram 13	13
KIB 20	Other 7	7

Section II. Rise and spread of extremist narratives

Social media accounts with violent extremist content typically feature a combination of both neutral and extremist material. A review of the most active 60 violent extremist and third-party channels between June and November 2020 yielded a sample of 28,500 posts. SecDev classified the material into three broad categories: violent extremist, extremist and neutral. Overall, just 30 percent of the posts included violent extremist content followed by an equal share of the other two categories (about 35%). Neutral content, which typically included general news and religious content, plays an essential role in enabling channels to evade content moderation, while also attracting and retaining larger and more diverse audiences. It is important to underline that the extent of extremist content varies from platform to platform. The relative share of violent extremist content was highest on Telegram and Instagram and close to non-existent on Facebook and Youtube (Figure 5).

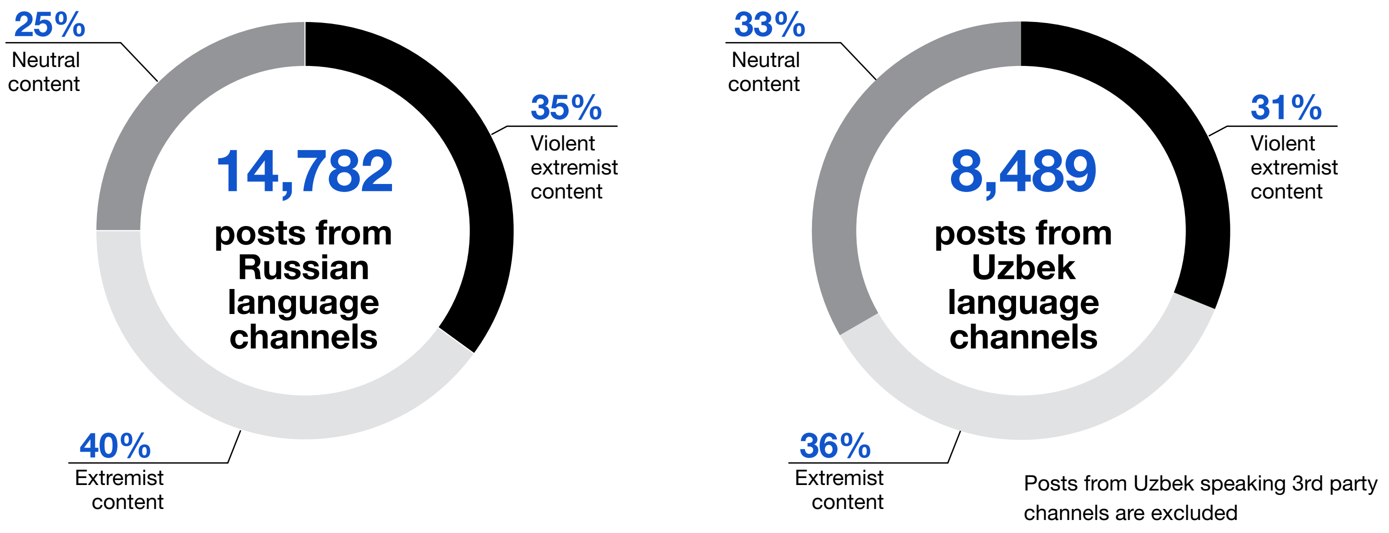
Figure 5. Distribution of posts by type of narrative



Across all monitored channels run by extremist actors, Russian is the lingua franca. Close to one third of the sample of violent extremist active, blocked and dormant channels under review were in Russian, along with 80 percent of all subscriptions. By contrast Uzbek, the second largest language community in Central Asia, with over 30 million speakers, is used by less than a third of all channels and constitutes just 15 percent of all subscriptions. Meanwhile, Tajik, spoken by at least 8 million Central Asians, along with Kazakh and Kyrgyz, is only weakly represented among monitored extremist channels and subscriptions.

There are noticeable differences between Russian and Uzbek language posts (Figure 6). For one, Uzbek language posts from violent extremist channels tend to exhibit a lower share of violent extremist content and more neutral content than their Russian equivalents. These differences may be due to the fact that Uzbek language channels tend to publish more neutral religious-themed content. This compares to Russian language channels that frequently disseminate more critical narratives classified as “extremist” such as the perceived global oppression of Muslims and criticism of governments across the region.

Figure 6. Russian versus Uzbek language channels

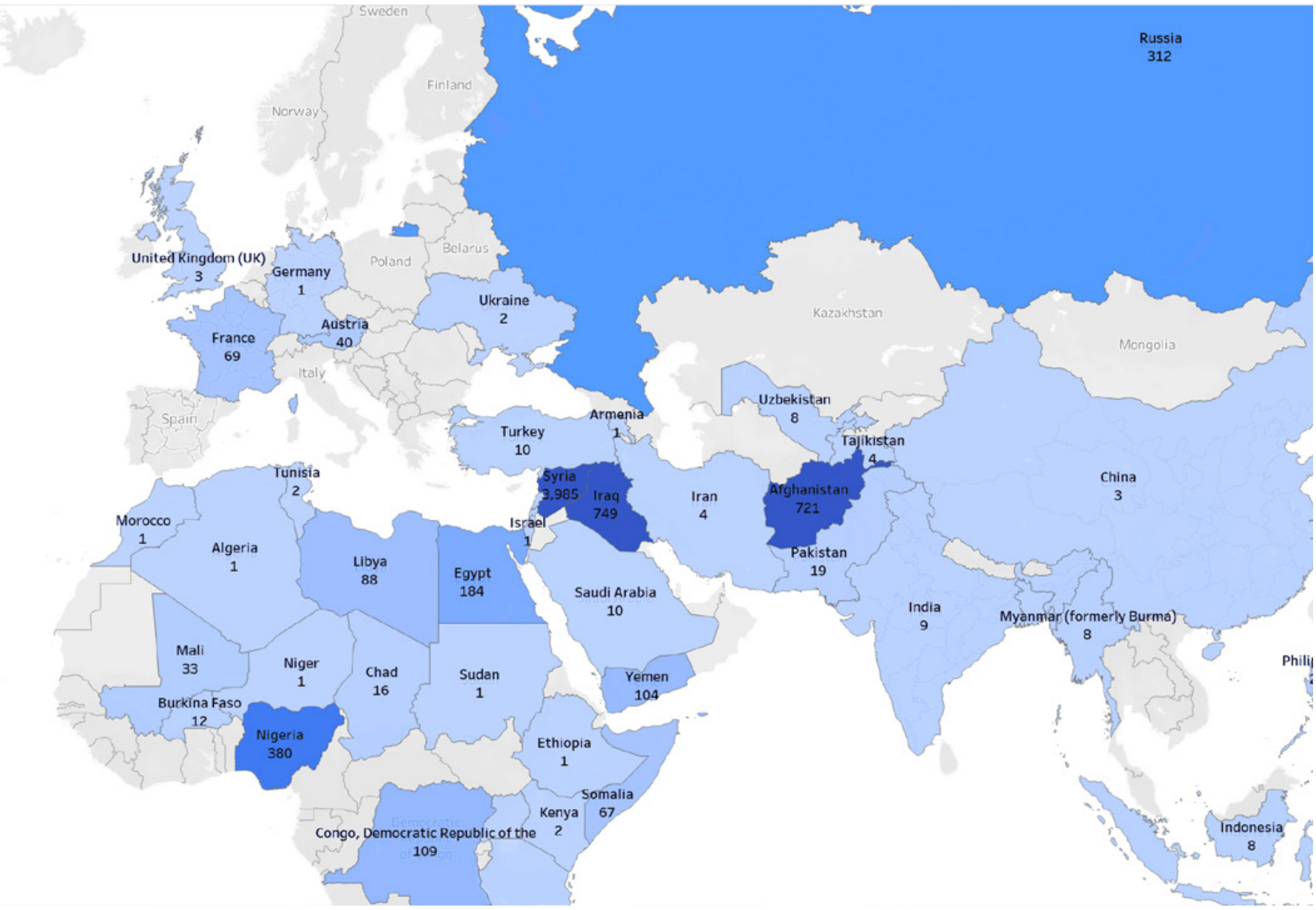


Posts from Uzbek speaking 3rd party channels are excluded

A small number of extremist groups were responsible for a disproportionate share of violent extremist content. Of the aforementioned sample, HTS, IS and TJK published three quarters of all posts. Specifically, HTS published about 10,000 posts, IS published roughly 7,000 and TJK produced approximately 4,000. Slightly more than half of all IS posts were “violent extremist” in nature as compared to 25 and 22 percent for HTS and TJK respectively. As for the content of their messages, there is a combination of extreme political, ideological and religious propaganda (21 percent), threats of violence (17 percent), justification of Jihad linked to narratives of Muslim oppression (12 percent) and active incitement of terrorism (10 percent).

There is a tendency for violent extremist narratives to “internationalize” calls for action. While target audiences in Central Asia are urged to join the ranks of jihadist movements, many of the underlying justifications continue to be linked to “global” events. Specifically, online depictions of terrorism and organized violence are routinely connected to active conflicts in Afghanistan, Iraq and especially Syria (Figure 7). There are very occasional references to local dynamics involving arrests of violent extremists, including in, for example, Uzbekistan (8 posts) or Tajikistan (4). By contrast, there is a more frequent reference to Russia (312 posts) or France (69 posts) on violent extremist channels.

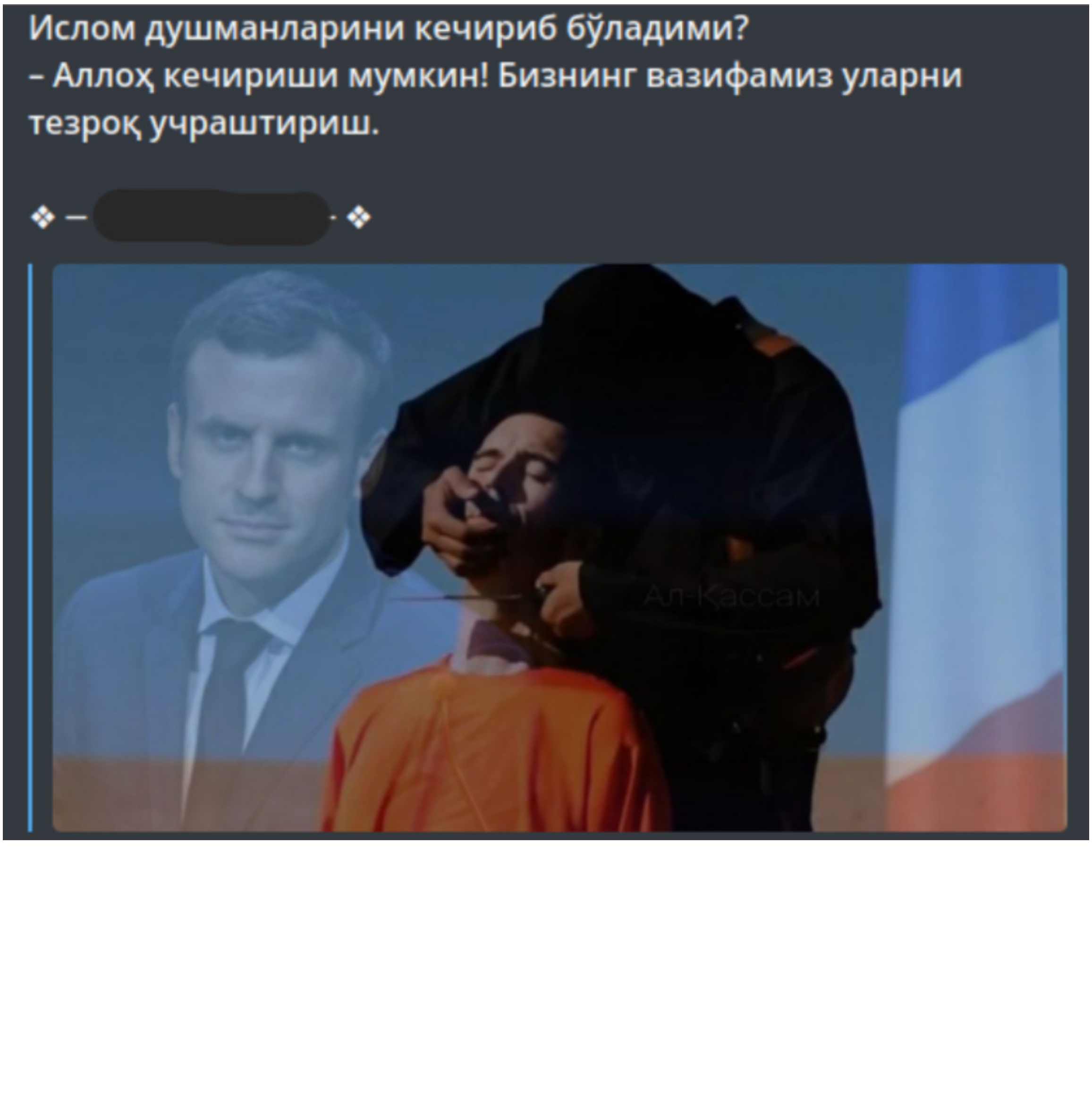
Figure 7. References to specific countries in extremist channels



There is evidence that extremist narratives seek to generate engagement by addressing perceived injustices occurring both in and outside Central Asia. Common themes include the failures of democratic governance, attacks on democratic values, the limited credibility of moderate political and religious leaders, oppression against Muslims and calls for Sharia. SecDev detected over 194 posts on such themes from Uzbekistan and 22 in Kyrgyzstan during the reporting period. This is in contrast to 547 posts focused on grievances in Russia, 208 from Afghanistan and 102 from Turkey.

Narratives propagated by hardline violent extremist actors appear to have comparatively limited impact on mainstream digital discourse, with the notable exception of religious content. One of the reasons for this is that the actual number of violent extremist channels detected on Facebook, Youtube, Twitter and other popular platforms is low. What's more, owing to a combination of aggressive platform policing and law enforcement, extremist content oriented toward Jihadism is even more rare.

Figure 8. Telegram post from a religious channel that reads: "Is it possible to forgive the enemies of Islam? - Allah may forgive, but our duty is to arrange the meeting with Allah [kill]". (October 26, 2020)



Ислом душманларини кечириб бўладими?
– Аллоҳ кечириши мумкин! Бизнинг вазифамиз уларни тезроқ учраштириш.

❖ – [redacted] · ❖

Yet there is potentially an exception with respect to the cross-pollination of religious content disseminated through third party channels. SecDev identified a cluster of 100 Uzbek-language social media channels on Facebook, Instagram, Youtube and Telegram that may serve as an amplifier network for content from violent extremist actors. Analogous clusters of religious channels exist in Russian and Tajik languages. The Uzbek language cluster features sermons from prominent (moderate) clerics and content related to prayers, Quranic readings and fasting during Ramadan. It reaches a combined audience of 2 million subscriptions. While the vast majority of content is not extremist, roughly three per cent including calls to join Jihad and extremist narratives that weaponize references to Muslim oppression.[3] One typical example of such content is presented in Figure 8.

There is evidence that more violent extremist and extremist content tends to generate more user engagement than neutral content. A review of a subset of Telegram channels and posts[4] determined that extremist narratives generated on average the most views (505) followed by violent extremist narratives (453) and neutral content (431). When controlling for the number of subscriptions, the views-to-subscriptions ratio for violent extremist and extremist content was 78 percent and 84 percent respectively, while the ratio for neutral content was 61 percent.

SecDev identified a cluster of 100 Uzbek-language social media channels on Facebook, Instagram, Youtube and Telegram that may serve as an amplifier network for content from violent extremist actors.

Notwithstanding the presence of violent extremist content across mainstream religious channels, its direct influence on offline activity appears to be limited. Social media propaganda is of course just one tactic of many used by extremist movements. What is more, violent extremist content is rarely the determinant independent variable shaping real world behavior. To this end, SecDev did not generate any conclusive evidence that specific offline incidents were influenced by specific radical narratives in the public space. Indeed, none of the major incidents occurring during the reporting period - including the unrest in Kyrgyzstan following the October parliamentary elections - appeared to be preceded by a surge in online violent extremist activity.

Section III. Uneven responses to online harms

Social media platforms have struggled to minimize online harms. All major companies are taking measures to identify and remove content that violates their policies, applying a combination of automated detecting, user reporting, and moderator reviews. SecDev found that platforms successfully removed 195 active and inactive channels overseen by violent extremist groups such as IS, HTS and TJK. This represents roughly 27 percent of all violent extremist channels monitored over the second half of 2020.[5] The most common takedowns were of Telegram and Instagram channels, followed by Facebook, Twitter and Youtube.[6] Yet at the same time as take-downs were occurring, violent extremist groups created 270 new channels, which means that by the end of 2020, there were 201 active channels with some 138,000 subscriptions (see Figures 9-11).

Figure 9. Effect of takedowns on violent extremist channels and subscriptions

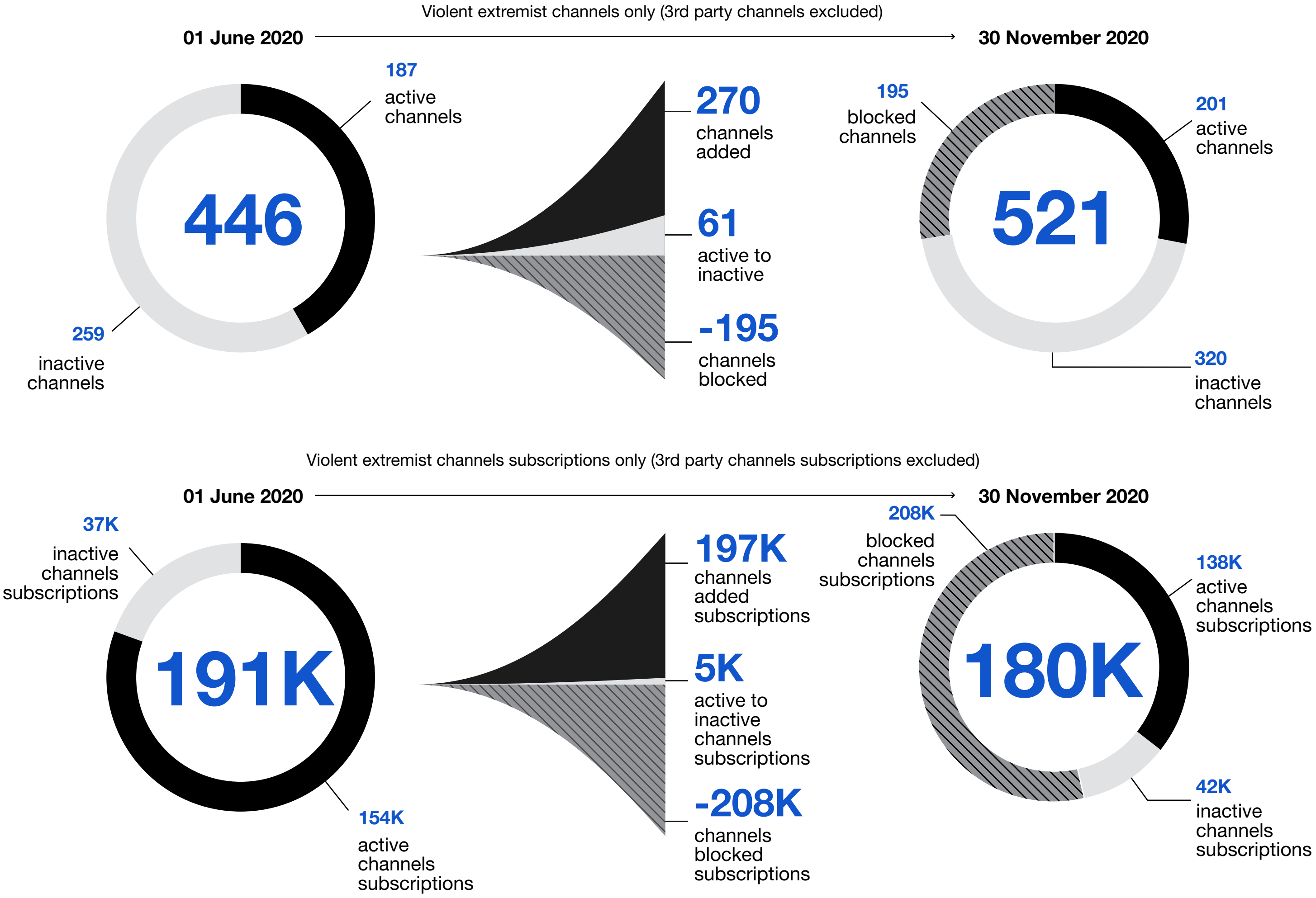


Figure 10. Weekly dynamics of channel takedowns and re-emergence, June-November 2020

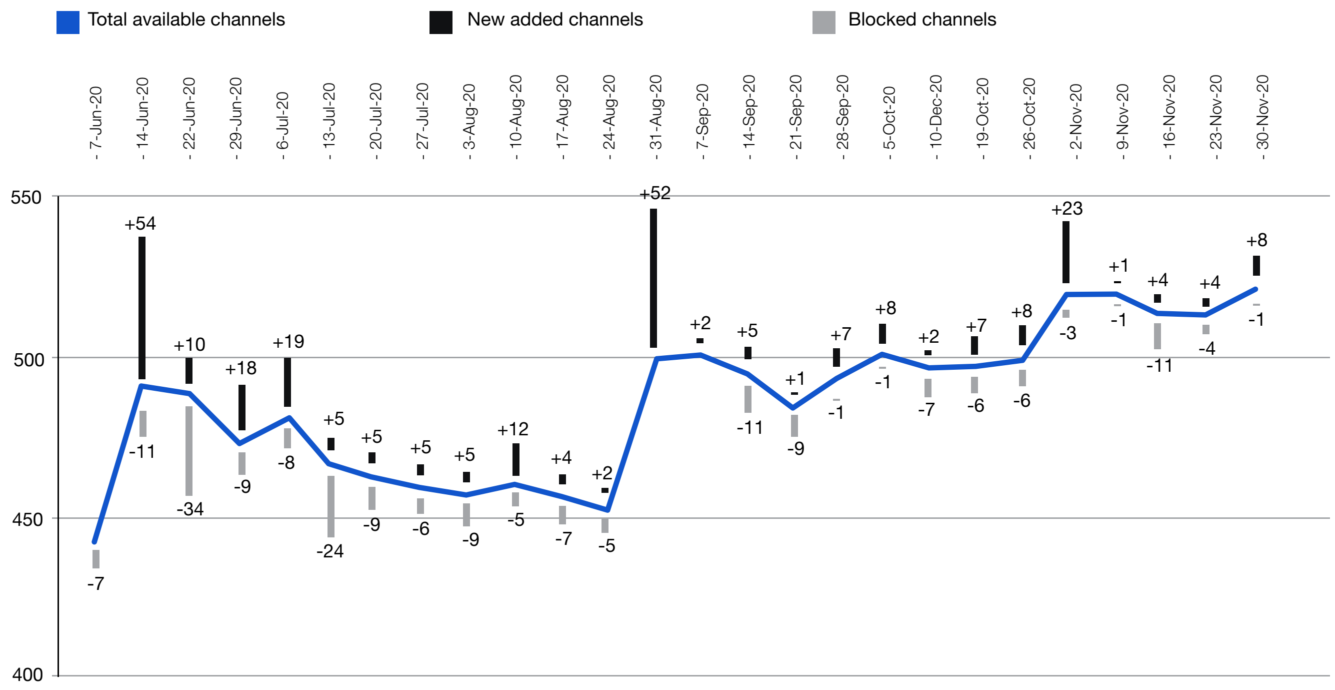
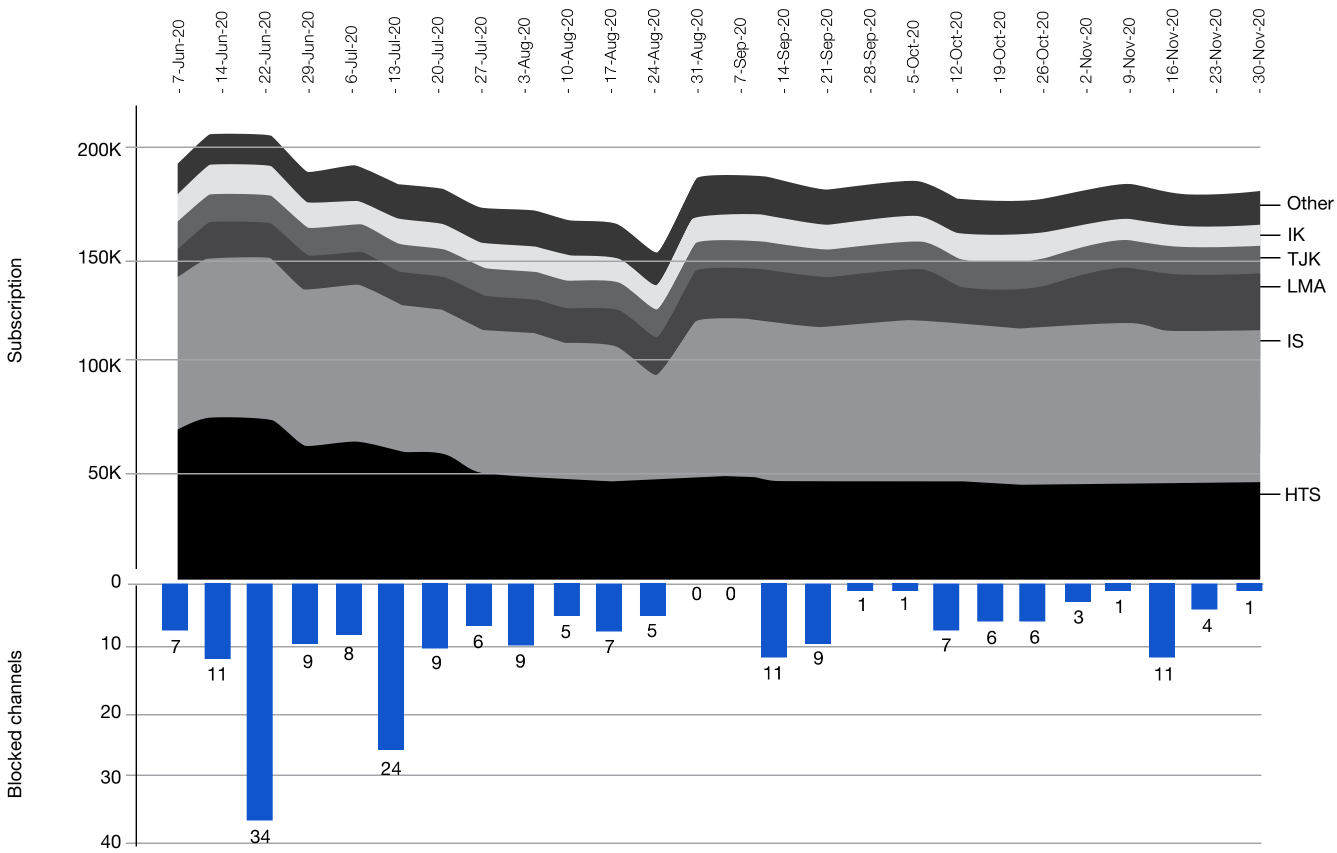


Figure 11. Effect of takedowns on major violent extremist groups, June-November 2020



Central Asian governments have enacted a range of penalties for sharing violent extremist content online.

Even so, takedowns help shorten the longevity of violent extremist channels and limit their ability to attract large following. SecDev determined that the average life-span of violent extremist channels under observation was between 3.5 and 4 months from their period of creation to their removal. In general, Instagram was quickest to react with a mean response time of 104 days, as compared to 154 days for Facebook and 208 days for other platforms. Meanwhile, Youtube (125), Telegram (128) and Twitter (143) were in the middle of the pack.

There are slight differences between Russian and Uzbek language channels in terms of how long they remain online (126 and 123 days, respectively). However, a sample of Kyrgyz and Tajik language channels demonstrated a longer lifespan - some 319 and 197 days respectively - most likely due to more limited monitoring and fewer user complaints. In general, the more active the violent extremist group, the more posts get flagged and the shorter the lifespan. IS channels exhibit a median lifespan of 93 days, HTS roughly 104 days and TJK some 128 days.

For their part, Central Asian governments have enacted a range of penalties for sharing violent extremist content online. At one end of the continuum are administrative measures, such as in Kazakhstan that issues fines of up to $450 for posting audio and images classified as “extremist”.[7] At the other end is prison sentences, such as in Tajikistan, where even “liking” a post with terrorist content was at one point punishable by up to 15 years in prison.[8] These risks are often singled out on platforms themselves. To wit, on its Telegram channel, Uzbekistan’s Ministry of Interior warned social media users of the penalties associated with sharing violent extremist content of a religious nature in the “Uzbek segment” of social media.[9]

Central Asian governments have also taken pre-emptive action to deter the offline activities of violent extremist movements. The case of TJK, a prominent movement that has steadily grown its online presence, stands out. Throughout 2020, TJK affiliates have been arrested. Among those reported in the media are an alleged recruiter in Uzbekistan accused of sending followers to Syria; 25 supposed TJK members and followers in Tashkent, the capital of Uzbekistan; a suspected 15-member cell of would-be TJK members in southern Uzbekistan; and arrests of suspected TJK members across Russia.[10]

Most Central Asian countries have initiated comprehensive programs to counter violent extremism. They typically combine offline operational, preventive and communication-oriented measures with the goal of minimizing risks to the general population and honing in on particular segments deemed to be “at-risk” or “vulnerable” to radicalization. Strategies also frequently include active monitoring of social media, blocking access to violent extremist content, public awareness campaigns, training in media and digital literacy, as well as online counter messaging and promotion of alternative narratives.

A common strategy to prevent online harms is to police and block offending content. For example, the Kazakhstan authorities removed 21,000 extremist resources and blocked over 200 links to offending content in 2020.[11] Yet there are real concerns about such blocking measures, since they can be conducted lawfully, but also extrajudicially for ostensibly political ends. In Kazakhstan, rules designed to ban and block content from extremist groups were applied to one of the opposition political parties.[12] But blanket bans can be incredibly disruptive far beyond the intended target. For example, in Kyrgyzstan, entire online platforms such as Archive.org were blocked, while in Tajikistan, YouTube was temporarily taken down in the name of "fighting extremism".[13]

Initiatives range from imposing intermediary liability to the full-scale regulation of foreign social media presence.

Central Asian governments are increasingly enforcing content moderation on social media and online platforms. Initiatives range from imposing intermediary liability to the full-scale regulation of foreign social media presence. The Uzbek authorities, for instance, may impose penalties on any resources where illicit content is shared through online comments.[14] The Agency for Information and Mass Media can file a lawsuit against entities failing to remove offending comments within 24 hours. Kyrgyzstan is also focusing on the responsibility of online intermediaries, though such efforts have been criticized on the grounds they facilitate online censorship.[15] And Kazakhstan also may more aggressively regulate social media companies - the Ministry of Information and Societal Development circulated draft legislation for a Law on Mass Media in late 2020.[16]

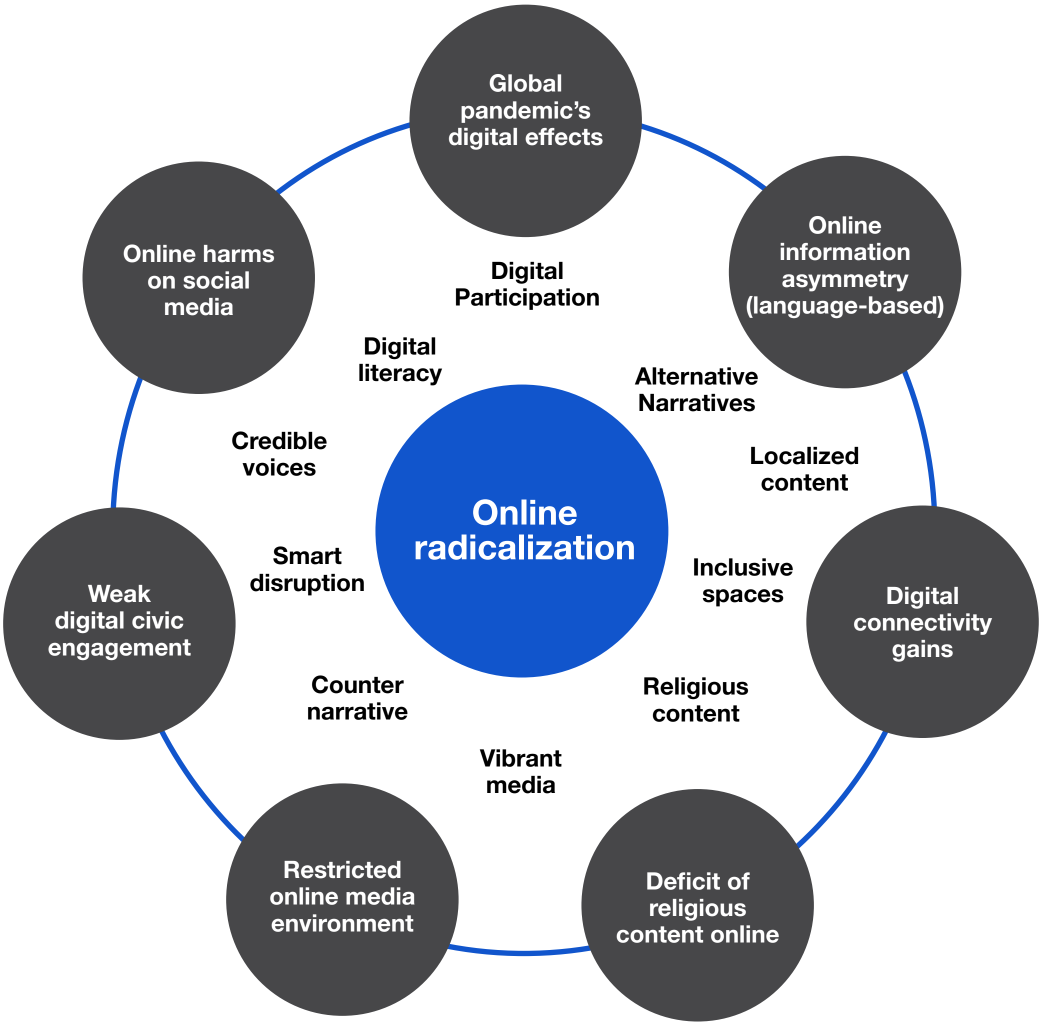
Section IV. Risk and resilience factors

Some Central Asian countries and communities are more susceptible to online violent extremism than others. The reasons why are widely debated, but generally boil down to a combination of risks and the extent of their resilience. These risk and resilience factors shape the real-life changes at the societal, community, interpersonal and individual levels. Efforts to mitigate online harms must depart from a basic understanding of what risks and resilience factors are most prominent and how they can be alternately diminished and amplified. Minimizing the threat of violent extremism and associated digital harms is similar, then, to efforts to control disease and adapt to climate change. Identify the risk factors and minimize them, strengthen the resilience factors, and repeat.

Minimizing risks

While there is accumulating evidence of the underlying risk factors for radicalization, including so-called “push”, “pull” and “trigger” factors, the online dimensions of what drives violent extremism are still under-examined.[17] Ultimately, the onset, spread and intensity of online violent extremism is multifactorial. There is no single or monolithic variable that explains the spread of extremist content. SeDev Group has identified an array of structural and proximate factors, some of them linked to the particular context of Central Asia and others less so (Figure 12). Determining precise attribution is challenging owing to the way these factors are interconnected and mutually reinforcing.

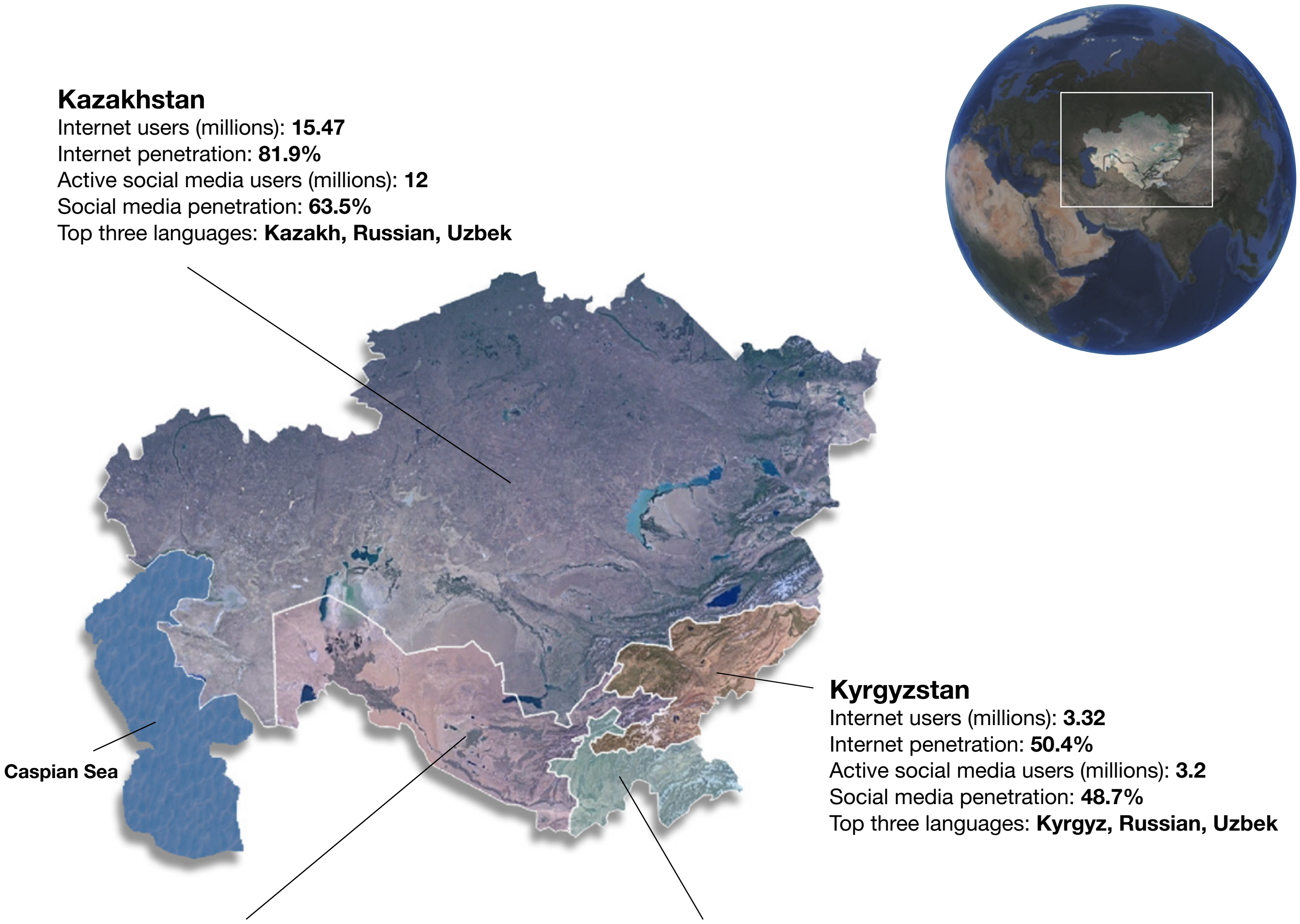
Figure 12. Risk and resilience influencing online radicalization. Outside circles are risk factors and the text inside are the resilience factors.


Global pandemic's digital effects
Online information asymmetry (language-based)
Digital connectivity gains
Deficit of religious content online
Restricted online media environment
Weak digital civic engagement
Online harms on social media
Online radicalization
Digital Participation
Alternative Narratives
Localized content
Inclusive spaces
Religious content
Vibrant media
Counter narrative
Smart disruption
Credible voices
Digital literacy

The **COVID-19 pandemic** and government responses to it increased both the exposure of Central Asians to online content and fueled grievances. Lockdowns and stay-at-home orders resulted in a dramatic onboarding of large numbers of people exposing them to a vast array of online harms, including misinformation, disinformation, hate speech and extremism. As governments struggled to respond, and in some cases over-reacted, frustration and public protests likewise escalated.[18] For their part, violent extremist networks shifted tactics - focusing less on online recruitment and more on promoting conspiratorial and anti-government narratives.[19]

Accelerated digital connectivity and dependence has also accelerated the spread of digital harms (Map 1). Throughout 2020, millions of Central Asians started using the internet - and social media - for the first time. The changes over the past year are dramatic. In January 2020, Kazakhstan, Kyrgyzstan, Uzbekistan and Tajikistan registered a combined active social media population of 16 million.[20] By January 2021, this number rose to 21 million users. The bulk of this growth occurred in Kazakhstan (2.5 million, or 51 percent of total) and Uzbekistan (1.4 million, or 28 percent of the total).[21] More internet and social media growth is expected, especially due to the low penetration rates across the region.[22]

Map 1. Digital dimensions of Central Asia (countries of focus, excludes Turkmenistan).[23]



Kazakhstan
Internet users (millions): **15.47**
Internet penetration: **81.9%**
Active social media users (millions): **12**
Social media penetration: **63.5%**
Top three languages: **Kazakh, Russian, Uzbek**

Kyrgyzstan
Internet users (millions): **3.32**
Internet penetration: **50.4%**
Active social media users (millions): **3.2**
Social media penetration: **48.7%**
Top three languages: **Kyrgyz, Russian, Uzbek**

Uzbekistan
Internet users (millions): **18.67**
Internet penetration: **55.2%**
Active social media users (millions): **4.6**
Social media penetration: **13.6%**
Top three languages: **Uzbek, Russian, Kazakh**

Tajikistan
Internet users (millions): **3.36**
Internet penetration: **34.9%**
Active social media users (millions): **1**
Social media penetration: **10.4%**
Top three languages: **Tajik, Russian, Uzbek**

This has led to a rapid **expansion in the potential addressable audience** for the violent extremist actors. In some countries, weak digital and media literacy, uneven and limited access to independent media and rising grievances could increase the vulnerability of certain user groups to online harms ranging from misinformation and disinformation to hate speech and extremist material. While groups are exposed to online "bads", it is also important to underline how the internet also accords a host of "goods" including tools to increase resilience to extremist content. Discussed below, these include diverse media landscapes, fact-checking services and boundless opportunities to verify information.

At the same time, smaller local language groups face digital information asymmetries that may increase their vulnerability to online harms. Central Asia is a heterogeneous region where at least six distinct languages are spoken and dozens of dialects. An individual's online experience can vary significantly depending on their language bubble. The quality, diversity and reliability of information available for a speaker of Kyrgyz, Tajik or Uzbek is different from the experience offered to those operating in larger language groups such as Russian. Yet demand for local news content is growing in local languages, especially from rural internet users.[24] Even superficial differences in people's media literacy, area of interest, religiosity can shape their resilience to online messaging from violent extremist actors who may exploit smaller language bubbles, reinforcing echo chambers.

There is also growing popularity for social media channels delivering religious content that can indirectly serve as a conduit for violent extremist groups to amplify their audiences. The flip-side is that there appears to be a deficit of trusted religious content online in local languages that can support, rather than weaken resilience to violent extremist propaganda. Until recently, religious content was tightly controlled in most Central Asian countries.[25] There is also comparatively limited Russian-language content of religious nature and few religious leaders in Central Asia who are fluent in Russian.[26] While the pandemic forced many religious groups to adopt online engagement practices, especially in Kazakhstan,[27] they are not as prolific on social media as the third-party channels from the religious communities of interest, monitored in SecDev's sample.

Central Asian countries also tend to lack genuinely free and independent media, including online. Mainstream journalism that offers trusted, independent public-interest reporting across the full spectrum of issues is an important prerequisite for societal resilience to violence and extremism. In recent period, the region has been backsliding: Kyrgyzstan, Kazakhstan and Tajikistan experienced declines in media freedoms between 2019 and 2020.[28] When it comes to internet freedoms, Kyrgyzstan and Kazakhstan also experienced declines between 2018 and 2020.[29]

Only Uzbekistan has registered modest improvements in media and internet freedom in the last few years, though it started from a very low ranking. There is frequent harassment and prosecution of influencers, journalists, and critics in all Central Asian countries. In 2020, the online media environment worsened further still owing to newly introduced regulatory frameworks strengthening liability for disinformation related to the COVID-19 pandemic. Exploiting the limited space for credible, inclusive media-based dialogue and engagement, extremist influencers found fertile ground from which to propagate radical worldviews and distorted perceptions of reality.

Central Asian countries also tend to lack genuinely free and independent media, including online.

There is a comparatively weak online civic engagement across Central Asia. While Central Asian governments are aggressively seeking to digitally transform their societies online citizen participation based on genuine stakeholder representation, unrestricted feedback and inclusive participation is uneven. The lack of digital participation reflects a broader challenge with governance in the region more generally, dominated as it is by authoritarian tendencies. The outcomes of weak digital participation are similar to those arising from offline exclusion: citizens may instead seek alternative venues and stakeholders to express their views, call for increasingly radical changes to the status quo, and justify violence to effect change and act against perceived injustices.

Central Asia's **online social media ecosystem** itself is a kind of risk factor, overrun as it is with a wide range of digital harms. The spread of misinformation and hate speech, coordinated inauthentic behaviour campaigns, targeted abuse and harassment, discrimination and intolerance, disturbing and inappropriate content with violence, and glorified criminal behavior has potentially corrosive implications for social cohesion and efficacy. One of the cumulative effects of these online harms is the erosion of trust in social media discourse and normalization of radical views espousing violence for a host of causes.

Maximising resilience

There is growing awareness of the ways in which to protect societies and individuals from violent extremism and enhance their resilience to online harms. While it is impossible to completely inoculate someone from digital threats, there are proven ways to reduce their susceptibility. Resilience here refers to the ability of governments, businesses and civil societies - including of course individual users - to anticipate, understand, cope with, adapt to and bounce back from digital threats. Approaches that build resilience involve strengthening targeted communications, offering reliable content, promoting digital literacy and expanding meaningful opportunities for online participation. A host of interventions combining these approaches are already being supported by Central Asian governments, digital platforms, civil society groups and media communities.

At the center of the communication-based approach is the idea of substituting offensive online content with more positive alternatives. Its proponents offer alternative narratives and spokespeople to undermine the efficacy of violent extremist messaging. Specifically, this may include the mobilization of progressive influencers or moderate religious figures. It usually also engages credible role-models including educators, parents and community leaders. By empowering respected messengers to convey alternative non-violent narratives online, together with tailoring and adjusting messaging to online response, it is possible to diminish the likelihood of online conversion to extremist viewpoints.[30]

By comparison, **content-based interventions** are focused on shaping the quality of the online environment to ensure the availability of more balanced and verified information.[31] This approach will work better provided it is not narrowly focused on content development and is accompanied by media development efforts. Strengthening of credible independent media production, especially in local languages could potentially reduce dependence on (globally-syndicated and locally-produced) extremist content that purports to faithfully explain international affairs. It may also entail engaging local independent media outlets and moderate religious groups to build a more robust online presence on popular social media platforms. Indeed, increased social media presence from religious leaders, in particular, can help meet demand for emotionally and spiritually-engaging religious content without blended radical messages.

A key approach to strengthening online resilience in the face of violent extremism is through **building digital literacy.**[32] Any approach to building such capabilities, however, should adopt an approach that accounts for a wide spectrum of digital harms. When users are made more aware about the multifaceted threats existing in cyberspace, they are more inclined to develop an immunity to their effects.[33] Focusing training and education campaigns - as well as more subtle online educational nudges - is critical for newer internet and social media users, people living in smaller language communities, and those with more limited access to independent and diverse media sources.

Initiatives designed to improve digital opportunities for **meaningful and inclusive civic participation** in decision-making at the regional, national and local levels also carry significant potential for engineering online resilience.[34] Genuine channels for engaging with decisions, including on rules for social media, can help build accountability, transparency and trust. Where younger people, including migrants and minorities, have access to participatory mechanisms that allow their concerns to be heard at local community and national levels, they may be less inclined to search out other forms of identity and belonging. By curating and reinforcing positive ecosystems of digital participation, it is possible to provide at-risk populations a positive steer.

Recommendations

Central Asia is at the center of a new kind of hybrid conflagration in which the physical and digital worlds are blurred. In this fast changing scenario, the disruption of online violent extremism and digital harms is just as important as counterterrorism, law enforcement, and development measures in the real world. This is because in the region, and around the world, the process of radicalization intentionally combines virtual and physical interactions, using new tools to identify, groom, train, and deploy recruits. In this, governments, social media companies, and civil societies are facing immense challenges. Working together to fight the problem will be tricky, but the alternative is worse.

Platforms

Coordinate action across social media platforms to improve not just short-term, but also the long-term effectiveness of takedowns. This can be achieved through smarter global coordination and leveraging existing partnership mechanisms in region-specific engagements. Any intervention must be data-driven, comprehensive and systematic in order to ensure coordinated content removal. Measures must also be sensitive to the ways in which violent extremist tactics are changing and informed by specialist knowledge of the linguistic, cultural, religious and socio-political landscapes in which they are taking place.

Invest in tested behavioral change strategies designed to improve digital hygiene. For example, Facebook has launched the Re-Direct Program[35] which discourages users from accessing violent extremist content by re-directing them to alternative resources, education and help communities. Another strategy is the hash-sharing database and URL-sharing program initiated by the Global Internet Forum to Counter Terrorism.[36] These and other user-centered approaches apply basic nudge theory to strengthen positive internet use and minimize the spread of online harms. A good model to follow is Facebook and Google's efforts to encourage users to seek evidence-based material when searching for content related to COVID-19.

Carefully examine and revisit the role of content personalization algorithms in facilitating the discovery of violent extremist content. This is a pervasive challenge, and is only getting worse in many parts of the region. SecDev Group research revealed how multiple violent extremist channels were identified through automated personalized recommendations and suggested content interest features. A concerted effort is required to radically minimize these features.[37]

Launch a major drive to improve the availability and reach of high quality independent media. Central Asian violent extremist actors routinely reinterpret global news developments with radical messaging. Media actors have an opportunity to offer the region's audiences clearer, more objective and more timely analysis of events that evade mainstream media coverage - one example would be online series in Uzbek, Tajik, Kazakh and Kyrgyz languages documenting the situation in locations that are most frequently referred to in violent extremist propaganda.

Civil society, media and academia

Strengthen collaboration at the regional and national levels between government and civil society for coordinated communication and content based responses to high-impact narratives of online violent extremism. A common front is required to address region-scale radical narratives that deliberately seek to exploit existing political and social risks and inflame grievances in local languages. Collaborative action will help achieve production and dissemination related economies of scale.

Double down on media and digital literacy, fact-checking, countering disinformation, media development and digital safety campaigns. There is a real need to inventorize and invest in successful and scalable programs that can enhance overall digital resilience to online harms in Central Asia. A wide range of international and national non-governmental organizations also need to ensure that the issues of online harm reduction are integrated into existing programs.

Strengthen digital inclusion programs that reinforce values of tolerance and diversity and strengthen digital assets of vulnerable groups. Given their particular vulnerabilities, measures that enhance digital access and the online voices are critical. A particular focus should be on women, youth, minorities, migrant workers, refugees and other marginalized populations, including through greater online participation of traditionally offline actors - religious and community leaders, local media, radio, local self-government bodies and community organizations.

Support high quality research on both quantitative and qualitative language and community-focused monitoring of online violent extremist narratives. Applied research using a combination of data analytics together with behavioral and sociological methods could focus on online and offline audience responses among the targeted groups to extremist content - including segments of youth and religious communities. This will help address the deficit of evidence on behavioural response (as opposed to perceptions) of the Central Asian audiences to both the extremist propaganda and countermeasures and guide improved cycles of P/CVE programs.

Governments

Begin planning the next generation online harm reduction strategies as a matter of urgency. Central Asia's existing strategies to counter and prevent violent extremism are approaching the end of their planned life-cycles. A new generation of policy responses to online violent extremism should be to address the new realities and challenges, not least the fallout from the global pandemic, accelerated digitalization and increased risks of geopolitical and regional instability.

Upgrade the efficacy of prevailing online communication approaches to address a broad spectrum of online harms. Past P/CVE strategies have run their course. What is needed now is a more robust focus on encouraging higher quality and diversity of digital engagement, availability of content for communities of interest, including religious communities, and particularly in local languages, informed by evidence-based segmentation of more vulnerable target audiences. Authentic and inclusive communication that goes beyond reminders of liability is key to minimizing the impact of radical social media presence.

Revisit the consequences of intermediary liability and extra-judicial blocking regulations on the principles of freedom of expression, privacy and digital transformation. In particular, governments should review the implications of overzealous content moderation regulations that place undue burden on platforms and may result in content removal, blocking and filtering patterns that negatively impact access to information, media freedom, and Internet access. The countries can also benefit from preventing "dual purpose" use of legitimate measures developed to counter violent extremist influence online towards political opposition, independent media and civil society actors.

Annex 1. Selected digitalization metrics in Central Asia

January 2021	Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan
Internet penetration	81.9%	50.4%	34.9%	55.2%
Internet users, millions	15.47	3.32	3.36	18.6
Social media penetration	63.5%	48.7%	10.4%	13.6%
Active social media users, millions	12	3.2	1	4.6
Top three languages	Kazakh, Russian, Uzbek	Kyrgyz, Russian, Uzbek	Tajik, Russian, Uzbek	Uzbek, Russian, Kazakh

Annex 2. A taxonomy of the primary violent extremist actors in Central Asia

The core of the Central Asian violent extremist ecosystem consists of groups active in conflicts in Syria and Afghanistan, within the coalitions under Al-Qaeda, Taliban, and the Islamic State.

Group name	Description	Languages used	TO designation by the UN	VEO designation by individual states
1. Hayyat Tahrir al-Sham	The large transnational VEO Hayyat Tahrir al-Sham (HTS) heads a major coalition in Syria that includes the multiethnic mercenary/training group Malhama Tactical (MT) and two Uzbek VEOs, Tavhid va Jihod Katibasi (TJK) and Katibat Imam Bukhori (KIB).	Russian, Arabic, English	✓	US, RU, TJ
2. Malhama Tactical		Russian, Arabic, English	—	—*[38]
3. Tavhid va Jihod Katibasi		Uzbek, Tajik	—	RU, UZ
4. Katibat Imam Bukhari		Uzbek	✓	KG
5. Imarat Kavkaz	Imarat Kavkaz (IK), Liwa al Muhajireen wal Ansar (LMA), and Nogai Djamaat (ND)—represent a coalition of smaller Caucasian groups also allied with HTS.	Russian	✓	US, RU
6. Liwa al Muhajireen wal Ansar		Russian	—	US
7. Nogai Djamaat		Russian	—	RU
8. Jannat Ashugu	HTS also includes Katibat al Ghuraba al Turkistan (KGT), a unit composed of ethnic Uyghurs from Uzbekistan, and the Kyrgyz affiliate Jannat Ashugu (JA). Both groups are believed to be affiliates of the Uyghur Turkistan Islamic Party (TIP).	Kyrgyz	—	—*
9. Katibat al Ghuraba al Turkistan		Uzbek, Uyghur	—	US, KZ, KG, TJ
10. Islamic Jihad Union	Islamic Jihad Union (IJU) is an Uzbek Taliban-affiliated VEO that operates in Afghanistan	Russian, Uzbek	✓	US, RU, KG, UZ
11. Jamaat Ansarullah	Jammat Ansarullah (JAN) is a Tajik VEO linked to global jihad groups, including over time Taliban, Al-Qaeda, and Islamic State.	Tajik	—	TJ
12. Jabhat Ansar al Din	A group, operating closely alongside Hurras al Din, the current al Qaeda franchise inside Syria. The UN's report, dated July 27, 2018, states that this new group was formed following a dissent within HTS ranks.[39]	Uzbek	—	—*
13a. IS Wilayah Caucasus	Islamic State (IS) is represented by its official regional provinces, Islamic State Wilayah Khorasan (ISWK) and IS Wilayah Caucasus (ISWC)	Russian	✓	US, RU, KZ, TJ
13b. IS Wilayah Khorasan		Uzbek, Tajik, Kyrgyz	✓	US, RU, KZ, TJ, UZ, KG

Endnotes

1 VEO/TO term is used throughout the report to refer to these 13 groups. Annex 2 provides the name and details of each group.

2 SecDev also detected over 50 VE channels in Tajik-language on Zello, a platform for audio messaging, excluded from analysis due to the time-intensive nature of audio content analysis.

3 Monitoring revealed a notable spike in VE content on religious channels in the October-November timeframe, following cases of extremist violence in France linked to the Charlie Hebdo caricatures of the Prophet Muhammad.

4 4294 posts published in June-November 2020, with combined 1.9 million views.

5 This figure is determined by dividing the number of documented take-downs (195) by the number of documented channels overseen by violent extremist groups (716 as of November 2020).

6 73 percent of all observed takedowns were on Telegram (142 channels). Takedowns on Instagram were responsible for another 17 percent (33), followed by Facebook (6), Twitter (5) and Youtube (5). However, Telegram is among the less effective platforms in removing the observed VE channels - it blocked 28 percent of all detected channels in June-November 2020, compared to 43 percent by Instagram and 33 percent by Facebook. Youtube blocked 17 percent of all detected channels, while Twitter blocked 14 percent.

7 See https://liter.kz/kostanajca-nakazali-za-propagandu-religioznogo-ekstremizma/ and https://forbes.kz/news/2020/09/19/newsid_233869/

8 https://asiaplustj.info/news/tajikistan/society/20180809/kogo-v-tadzhikistane-uzhe-posadili-za-laiki-v-sotssetyah

9 The government reminded users of Criminal Code articles on criminal responsibility for disseminating radical content. See https://t.me/iivuz/27840.

10 Earlier in October, responding to activity in Telegram channels, FSB operatives investigated TJK members in six Russian cities, including a large cell in Volgograd, and arrested several suspected members.

11 https://www.gov.kz/memleket/entities/qogam/activities/2894?lang=ru&parentId=141

12 See https://www.sova-center.ru/files/books/wg-4-2020-rus.pdf.

13 See https://advox.globalvoices.org/2017/07/21/kyrgyzstan-blocks-archive-org-on-extremism-grounds/.

14 In December 2020, Uzbekistan passed a resolution specifying a process for a state media and information agency to notify the owners of websites, online media, messenger channels and bloggers that are accessible from Uzbekistan about audience comments carrying “prohibited information” and seek removal of such comments within 24 hours. See https://www.gazeta.uz/ru/2020/12/25/comments/.

15 In June 2020, MPs in Kyrgyzstan passed the law “On Manipulating information”, obliging the owners of websites and/or pages of websites, to promptly block access to content that is restricted or banned in the country and moderate content to prevent violations of legislation. In August 2020, President Sooronbai Jeenbekov declined to sign the law and returned it to Parliament for revision. See https://internews.kg/wp-content/uploads/2020/05/Zakonoproekt_O-manipulirovanii-informatsiei-.pdf .

[16] The document seeks to regulate the new types of communication - social media networks, messengers, video hosting platforms, online television and radio, virtual servers and bloggers. In particular, it seeks to define the “legal status at the level of a law, of social media and messengers, such as Facebook, WhatsApp, Telegram”. In November 2020, citing concerns with social media content disrupting national security and instigating “interethnic hatred”, a government working group proposed legislative amendments calling for requiring registration of foreign social platforms in Kazakhstan and linking of social media user accounts with registered mobile numbers.

[17] See https://www.unodc.org/e4j/en/terrorism/module-2/key-issues/drivers-of-violent-extremism.html, https://www.radicalisationresearch.org/research/vergani-the-three-ps/, https://steptogether.com.au/blog/push-and-pull-factors-in-violent-extremism/, https://www.cipe.org/resources/drivers-violent-extremism/.

[18] See https://www.hrw.org/news/2021/01/13/central-asia-pandemic-response-threatens-rights.

[19] See https://foreignpolicy.com/2020/11/11/online-extremism-central-asia-islamic-state-terrorism/.

[20] See https://datareportal.com/reports/?tag=Central+Asia.

[21] The four countries also gained 2.2 million new internet users, almost 43 percent of which were in Tajikistan, and another 34 percent in Kazakhstan.

[22] With the exception of Kazakhstan, Central Asian countries are still lagging behind the regional average. Social media penetration rates in Uzbekistan include just over 13 percent of the total population. If the country were to reach the same levels as Kazakhstan, this would add another 17 million social media users. In Tajikistan, slightly more than 10 percent of the population are social media users. It is likely that most future growth will occur quickly due to the introduction of mobile broadband networks. The share of broadband in mobile connections is still relatively low in Tajikistan (60 percent) and Kyrgyzstan (66 percent), compared to 83 percent in Kazakhstan.

[23] See Annex 1 for data on digitalization.

[24] See https://cabar.asia/en/central-asian-audience-receives-news-from-social-media-and-messengers-iwpr-research.

[25] For instance, under Kazakhstan’s legislation on religious organizations, dissemination of even non-extremist religious content is only allowed through a network of registered religious organizations and their officially sanctioned outlets. The authorities routinely identify and fine online users attempting to sell a book with Quranic teachings or upload religious content online. See https://www.inform.kz/ru/shtraf-pochti-v-146-tysyach-tenge-za-publikaciyu-v-socseti-grozit-zhitelyu-sko_a3750467 and https://www.inform.kz/ru/tri-fakta-nezakonnogo-rasprostraneniya-religioznoy-literatury-vyyavleno-v-zko_a3711475

[26] See https://bigasia.ru/content/pub/review/alina-iskanderova-ano-institut-issledovaniy-tsentralnoy-azii/.

[27] See https://www.zakon.kz/5045375-vo-vremya-pandemii-rezko.html.

[28] See https://thediplomat.com/2020/04/have-press-freedoms-improved-in-central-asia/.

[29] Kazakhstan’s score declined from 38 to 32 and Kyrgyzstan’s score from 62 to 56. See https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism and https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow

[30] A 2018 report by the Civil Initiative on Internet Policy on alternative and counter-narratives reviewed over 105 narrative-based video materials produced in Kyrgyzstan with assistance from UNICEF, UNFPA, UN Women, UNODC, UNDP, Search for Common Ground, International Alert, Safer World International/FTI, DVV International, Hedayah Center, Internews Europe, GIZ, HELVETAS Swiss Intercooperation, East West Management, MSDSP and OSCE. https://internetpolicy.kg/2019/06/29/issledovanie-alternativnyh-i-kontr-narrativov-v-media-prostranstve-kyrgyzstana/

[31] For instance, in 2020, as part of Kazakhstan's CVE action plan, the government bodies trained 350 social media specialists engaging the public on religious themes and built a monthly audience of 30 thousand users for the government sponsored religious portal Kazislam, posting over 5,000 media materials. https://www.gov.kz/memleket/entities/qogam/activities/2894?lang=ru&parentId=141

[32] One example is the social media campaign "ThreeDots. Know what you are watching" by Internews, launched in September 2018. https://www.facebook.com/threedotsCA/

[33] See Innes von Behr, Anais Reding, Charlie Edwards and Luke Gribbon. 2013. Radicalization in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism. Brussels: RAND Europe.

[34] One example is the "whole-of-society" approach, promoted in the Central Asian context by most international development actors, in particular the OSCE https://www.osce.org/files/f/documents/a/7/444340_0.pdf

[35] See https://counterspeech.fb.com/en/initiatives/redirect/.

[36] See https://gifct.org/joint-tech-innovation/#row-hash.

[37] See for instance the December 2020 policy note from the EU Counter-Terrorism Coordinator "The role of algorithmic amplification in promoting violent and extremist content and its dissemination on platforms and social media"

https://data.consilium.europa.eu/doc/document/ST-12735-2020-INIT/en/pdf and a position paper from Tech Against Terrorism on content personalization https://www.techagainstterrorism.org/2021/02/17/position-paper-content-personalisation-and-the-online-dissemination-of-terrorist-and-violent-extremist-content/

[38] MT, AD and JA are classified by SecDev analysts as VEOs based on the content they post and the VE activities they engage in.

[39] See https://undocs.org/S/2018/705.

Layout

Raphael Durão
STORMdesign.com.br

About SecDev

SecDev is an agile research and innovation firm helping clients navigate digital-geopolitical, geospatial and geodigital risk. Our team of experts, forecasters and data scientists support a wide range of clients including public sector, corporations and international organizations in meeting their need for timely, accurate decisions. We transform data into intelligence and identify opportunities to drive digital transformation. SecDev builds value through **strategic foresight, data science on demand and intelligence as a service**. We are global in scope, fluent in data collection and analytics, experienced in cutting edge technology and singularly results-oriented. We empower clients to make informed choices in a rapidly digitizing era.

To learn more, visit http://www.secdev.com

SecDev Analytics