

The logo for SRM, consisting of the letters 'S', 'R', and 'M' in a bold, white, sans-serif font. A small red triangle is positioned between the 'S' and 'R'.

SRM

2024

**TRAVEL
SECURITY**

SPECIAL EDITION



FOR MORE INFORMATION, PLEASE CONTACT:

Markus Korhonen
m.korhonen@s-rminform.com

CONTRIBUTORS

Erin Drake
e.drake@s-rminform.com

Richard Gardiner
r.gardiner@s-rminform.com

Shannon Lorimer
s.lorimer@s-rminform.com

Tamsin Hunt
t.hunt@s-rminform.com

Contents

Editorial	04
Education on the frontline: Security threats facing schools around the world	06
Meeting their match: The mounting adversities confronting sporting organisations.....	12
Rolling with the times: Technological progression drives criminal innovation	16
Insidious: Gang rivalries fuel violence in current and emerging hotspots.....	20
Expert interiew with Paul Padman	24

Editorial

Travel security risks are never static. Socio-economic changes, disease outbreaks, new technologies, political uncertainty, conflict, and many other variables inexorably shift the sands of the security landscape.

Major events with wide geopolitical ramifications – perhaps most forcefully exemplified in 2023 by the Israel-Hamas conflict – bring an immediate focus to travel security considerations, both for the affected region and for their wider global consequences. At the same time, more subtle shifts in the global landscape can have equally consequential impacts, and as such, from a risk management perspective, they too bear studying. It is with this reasoning in mind that we write our 2024 Travel Security Special Edition, exploring several important security trends and developments relevant to both personnel safety and business continuity concerns alike.

The education sector has been one area we have had a particular focus on this year. Despite education institutions being perceived as overtly safe spaces, the shifting sands mould the security environment here too, and changes in war, crime and other threat dynamics bring new challenges to educators, administrators, and school officials. As seen in the Ukraine, Sudan and Israel-Hamas conflicts, the education sector is not insulated from growing insecurity and has been subject to direct attacks and surrounding violence that has necessitated staff and student evacuations through 2023. With no clear end in sight for numerous conflicts globally, schools and universities are set to suffer from both targeted attacks and collateral damage in the coming year. Militant groups and kidnappers, too, will continue to seek targets in this sector as they have over the past 12 months, driven either by ideological or financial motivations. Finally, educational institutions across the world, but nowhere more so than in the US, will continue

to seek ways to prevent or limit the impacts of indiscriminate attacks, where assailants in many cases emerge from within the institution itself.

As with playgrounds, sports grounds too are subject to a range of security threats and unscrupulous actors seeking profit. The growing value of the sporting industry, appraised at some USD 500 billion, is itself an indelibly luring prospect to banker and burglar alike. At the same time, the sports industry is not immune to political realities either, with threats and attacks against both fans and teams informed by global developments, while missteps in navigating ever-evolving and contrasting social norms can leave organisations vulnerable to social media backlash and associated reputational risks.

Challenging socio-economic conditions, policy shifts and regional instability across the globe have also left their mark on the organised crime landscape and criminal groups have had to adapt these changes. In some parts of the world, we have seen an increase in violence by such actors while elsewhere crime organisations too have felt new pressures, splintering into small groups. As authorities scramble to extinguish new and evolving organised crime activities, bystanders remain vulnerable. Increasingly, we have seen these patterns play out in commercial centres and tourist destinations over the past year, bringing with them greater need for security awareness and mitigation for business and leisure travellers that will extend well into 2024.

In the virtual world, novel and increasingly widespread technological tools in banking, dating, and the creative industries to name a few, have been embraced both by the public and by tech-

savvy criminals. And now, with generative artificial intelligence having gained a firm footing in 2023 – brought to the fore by popularised applications in large language model chatbots, among others – this technology too offers criminal groups new tools for their crimes. Scams, including virtual kidnapping that involve increasingly complex deepfakes, continue to proliferate, and the coerced use of banking applications allow criminals to elicit payments and quickly empty bank accounts. Regulation and effective policing in the AI sphere are understandably slow and need to constantly evolve. At the same time, measures employed to counter the misuse of applications must be carefully balanced against creating a better experience for legitimate users. With these evolving threats, both in terms of technological developments and their broader societal backdrop, 2024 may indeed unfold as a game of cat-and-mouse between the use and misuse of new technologies.

Finally, within the shifting threat environment, the importance of expert assistance and support remain as one constant. We therefore take the opportunity in this Travel Security Special Edition

to speak with a crisis response expert to dissect some of the global trends in kidnapping, political evacuations, and wrongful detention cases, discussing how these feed into and inform crisis response operators' work.

As the sand shifts, retaining an informed and balanced understanding of the travel security landscape remains a fundamental component of organisations' risk management protocols. Our team looks ahead to working with our clients in 2024 to help them navigate the evolving security environment and the threats they face within it.



Markus Korhonen
SENIOR ASSOCIATE,
STRATEGIC INTELLIGENCE



SECURITY THREATS FACING SCHOOLS AROUND THE WORLD

EDUCATION ON THE FRONTLINE

Over the course of 2023, educational institutions have faced bomb threats, shootings, kidnappings and more. **Dr Tamsin Hunt** collates some of the key statistics, trends, and descriptive examples from 2023, highlighting the nature of global threats that will continue to affect schools and universities in the coming year.

Schools and universities around the world face a vast range of threats that jeopardise the safety of staff and students alike. Schools are often viewed as soft targets in comparison to other official institutions; but aside from ease of access, violence against students and teachers is also highly emotive – and purposefully so. The potential for an attack – and its motive and manifestation – varies tremendously between different jurisdictions. But wherever they occur, attacks on the vulnerable youth attract attention on the global stage, and create urgency and panic among families, communities, organisations and governments. Here, we look at the nature and impact of several security threats that have affected schools over the past year, underscoring the vulnerability of educational institutions as we look ahead to 2024.

WAR

Schools in active conflict zones are technically protected against attack under international law. However, it rarely – if ever – works out that way. Schools are often subject to direct bombings and armed attacks; but they also face the consequences of infrastructure damage, large-scale community displacement, and even the repossession of school property for the use of invading or defence forces. When schools are forced to close, local communities lose access to critical nutrition, healthcare and social support at a time when such services are needed the most. Furthermore, with the outbreak of war, international educational and study abroad programmes are often suspended, and foreign staff and exchange students are evacuated with little to no notice. Some of the conflicts in 2023 have had an immense impact on schools in the affected countries.

CASE STUDIES

📍 SUDAN

Between April and October 2023, 10,400 schools closed in conflict areas due to violence and insecurity, and 6.5 million children have lost access to education facilities.

📍 UKRAINE

As of October 2023, 3,428 schools have been damaged and 365 have been destroyed since Russia's invasion began in February 2022.

📍 ISRAEL AND GAZA

After Hamas's attack on 7 October 2023, schools across Israel closed and switched to online learning for several weeks, and international universities evacuated dozens of foreign exchange students from the country. Weeks later, the future of many study abroad programmes in Israel remains uncertain, and for educational institutions in border areas with Gaza and Lebanon, the decision to teach in person or online remains dependent on the school's proximity to bomb shelters. Meanwhile, in Gaza more children were killed in the first three weeks of the conflict with Israel than in any other armed conflict globally over the whole of 2023, according to the international charity, Save the Children.



TERRORISM AND MILITANCY

Educational institutions – and their staff and students – present particularly attractive targets to extremist groups and radicalised individuals the world over. But what do these threat actors hope to gain? The objective behind an attack against a school can range from attaining local and international notoriety, to influencing the actions of local authorities and intimidating rival communities, to simply drawing attention to a particular political cause.

In Europe, bomb threats against schools have become increasingly common, prompting school closures and panic among local communities. There is no common thread linking the threats, but they tend to occur during elevated political tensions, relating either to the war in Ukraine, or to the conflict in Israel and Gaza, which has driven a resurgence in Islamist extremism and pro-Palestinian sentiment. In Sub-Saharan Africa, a multitude of militant groups stage attacks against schools – from bombings, to arson, to machete attacks – and often result in high numbers of casualties at a time. Mass kidnappings are also frequent in countries including Cameroon, Nigeria and Uganda.

CASE STUDIES

📍 LITHUANIA, LATVIA AND ESTONIA

In October 2023, more than 900 kindergartens, schools and universities in Lithuania received emailed bomb threats written in Russian. Hundreds more were delivered to schools in Latvia and Estonia. All three countries are highly critical of Russia's war in Ukraine. The emails all turned out to be hoaxes.

📍 FRANCE AND GERMANY

Also in October 2023, dozens of schools, airports, and tourist attractions across France received bomb threats over phone and email, and French police arrested dozens of perpetrators, many of them students. Six schools in Germany received bomb threats too. A common motive for the threats remains unclear, but they followed an Islamist extremist attack in the French city of Arras on 13 October, in which schoolteacher was stabbed and killed.



CASE STUDIES

📍 NIGERIA

In September 2023, armed bandits kidnapped 24 students from the Federal University Gusau in Nigeria's Zamfara State, 14 of whom were later rescued by security forces. Loosely organised armed groups – or bandits – are increasingly well armed, perpetrating such violence during looting, raiding and territorial disputes that they now rival regional extremist groups, Boko Haram and Islamic State West Africa Province, for deadly attacks in Nigeria.

📍 UGANDA

In June 2023, militants attacked a secondary school in Mpondwe in Uganda, killing at least 40 students and kidnapping six others. The Allied Democratic Forces (ADF) insurgency group were most likely responsible.



KIDNAP FOR RANSOM

Militant groups are responsible for a number of high-profile school kidnappings around the world, but criminal elements play their part too. Organised criminal groups – and opportunistic individuals – are largely motivated by financial gain, targeting students and staff for ransoms that can reach into the thousands of US dollars.

CASE STUDIES

📍 SINGAPORE AND CAMBODIA

In June 2023, kidnapers told a Chinese student studying in Singapore that he was wanted by the authorities and must go into hiding in Sihanoukville in Cambodia. Kidnappers seized the victim on arrival and demanded a ransom of USD 410,000. The student was rescued three days later through a collaborative effort between Chinese, Cambodian and Singaporean police. No ransom was paid.

📍 ECUADOR

In August in Ecuador 2023, armed criminals kidnapped the dean of the Faculty of Medicine at the University of Guayaquil on Avenida Orellana while the victim was on her way to work. Police rescued the victim from a private residence in Guayaquil that same day.

📍 SOUTH AFRICA

In September in South Africa 2023, kidnapers used a dating app to lure a university student to a hostel in Johannesburg, where he was then held hostage. The kidnapers demanded a ransom of USD 1,600. Police rescued the victim and arrested seven perpetrators.



MEETING THEIR MATCH

THE MOUNTING ADVERSITIES CONFRONTING SPORTING ORGANISATIONS

As sporting organisations extend their global reach and accumulate greater wealth, they face increased susceptibility to various threats, including criminal activities and targeted attacks that jeopardise the safety of athletes, coaches, and spectators. Additionally, a perceived lack of social awareness and responsibility within teams and organisations can carry significant reputational risks. **Richard Gardiner delves** into the evolving challenges that confront these organisations and highlights the considerations they must address to prevent succumbing to these adversities.

The global sports market, valued at over USD 500 billion, has always attracted the world's elite athletes, major institutional investment and international publicity. However, there is a flip side to the lucrative industry. The substantial incomes that professional sportspeople earn has made them and their families attractive targets to increasingly sophisticated criminal actors, while the major public attention and media coverage that athletes, teams and events draw, generate significant security concerns during matches and large events. As the sports industry continues to grow, there must be greater collaboration between sporting organisations, athletes, law enforcement agencies and private security firms. Security issues aside, the spotlight that sports personalities and teams find themselves in also creates the potential for public outcry when they are perceived to respond inappropriately to polarising societal debates. As such, there is an increasing need for greater awareness and adaptation to societal issues that can negatively impact the reputational integrity of sporting brands.



The gloves are off: Violent criminals target European footballers

One of the most alarming patterns to develop in recent years has been the surge in violent robberies targeting top-tier European footballers, carried out by sophisticated crime syndicates. Since 2019, there have been over 20 incidents against players in European leagues. For example, in July 2023, criminals attacked Paris Saint-Germain player Gianluigi Donnarumma and his partner in their Paris apartment. They tied the couple up briefly, then fled with valuables worth nearly USD 550,000. Similarly, in August 2022, assailants held Barcelona player Pierre-Emerick Aubameyang and his family at gunpoint at his home outside Barcelona, causing Aubameyang light injuries. The assailants fled with jewellery and other valuables after accessing the family safe.

The trend is fuelled by various factors, including the lucrative earnings of the athletes; the well-publicised nature of team schedules, which indicates when homes are likely to be unoccupied; and the rapidly expanding online presence of footballers who unwittingly showcase their valuable possessions on social media. While some security experts have criticised certain players for neglecting to invest in robust security systems – ranging from cutting-edge CCTV setups to personal security teams, guard dogs, and panic rooms – there are instances where footballers and clubs have poured substantial resources into fortifying player security. Yet despite these efforts, the robberies have continued. The fact that many of these cases remain unsolved points to a high level of professionalism, often involving criminals who specifically travel to countries like the UK from other parts of Europe or Latin America with the singular aim of executing meticulously planned heists. With few suspects arrested, players and clubs across the board will need to take greater security precautions in the future, such as further upgrades to security systems and greater awareness of the dangers associated with publicising the details of their private life on social media.

Hitting below the belt: Families in the crosshairs

There have been multiple incidents in the past year where sportspeople's or match officials' families have faced kidnappings, attacks, or death threats. In October 2023, the Colombian rebel group Ejército de Liberación Nacional (ELN) kidnapped Luis Manuel Díaz and Cilenis Marulanda, parents of Liverpool football player Luis Díaz, in La Guajira State, Colombia. While Marulanda was swiftly released, Manuel Díaz was held hostage for nearly two weeks before he was released, reportedly without a ransom being paid. In another incident, in March 2023, unidentified assailants fired upon a supermarket owned by Lionel Messi's parents-in-law in Rosario, Argentina, and left threatening messages aimed at the footballer. However, it is not just players' families in danger; relatives of match officials face threats too, especially those officiating high-profile matches. In April 2023, after the contact details of referee Kevin Clancy, who officiated the Scottish Premier League match between Celtic and Rangers, were leaked online, his family received death threats. These events underscore the need for team management and sports authorities to ensure security measures cover not only players and referees, but their families too.



publicity, large crowds, and expansive geographical areas these events encompass. A recent incident in October 2023 underscored this when football fans from French Ligue 1 team Marseille threw stones at the Lyon team bus as it entered the Marseille stadium, shattering the vehicle's windows and causing injuries to the Lyon team manager. Liverpool Football Club encountered a similar incident in April 2023, when a brick was thrown at the team bus as it left the Etihad Stadium, the home ground of Manchester City.

Political events and public sentiment also directly feed into the safety of sporting events and matches. In response to increased levels of anti-Semitism and Islamophobia related to the ongoing Israel-Hamas conflict, heightened security measures were implemented ahead of the New York Marathon in November 2023. Despite the absence of credible threats and incident-free conclusion of the marathon, event organisers worldwide must consistently reassess their security protocols and preparations to align with current global security concerns. For example, in November 2023, the Swedish ice hockey team chose to travel to Finland for the Euro Hockey Tour while dressed in civilian clothing to avoid being easily identified. This followed the attack in Brussels in October, in which an Islamic State inspired assailant opened fired in Boulevard d'Ypres, Brussels, killing two Swedish nationals who were wearing football jerseys ahead of a Euro 2024 qualifier football match between Sweden and Belgium.

Toeing the line on social issues

It is not just concerns about physical safety that sports organisations need to take into consideration, but also reputational concerns around the public backlash when they are perceived to fall afoul in relation to contentious social issues, such as gender and racial equality. Whether protests against police brutality in the National Football League (NFL) in the US, criticism of Arsenal's women's team for lack of diversity, or various controversies surrounding the use of rainbow colours in laces or armbands during matches, the sports field is not insulated from broader social debates.

As public awareness of these concerns grows and the call for greater social responsibility in sports intensifies, teams and sports personalities can ill-afford to attract significant negative media attention. Such adverse publicity can have severe commercial ramifications for teams, particularly if the public outcry reaches a level where sponsors decide to cut ties with the organisation. It underscores the need for sports organisations to develop clear policies on social issues to avoid scandals and effectively address sensitive public matters that compel clubs and teams to react. ^{TS}



As the sports industry continues to grow, there must be greater collaboration between sporting organisations, athletes, law enforcement agencies and private security firms.

Blind-sided at sporting events

The high-profile nature of sporting events and the massive crowds they attract pose significant challenges for event security teams. These gatherings present opportunities for petty crimes like mugging and bag snatching, as well as far more serious incidents, including targeted assaults on sports teams by rival supporters or terror attacks such as the 2013 Boston marathon bombing. Such incidents have prompted global reforms in sports event security, although certain inherent security threats remain due to the extensive

ROLLING WITH THE TIMES

TECHNOLOGICAL PROGRESSION DRIVES CRIMINAL INNOVATION

The recent release of generative artificial intelligence tools, together with increased user engagement with a proliferation of digital dating and payment platforms, have enhanced criminal opportunities and capabilities to carry out virtual scams, including extortion and fake kidnappings, **writes Shannon Lorimer.**

In June 2023, the Federal Bureau of Investigation (FBI) reported an increase in US extortion cases using “deepfakes” – manipulated versions of original photographs and videos, extracted from victims’ social media, private messages and video chats – to threaten relatives into paying extortion or ransom demands. Artificial intelligence (AI) powered content has increasingly been used in virtual kidnappings and other scams, with several incidents over the last year highlighting the downside of rapidly advancing digital technologies. Compounding this, continually rising user engagement with online social media platforms and digital applications has provided greater opportunities for criminal engagement with potential targets. As criminals exploit these tools and platforms for financial gain, opportunities emerge for more polished crimes on a significantly larger scale.

AI-empowered: Criminal tactics evolve

Where online extortion and virtual kidnappings have historically been perpetrated by hackers with sophisticated skills, criminals with limited capabilities and resources can now easily and realistically mimic an individual, allowing them to enhance the credibility of a threat and convince the intended victim that a relative or employee is in immediate danger. Tools designed specifically for criminal purposes are also emerging; in August 2023, English and Russian advertisements appeared on popular messaging platforms and hacking forums offering AI-powered software and training to create deepfake videos for phishing scams, extortion, and fraud, with training costing between USD 20-200, while ready-made videos priced at USD 250.

AI’s ability to automate interactions with potential victims further boosts criminal arsenals. Just as businesses increasingly use chatbots to assist online users, criminals can set up automated responses impersonating people and businesses like banks, generating faster engagement with thousands of potential victims. Increased use of such technology in the commercial space also makes it difficult to distinguish between legitimate versus deceitful bots.



AI-POWERED SCAMS

INDIA

In July 2023, criminals in Kerala used deepfakes to impersonate their victim’s former colleague, requesting money for a medical emergency. After the victim transferred IND 40,000 (USD 480), the perpetrators requested more money, which prompted the victim to alert authorities.

US

In January 2023, a woman in Arizona reported that criminals used AI to clone her daughter’s voice, claiming that she had been kidnapped. During ransom negotiations, relatives located the daughter, who was safe and on holiday at the time.

A wider net

Kidnappers, extortionists, and scammers are also capitalising on increased engagement with online social media platforms and apps to mine for personal information and bait victims.

Online dating remains extremely popular; 366 million people used dating apps in 2022, and the most popular platform, Tinder, reported 70 million users worldwide in 2023. High user volumes have widened the available victim pool for criminals looking to exploit vulnerable individuals. Notable cases of traditional and express kidnapping facilitated through dating apps have been recorded in Brazil, South Africa, and the US, in some cases targeting LGBT platforms. In Johannesburg, South Africa, seven men baited and kidnapped a university student through the LGBT dating app Grindr, demanding USD 30,000 from his family. The ease with which criminals can identify and lure potential targets – especially amid a popular tendency to share itineraries, locations, and other personal information – will continue to provide thousands of potential victims for such crimes.

Meanwhile, the increased availability and use of money transfer and banking apps, like Brazil's PIX, has prompted concerns over the potential to make express kidnappings, scams and even muggings, easier and more lucrative. Brazilians lost around BRL 2.5 billion (USD 500 million) to financial scams in 2022, 70 percent of which were conducted via PIX. Meanwhile, the ability to transfer large amounts of money via phone or laptop reduces the need to drive victims to multiple ATMs and hold them overnight to circumvent withdrawal limits, commonly the case in express kidnappings.

CASE STUDY

CRIMINAL GROUPS SPECIALISE IN DATING APP SCAMS IN SÃO PAULO

In São Paulo, a surge in online dating scams has coincided with the increase in dating services and mobile payment applications. Police statistics indicate that nine out of 10 kidnappings were orchestrated through dating apps, often targeting men between the ages of 30 and 65. Malicious actors use fake profiles to organise dates, luring victims to isolated areas, where victims have reported being met with groups or pairs of kidnappers who use force to demand access to their bank accounts.

In June 2023, a doctor was kidnapped in Brasilândia, a district in São Paulo, after arranging a meeting through a dating application. The victim was abducted by three armed men and held hostage for 30 hours, until he was rescued. While he was held captive, the kidnappers transferred BRL180,000 (USD 36,807) from his account.

A losing battle?

Regulations around AI are still catching up, and mechanisms to limit the use of AI-powered tools for criminal purposes is similarly lacking. Some governments have made progress in developing regulatory frameworks, including obligations for creators to disclose the use of AI-generated and manipulated content, although such regulations are difficult to enforce. Some companies have also developed software that can identify manipulated voices and images, although solutions are often geared towards the commercial sector rather than private individuals. Meanwhile, applications like Tinder have introduced intensified user verification processes, while PIX has attempted to protect users by setting transfer limits and restrictions on nighttime transaction hours to offset typical times in which express kidnappings take place.

Nevertheless, criminals will also continue to leverage technological advancements to improve their own ability to circumvent these measures and operate undetected. The wider adoption of AI technologies, alongside a growing online audience, will simultaneously contribute to evolving criminal tactics and opportunities to enact more convincing, refined scams in the coming years. ^{TS}

CASE STUDY

BANKING APPS AUGMENT KIDNAPPINGS IN SOUTH AFRICA

South African banks have encouraged the adoption of digital payment methods, including linking bank cards to smartphones for contactless payments. This coincides with a recent uptick in reported kidnappings wherein perpetrators force victims to transfer all available funds from their digital wallets to accounts outside of South Africa, or make massive online purchases. Such cases are also increasingly initiated through vehicle hijackings at gunpoint. The banking sector has reported incidents perpetrated by specialised syndicates as well as opportunistic individuals, and businesspeople or individuals perceived to be wealthy have been specifically targeted. Professional platforms like LinkedIn, where users display up-to-date information and contact details, have already been a target for criminals using web scraping tools to compile victim lists.



INSIDIOUS

GANG RIVALRIES FUEL VIOLENCE IN CURRENT AND EMERGING HOTSPOTS

While organised crime is often thought to occur on the fringes of society, a combination of shifting trafficking routes, migration, and socio-economic challenges are increasingly facilitating gang rivalries that have driven brazen, often indiscriminate violence in tourist hubs and major urban centres, **writes Erin Drake.**

Several countries have experienced an uptick in gang violence in 2023, as criminal groups fragment, expand, and jostle for territorial control amid a rise in global demand for cocaine. Despite efforts by various governments to crack down on points of entry, gangs have simply sought alternative routes and more permissive operating environments. Exacerbating these dynamics is the fact that, since the Covid-19 pandemic, many governments have faced intensifying domestic and geopolitical pressures, including cost-of-living crises, migration due to regional conflict and instability, and endemic corruption, challenging law enforcement's ability to adapt to shifting criminal landscapes. While not a new predicament, these factors have enabled greater opportunities for organised crime to flourish, particularly in major port cities and travel hotspots. In the midst of these rivalries, civilians – including travellers – are becoming more vulnerable to indiscriminate violence.

Security crackdowns and gang rivalries breed violence

Traditional cocaine transit routes are shifting, creating new hotspots and stoking competition between gangs. Trafficking between Latin America and Europe has strengthened considerably in recent years as cartels diversify from the US market to expanding European markets. Belgium and the Netherlands, specifically, have become instrumental transit points in this supply chain, overtaking Spain and Portugal as the main entry points for cocaine from Latin America. In May 2023, INTERPOL's Secretary General, Jürgen Stock, stated that this has been accompanied by a "corresponding rise in violent crime...of unprecedented scale."

With European authorities escalating drug seizures at ports, rivalries have intensified as gangs vie to maintain control of trafficking and distribution networks – and civilians have not escaped the violence. Record cocaine seizures at Rotterdam Port have triggered a wave of

Violent organised crime: Current and emerging hotspots in 2023 and 2024

AMERICAS

📍 MEXICO

Officials in **Quintana Roo, Mexico**, have warned of at least 28 'high-risk' locations as cartel violence drives excessively high homicide rates and residual violence that has killed and injured bystanders and tourists.

📍 CHILE

Pressure on Brazilian and other gangs have prompted them to look to Chile's generally unpopulated organised crime landscape for a foothold, escalating the threat of violence in the coming year.

AFRICA

📍 MOROCCO

With Morocco an increasingly strategic transit point in the cocaine trade, the country's powerful Mocco Mafia controls a large portion of Europe's drug market and has been responsible for violence and assassinations of rivals, officials and journalists in the Maghreb and Europe.

📍 NIGERIA

Cult groups specialising in violence for hire have bolstered Nigeria's organised crime landscape, becoming intermediaries for a range of violent activities like enforcing extortion and carrying out retaliatory kidnappings and assassinations.

📍 SOUTH AFRICA

The prominent Capetonian Hard Livings gang has also infiltrated **Durban**, a growing cocaine transit hub, driving a spike in skirmishes and retaliatory shootings and kidnappings with local gangs.

EUROPE

📍 SWEDEN

In **Stockholm** the government has requested assistance from its armed forces to support in combatting a rise in gang violence and assassinations that have killed bystanders.

📍 BELGIUM

In January 2023, an 11-year-old girl was killed in her home in **Antwerp** during a retaliatory shooting as gang violence escalates.

📍 FRANCE

On 10 September 2023, an inter-gang skirmish, in which shots were indiscriminately fired into nearby buildings in **Marseille**, killed a 24-year-old woman in her apartment.

📍 ITALY

In 2023, **Rome** experienced a wave of public mob-like assassination as mafia groups seek to fill a power vacuum left by security operations against their leaders.

📍 AUSTRALIA

Sydney has seen a spike in violence, kidnappings and assassinations – including in public spaces – amid record seizures of cocaine and methamphetamines in 2023. **Adelaide** has become subject to skirmishes between Sudanese gangs in northern and western suburbs.

retaliatory attacks as gangs scramble to reconfigure their operations and territory; over 50 explosions and arson attacks have hit homes and businesses across the city, as gangs have targeted relatives and friends of rival group members to settle scores. Meanwhile, in Antwerp Port, violent competition between drug gangs has escalated as they vie for market share through Europe's second-largest cargo port, which has become a prominent smuggling hub. Violence has indiscriminately affected bystanders as gangs stage bombings, shootings and stabbings, with 70 incidents occurring between January and June 2023. The threat of bystander casualties will likely escalate in the coming year as security crackdowns continue.

Exploiting poverty and insecurity

With inflationary pressures driving higher living costs and increased poverty following the pandemic, already vulnerable communities have become increasingly exposed to criminal recruitment, especially among youth with limited opportunities for social or economic advancement. In some cases, this has driven an expansion in gangs' size, capabilities, and appetite for market share.

In South Africa, structural inequality, poverty and exploitation by drug lords and corrupt spiritual leaders have enabled the formation and expansion of violent youth gangs in townships like Nyanga in Cape Town, and Inanda in Johannesburg. These areas see high concentrations of homicides, extortion, and violence, although assassinations occasionally extend to upmarket neighbourhoods frequented by tourists. Sweden has also experienced rising gang violence in recent years, but the latest surge in Uppsala and Stockholm in 2023, with regular bombings and shootings, have resulted in several casualties. Authorities attribute this surge to clashes between rival gangs that have intensified efforts to recruit youth from economically disadvantaged immigrant neighbourhoods to distribute product and fight over territory. Police indicate that 42 people have died in 290 shootings in 2023. Meanwhile in Marseille, France, unemployment and high living costs have also encouraged gang membership, and the city has seen a significant rise in homicides and assassinations stemming from a war between two rival local gangs amid Europe's growing demand for cocaine. At least 44 people have been killed and 109 injured in associated violence, including indiscriminate shootings, since January 2023.

Leveraging regional instability and migration

In Latin America, a combination of El Salvador's violent crackdown on gangs, a resurgence in violence between

Colombian drug gangs, Haiti's domestic insecurity, and wider regional economic struggles have caused migration to surge. Criminal groups have exploited overwhelmed security forces and vulnerable populations to smuggle drugs, weapons and people across porous borders, and increase their presence and operations along trafficking routes in the region. Members of El Salvador's powerful street gangs have increased activities in Guatemala, Honduras and Mexico, while Brazilian, Mexican and Colombian gangs seize similar opportunities in Ecuador, Costa Rica and Chile, driving violent rivalries over extortion and trafficking networks.

Mexican cartels have leveraged migrant flows to facilitate human and drug trafficking into the US, regularly clashing over and abducting migrant communities, and targeting rival 'polleros' (coyotes) suspected of operating in cartels' turf. This has prompted civilian deaths and kidnappings, including of US and other foreign tourists. In March 2023, four US nationals travelling in Mexico's northern Tamaulipas State were abducted by cartel members who allegedly mistook them for rival smugglers, killing two victims. Travellers remain extremely vulnerable to threats of violence and kidnap in the coming year, particularly in cities bordering the US, which remain popular locations for medical tourism.

Outlook

Corruption and a lack of resources continues to render governments and police ill-equipped to curb persistent trafficking and gang violence. Criminal groups will continue to expand into ports and cities, forming rivalries and alliances, and triggering competition for turf. Insecurity, unemployment, and high living costs will also continue to push impoverished youth and vulnerable migrant communities to engage with gangs for security, driving the potential for intensified violence in existing and new hotspots the coming year. Governments will need to bolster regional and international cooperation to address this transnational challenge, which threatens to draw violent consequences of organised crime further and more frequently into tourist hotspots and commercial centres. ^{TS}

Q + A

EXPERT INTERVIEW

S-RM spoke to **Paul Padman, Deputy Head of Crisis Response**, about some of the global trends in kidnapping, political evacuations and wrongful detention cases, and to hear about some of the key considerations for S-RM's Crisis Response team when they are working on a live case.



PAUL PADMAN

Paul supervises all response cases, coordinating the 24/7 deployment of S-RM's global response team, and reviewing all critical incidents reported by clients, ensuring each receives an expert and bespoke response. He previously served as a senior Detective at New Scotland Yard and has over thirty years of policing experience and has undertaken as well as supervised major investigations within both the Specialist Operations and Specialist Crime Directorates, specialising in covert policing techniques and countering serious and organised crime groups. He has extensive international operational experience including terrorism, kidnap, piracy, extortion and unlawful detention cases, and has trained law enforcement and other government agencies domestically and internationally.

Q Response consulting is perhaps most readily associated with kidnap for ransom incidents. As a starting point, could you talk us through the range of work that the team is involved in?

We help our clients respond, with confidence, to a broad range of 40+ perils. These range from kidnap-for-ransom to complex and sophisticated cyber threats and attacks, piracy on the high seas, security incidents in their broadest sense, emergency evacuations, extortions and other threats, detentions, lawsuits and organisational crises.

Put simply we stand ready and capable of responding, within minutes, to pretty much any human crisis and never know, from day to day where the next crisis will spring from, or what it will be.

I think it is fair to say that the majority of our cases involve the response to kidnap, piracy (though less so in the

last 18 months), cyber-attacks and other threat extortions. Whilst complex and multi-faceted in scope, context and immediacy, evacuations stemming from political violence, war, natural disasters or regional instability still remain, happily, the exceptions to the rule.

Q Almost by definition, political evacuations happen in circumstances liable to rapid and unpredictable change. How do you weigh up the risks, and what information do you rely on to make decisions on when and how you evacuate people?

Over the last two to three years, we have planned and executed emergency evacuations in Hong Kong, Mozambique, Myanmar, Ukraine, Israel, and Palestinian Authority as well as several during the COVID pandemic. The golden rule in evacuation decision-making is working out what is actually going on and, if appropriate getting the client out before it is too late, whilst always bearing in mind that evacuation is not always the safest option! In our experience, most clients fail to contingency plan, or make overly complex, inflexible plans which are overly reliant on direction and support from local embassies and national authorities. As ever, flexibility, adaptability, and sharp thinking are our watchwords!

Generally speaking, at the national/pan-national level, governments tend to delay an executive order instructing their nationals to evacuate to the 'last safe moment' – in the hope that a diplomatic solution can be found. The key risk by this stage, is that it might already be too late, or an evacuation might only be possible under extremely difficult circumstances, possibly requiring a national/international military operation conducted in a context where there is increased risk to life.

The critical risk for our clients, irrespective of the existence or not of insurance cover, is the timing of a decision that anticipates political decision-making, so that they can evacuate their people before it becomes unsafe or impossible to do so and they are left with no option other than to stand fast, go into 'hibernation' and 'hope for the best'. Inevitably, given the 'chaos and 'fog of war' that will pertain at that moment, the 'go/no go' decision often comes down to an instinctive – and subjective – judgement of what is best and safest to do in the circumstances from their perspective rather than that of others who, unsurprisingly, will be acting with their own interests at heart.

Q Have there been any notable changes in the kidnapping landscape – whether looking at the way kidnappings are carried out, how long they last, the size of ransom payments, and so on – over the past year compared to what you have seen previously?

Kidnapping tends to flourish where state institutions are weak, the rule of law is not effective and the security environment permissive. Prevention is always the best option. Kidnap invariably changes the lives of the victims, their families and work colleagues.

S-RM has seen a year-on-year increase in kidnap events particularly in Sub-Saharan Africa, Central and Latin America but also in Asia Pacific and Middle East. The long-term trend of local nationals being the likely victim continues. In general, average demands are increasing whilst the durations of kidnap events are also shortening. We are seeing an increase in express and virtual kidnap. Some of these phenomena may be linked to post pandemic travel. For the criminal it is an easier crime to perpetrate with fewer logistical requirements, fewer overheads, a faster pay day and even less probability of being caught.

In the Gulf of Guinea there have been fewer reported piracy kidnap incidents. Nigeria's NIMASA organisation recently declared that Nigerian waters have been piracy free for almost two years. With the coordination of international maritime patrols and increased local Nigerian enforcement, the current response may be seen as an effective deterrent. However, it is likely still too early to tell whether pirates intent on kidnap have been truly deterred in the long term or merely displaced or suppressed for the time being.

Q Is there a 'basic formula' for kidnapping, in terms of how they take place and how negotiations are conducted, that is common globally, or are there major regional differences?

Every kidnap-for-ransom is unique in its circumstances, context, and human impact on the victims. Insofar as there is any commonality, our experience is that the vast majority of criminal kidnappers are motivated by a desire for financial gain. There are regional variations in 'style' and the probability of real harm being done to the victim, but most kidnaps-for-ransom conform to the principles outlined here. There is no 'template' or 'formula', and a kidnapper will continue the extortion until he/she feels that there is no

more to be gained – or the risks to the criminal enterprise outweigh the return on the investment. Ultimately, the solution lies in reaching a safe but robust agreement in response to coercive tactics; a release cannot be reached by offering money alone, and significant resilience is required in the face of unpleasant threats and other coercive tactics.

The response to kidnap is art not science; put simply, it is about transforming an unreasonable demand into an achievable one in a negotiation that is anarchic in comparison to traditional business norms and where criminal kidnappers make – and break – rules to suit their own agenda. It is not a quick process, though cases can resolve fast. The response is about managing risk to life in such a way that, unless absolutely unavoidable, decisions are based on what is safest to do rather than that which may be expedient in the circumstances. Above all it requires mutual trust, absolute consistency, moral courage, and endless patience.

Ultimately, kidnap is about people, not property, equipment, data or contracts and resisting the demands of a kidnapper in the negotiation process creates very real risks to the life of the victim. Nonetheless, provided that the risks are thoroughly and sensibly controlled, and the overall response handled sensitively, confidentially and in the best interests of the victim, their family and employer, it is likely that a kidnap case will end with a safe release.

“

The critical risk for our clients, irrespective of the existence or not of insurance cover, is the timing of a decision that anticipates political decision-making,”



Q What avenues are available for private sector crisis response operators in cases of wrongful detention, given how we have seen national players such as Russia use wrongful detention to extract concessions or prisoner swaps from other national governments?

Thankfully, wrongful detentions remain rare, but over the last decade, numbers have risen dramatically. For example, 150+ US citizens have been detained by foreign governments in the last 20 years, but over the last 10 years, that number has risen by over 150 percent.

The motivations behind wrongful detention are frequently complex, nuanced and opaque and this can complicate both the assessment and response process. Broadly speaking, however, wrongful detention at the state level amounts to the exploitation of a detained individual in order to gain information, negotiate prisoner releases, or wrest political/other concessions from another government.

Whilst the state-level is, potentially, the most serious level of wrongful detention, seemingly innocuous

behaviours that are not intrinsically criminal in nature also present challenges when viewed through the lens of a host country where different customs, morals and standards may apply. The reality is that an incident does not have to be high profile, or motivated by political considerations, for the unwary traveller to fall foul of a detention that might – or might not – be considered wrongful. Every region is a little different, and so is every country.

So, what scope is there for us as responders? As ever, prevention is likely to be far more cost-effective and less traumatic than the alternative, and time spent mitigating the risk of detention during travel to countries where there is a tangible risk of it is well worth the investment. We are developing a 'Detention' training product this year to help clients build an effective training and pre-travel awareness programme that accounts for the risk of wrongful detention. And, if a detention occurs, we are well placed to provide advice and guidance to employers/families, conduct a thorough risk assessment, and coordinate the overall crisis management of the incident. ^{TS}



S-RM is a global intelligence and cybersecurity consultancy

We support our clients by providing intelligence that informs critical decision-making and strategies, from investments and partnerships through to disputes; by helping organizations build resilience to cybersecurity threats; and by responding to cyberattacks and organisational crises.

The information provided to you in this document is confidential and prepared for your sole use. It must not be copied (in whole or in part) or used for any purpose other than to evaluate its contents. No representation or warranty, express or implied, is or will be made and no responsibility or liability is or will be accepted by S-RM, or by any of its respective officers, employees or agents in relation to the accuracy or completeness of this document and any such liability is expressly disclaimed. In particular, but without limitation, no representation or warranty is given as to the reasonableness of suggestions as to future conduct contained in this document. Information herein is provided by S-RM Intelligence and Risk Consulting Ltd on our standard terms of business as disclosed to you or as otherwise made available on request. This information is provided to you in good faith to assist you in mitigating risks which could arise. No implied or express warranty against risk, changes in circumstances or other unforeseen events is or can be provided. S-RM Intelligence and Risk Consulting Ltd accepts no liability for any loss from relying on information contained in the report. S-RM Intelligence and Risk Consulting Ltd is not authorised to provide regulatory advice. S-RM Intelligence and Risk Consulting Ltd is registered in England with Number 05408866 with its registered office at: Beaufort House, 15 St Botolph Street, London, EC3A 7DT, UK.

hello@s-rminform.com | www.s-rminform.com