# Russia World Cup Overview

HP Risk Management Ltd May 2018

## INTRODUCTION

The Russia World Cup runs from 14 June – 15 July and takes place across 12 venues in 11 cities. Accreditation registration deadlines for media staff travelling to Russia are now largely complete and the Association Internationale de la Presse Sportive (AIPS) estimates some 15,000 accredited media staff will travel.

The World Cup comes at a time of heightened geopolitical tensions between Russia and some Western powers. The alleged Russian involvement in the poisoning of a former Russian agent in England in March; ongoing competing interests in the Syrian conflict; unresolved tensions over Ukraine; and investigations into Russian interference in the 2016 US elections, pose just some of the most divisive areas of tension.

Within this context, multiple government and risk advisory specialists have published travel warnings and issued advice about travel to Russia next month. Yet media companies still remain uncertain about the threat level they face and practical mitigation measures to minimise exposure during their stay.

HP Risk Management summarises some of the most pertinent threats to the media and provides some general recommendations to consider before, during and after deployments to Russia this year. For more detailed advice, or to speak with one of the team, please get in touch.

## Cyber Awareness & Information Security

The relationship between Russian state agencies and organised criminal groups in the cyber sphere is opaque, but what is clear is that both sets of actors have strong capability to penetrate information security. This area is most relevant to media teams travelling to Russia; they require technology for their work; attract the attention of Russian authorities and have previously been exposed to cyber-attacks outside of the country. Although extremes such as live broadcast signal intrusion are unlikely during the tournament, less public forms of device information security interference should not be discounted.

Travelling crews and media staff should therefore appreciate their exposure to information security breaches and assume that devices might be tampered with. The impact of a device being compromised is rarely immediately apparent and can take a long time to manifest. It might not be until long after the World Cup that compromised equipment could affect your personal information security, or even wider business operations.

In the absence of leaving all technical equipment at home, circumventing all information security threats in Russia can certainly be difficult, especially if considered 'a person' of interest to Russian authorities. However, some basic security measures can be taken to reduce the threat:

- There is no definitive list of restricted media equipment in Russia. It is prudent to always document any relevant equipment that you are transporting should you be subject to questioning. Other equipment associated with hostile environment travel including body armour, or respirators are not considered necessary although medical kits should always be carried as standard protocol. Note that unlicensed aerial recording during the World Cup is banned and personnel should not use drones unless sanctioned to do so and in possession of relevant permits.
- With tens of thousands of people travelling to Russia and the international spotlight heavily focused on the tournament, customs and police are unlikely to be overly difficult, or hostile during the World Cup; however, you should remember that they do have the right to inspect and confiscate any equipment carried. Authorities can demand encryption codes and access to devices such as phones. Additional security practices deployed on devices such as VPNs, finger print or face recognition software should be temporarily removed prior to border checks.
- VPN is not strictly illegal in Russia but VPN services must be registered with the media watchdog Roskomnadzor following legislation introduced in 2017 to try and prevent access to banned websites. Many corporates continue to use VPNs inside Russia, but you could be questioned, or charged if using non-registered VPN technology; and it is not guaranteed to work. In general, avoid connecting to corporate systems; the use of a compromised device to do so could provide a backdoor to company IT networks, or give access to information that could later be used for criminal purposes.
- Encryption can help to protect your personal and corporate data. While there is no known legislation around the right to encrypt information, media outlets should be aware that the Russian government has passed legislation on the distribution and maintenance of encryption facilities for which users will need a license. Media outlets may be questioned over the use of encrypted material. The Russian

government can legally ask users of encryption to decrypt information. If media outlets decide to use encryption iOS devices have encryption activated by default. On MacOS it's called FileVault; for Windows it is called BitLocker, and on Android it is under device encryption.

- Avoid public Wi-Fi spots, especially in hotels and public areas. As anywhere, public Wi-Fi spots are among those most vulnerable to malicious cyber activity. It is generally preferable to use your own personal hotspots. If purchasing a Russian SIM card, you will be required to provide your personal details. Rossiya Segodnya International Information Agency centres will be present in each of the host cities for non-FIFA accredited media channels, offering Wi-Fi access. These media centres are unlikely to guarantee secure Wi-Fi protection and the same caution should apply if using their facilities.
- Use safer apps for communications. Signal, Wire, WhatsApp, or Facebook Messenger each have additional layers of security compared to SMS or email. Users should make themselves aware of the security vulnerabilities before using each app. Note that in 2018 Russia banned the use of Telegram on security grounds, citing its use by jihadist networks for private communications.
- If possible, travel with blank devices, containing no previous footage, sensitive information or documents. Alternatively delete any sensitive information from a device prior to travel, storing external back-ups. Burner phones are advised and you may wish to purchase a Russian SIM on arrival.
- Avoid using landline telephones for any sensitive communications, including hotel phones. Do not use public phone charging points as they might be compromised.
- Try not to leave devices unattended and if necessary to do so, leave with either a trusted source or in a secure location. Although hotel room security cannot be entirely guaranteed, do consider where in your room you might store laptops, cameras etc. If your phone is lost and then reappears, be suspicious as it could have been compromised.
- The threat does not end on return to your home country. Speak to your corporate IT security or risk management team about best practice on return from the World Cup. It is possible they might want to inspect corporate devices for any malicious software or viruses inadvertently downloaded, before you reconnect to the corporate network.
- There are multiple other general "cyber hygiene" recommendations available: for example, concerning best password practice, keeping software up-to-date, using multi-factor authentication and tips on avoiding phishing attacks.

## Media Profile & Logistics Considerations

The freedom of the Press is weaker in Russia than in most western states and existing tensions between the Kremlin and both Washington and London do inevitably raise the profile of US and UK media institutions. Generally, however, journalists reporting solely on the football tournament and related football affairs are unlikely to face any hostility or intimidation from authorities.

Journalists reporting on more provocative issues, such as Russian political affairs, minority rights or any subjects involving state security forces are much more likely to experience difficulties, including potential surveillance or temporary detention in Russia. Journalists could also be targeted by fake sources or have their public profile raised on Russian state media in an effort to discredit their work if it is considered a threat to national interests or Russia's reputation. Additional sensitivity should be taken if filming or recording around security forces or military sites in the country, which could lead to the confiscation of equipment.

The profile of journalists in-country should also be considered. LGBT and non-Caucasian individuals have both experienced discrimination and violence in Russia and police protections for both groups are poor.

Media personnel solely covering the football have a different accreditation process than news journalists during the period of the World Cup. Those travelling on a World Cup related visa are not permitted to report on other news affairs and could face detention or expulsion from the country if found to be in violation of these regulations. With the FAN ID acting as a visa for travelling fans, it is important to note that electronic migration cards are issued upon arrival for all personnel during the tournament. If you are moving city during your stay it is necessary to register your arrival in each new location within 24 hours. In most cases this is undertaken by your accommodation, but you should always check this in advance to avoid later penalties, or scrutiny by authorities on departure. Ensure that you maintain all documentation given on arrival as this can be subject to inspection by authorities on departure. It is a requirement to carry your passport on you in Russia and it is advisable to make several copies of key travel documentation prior to departure, leaving necessary information with a trusted family member or friend at home.

Public transport is being provided for free in most World Cup cities and some services have designated areas for the media that can be accessed with a media pass; driving should be avoided. Moscow has a notorious traffic problem, road restrictions will be in place around stadiums on match days and driving standards are generally poor.

It is advisable to have contingency plans in place should something go wrong. Although the likelihood of detention is considered low for most journalists reporting on the World Cup, news teams in-country could be subject to surveillance, or temporary detention to disrupt scheduled activities. As a minimum, personnel should give family members copies of identification documentation and scheduled travel times.

Before departure, set up your phone to allow remote wiping. In the event it is lost or stolen, you can then wipe the data stored on the device. Again, it is advisable to provide details to wipe the data to a friend or family member should you be unable to do this yourself.

Communication back-ups should be considered in the event that either phones are stolen or confiscated, or that communication blackouts are introduced in the event of unrest.

## Other General Security

Primary physical security considerations relate to the threat of terrorism and fan violence during the World Cup. In both instances, however it is worth noting that security will be elevated throughout the tournament and under the global spotlight, the Kremlin will be keen for the World Cup to pass without incident.

Regarding terrorism, Russia has a history of domestic extremism largely emanating from the North Caucuses and has become a target of Islamic State, primarily as a result of its military activities in Syria. Add to this the prestige of the World Cup and the history of Islamist groups issuing threats to the tournament, the terrorist threat should not be overlooked. Caucasian-Islamic militants have in the past targeted densely populated public areas in major Russian cities while recent years in Europe have illustrated the capability of individual attackers, or small cells claiming affiliation to Islamic State to target members of the public.

Further online threats and intelligence warnings will likely emerge as the tournament approaches, Russian security services will continue to report plots and make arrests: the Federal Security Services (FSB) claim to have foiled at least six plots already this year; and vigilance in all public areas should not of course be ignored. That said, Russian intelligence, heavy police deployments and strict perimeter security around stadiums will likely manage the direct threat of terrorism affecting games. Hotels, public transport and other popular public areas will be well policed and border controls and planned FAN ID schemes to limit travellers without tickets will all help manage the overall threat. Furthermore, both the Sochi Winter Olympics and 2017 Confederations Cup served as testing grounds for policing and counter-terrorism operations, albeit for smaller events in fewer locations.

Conversely, Russian interests outside the country could be more exposed to attack during the World Cup. The shooting of diplomat Andrei Karlov in Ankara on 19 December 2016 and the attack on the Metrojet 9268 flight after departure from Sharm el-Sheikh in Egypt in October 2015 both illustrate how Russian nationals have been targeted outside of Russian territory. An attack on Russian interests abroad during the World Cup would be easier to perpetrate yet still garner international media attention.

Russian security forces may help prevent attacks on World Cup venues and cities, however the potential disruption from hoaxes should not be discounted. Bomb hoaxes across 170 Russian cities between 11 September and 10 October forced the evacuation of more than one million people from over 2,400 different locations. The caution taken by security forces in conducting mass uncoordinated evacuations and the inability to determine the bomb threats as hoaxes suggests certain venues could again be exposed to mass disruption. The hoaxes - linked to a so-called “telephone terrorism” - were likely conducted by a form of

Internet Protocol technology that remains affordable to criminal groups and could again be used during the World Cup. Although arrests have been made, information is limited on what measures Russian security forces have since taken to prevent a repeat of similar disruption.

The prospect of violence by hooligans – or Russian ultras – targeting other groups of football fans has also attracted a lot of attention. The Kremlin however is unlikely to tolerate fan violence on its own soil and the FSB has accelerated efforts to identify and infiltrate ultras gangs since the issue came to light during the European Championship in France in 2016. Despite alleged ties between some ultras and security forces, it is thought that any mass unrest by Russian fans would require some form of implicit approval by authorities. Unrest and disorderly behaviour by other nationals will meet strict punishment, including imprisonment and the removal of FAN IDs and stadium access, thus likely deterring any clashes from escalating beyond isolated incidents.

Alcohol consumption has been restricted during matches to reduce the prospect of alcohol-fuelled unrest and tight restrictions are in place on public gatherings of more than three people, which could be used as a pretext by security forces to break up potentially volatile groups prior to the outbreak of unrest.

All travelling personnel should however be cautious in their interactions with security forces. Several layers of security forces, including the military and emergency services, will be used to assist in policing the tournament and each has different levels of experience and approaches to crowd management. During political opposition rallies in Russia the police have been regularly criticised as heavy handed and quick to detain participants and similar measures could be used in the event of crowd unrest during the World Cup. Although security forces will be under orders to maintain calm among fan groups, should political opponents seek to infiltrate crowds during the World Cup – both inside and outside the stadiums – a heavy-handed response should be expected. If reporting from or around crowds, remember to report from a safe position (high ground/building or from a distance), ideally with a colleague, and scope out an evacuation plan should the situation escalate or crowds quickly grow. Wear sensible footwear and try to conceal recording equipment as best you can until required.

## Variables

Although it is now less than a month until the World Cup starts, personnel should appreciate that the threat environment could quickly change. It is therefore advisable to continue to monitor events both domestically in Russia and on the international stage before and during the tournament. Although the Kremlin and all participating countries will want to see the tournament pass off smoothly, the current state of geopolitical affairs, particularly in the Middle East, do lend themselves to potential changes that personnel should be aware of. A few notable scenarios that could change the threat picture in Russia include:

The competing interests of Russia and several Western states in the Syrian conflict could become more complex if recent military confrontations between Iran and Israel escalate further. Although both the US and Russia likely favour a de-escalation of the situation in Syria, belligerent rhetoric between Tel Aviv and Tehran combined with proven willingness to conduct attacks against each other's interests could feasibly see the situation deteriorate

and quickly embroil other external powers. Further proxy conflict in Syria, on the back of the recent US withdrawal from the Iranian nuclear accord, could see bilateral tensions worsen, detract international attention from the World Cup and see foreign interests in Russia, including media personnel, increasingly subject to hostility from state authorities.

Several other international events could see a change in geopolitical relations around the World Cup. Ukrainian nationalists could also seek to use the World Cup as provocation or increase operations against Russian separatists along the Donbass Line or in the Luhansk region. New chapters in the poisoning of Sergei and Yulia Skripal in the UK, or the ongoing investigation into alleged Russian collusion with the Trump administration ahead of the 2016 US presidential elections could also have a knock-on effect on relations. These developments, or the aforementioned prospect of a terrorist attack against Russian interest outside of the country during the World Cup, would each prompt different reactions from the Kremlin at a time when it is keen to portray a picture of stability at home. Importantly for the media, it would also likely increase editorial appetite of newsrooms inside Russia to report on alternative issues to the World Cup, potentially stoking the ire of Russia's authorities.

Domestically, a poor performance by the Russian national team at the World Cup could potentially inspire some isolated unrest among Russian fans, especially if the team does not qualify beyond the tournament's group stages. Although hopes are not too high in the country following poor performance among the Russian team for several years, an early exit from the competition could spur some isolated acts of unrest among disgruntled fans, especially if a defeat were to occur among controversial circumstances such as questionable refereeing or decision making linked to the introduction of new Video Assistant Referees (VAR). As mentioned above, any opposition groups seeking to use the World Cup as a political platform could also trigger a crackdown by authorities. Although opposition protests of a similar scale to those witnessed in early May are not expected to be repeated, isolated public demonstrations of opposition to the government or other acts of defiance, for example by members of the LGBT community or protesters using ambush marketing techniques to get airtime, will garner the attention of journalists inside Russia and could inadvertently worsen relations between security forces and media teams.

### HP Risk Management

HP Risk Management specialises in advisory services, training and crisis management for the media and NGO sectors. We are providing on-hand risk management support, including digital safety advice and crisis management workshops, to several international newsrooms and digital media agencies travelling to the World Cup.

## Additional Information

- UK FCO World Cup Advisory: https://www.gov.uk/government/news/be-on-the-ball-world-cup-2018-in-russia

and
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/699686/000_FCO_World_Cup_advice.pdf

- UK FCO Russia Travel Advice: https://www.gov.uk/foreign-travel-advice/russia

- US Department of State Russia Travel Information: https://travel.state.gov/content/travel/en/international-travel/before-you-go/worldcup.html and https://travel.state.gov/content/travel/en/international-travel/before-you-go.html

- Russian Embassy visa information http://www.russianembassy.org/page/fifa-world-cup-2018-visa-information and http://www.russianembassy.org/sites/default/files/documents/mig_leg.pdf

- AIPS media information: http://www.aipsmedia.com/2018/05/09/22790/football-world-cup-russia-media-operations-accreditation

- FIFA Media and Marketing Regulations https://resources.fifa.com/image/upload/media-and-marketing-regulations-for-the-2018-fifa-world-cup-2922838.pdf?cloudid=dbibgs0syrpkdbzbgbxr

## Disclaimer