Solace Global

CSOs GUIDE TO:

Executive Travel and Corporate Espionage Risks

An assessment of corporate espionage risks to travelling executives and the executive protection measures required to mitigate them.

UPDATED: **FEBRUARY 2026**

Contents

INTRODUCTION

Executive Travel and the Growing Exposure to Corporate Espionage

Business travellers, particularly those working in sensitive industries, face increasingly significant threats from espionage, surveillance, eavesdropping and proximity-based hacking. Due to the potentially high value of intellectual property (IP) and business intelligence (BI), both state and non-state actors target business travellers to access their proprietary and confidential data to gain commercial and technological advantage. Compromised information can lead to substantial financial losses, harm a company's competitive position or reputation, and may carry legal liabilities.

For US companies alone, in 2015 the FBI estimated that acts of espionage result in the theft of about USD 300 billion worth of American IP and BI each year. In 2021, the FBI reported a considerable increase in the number of corporate espionage cases being investigated, primarily linked to China. While intra-industry and criminal espionage continue to pose a threat, the threat posed by foreign states is increasing. FBI statistics indicate that at least 23 foreign states are engaged in targeting US corporations for proprietary information, although the real number is likely much higher.

In the past, stealing IP and BI was primarily conducted by rogue insiders. However, with the proliferation of smartphones, other portable devices and the expanding storage of data on cloud networks, malicious actors are increasingly able to access valuable information without leaving a trace, through a variety of both simple and sophisticated methods.

300B

Estimated worth of American intellectual property (IP) and business intelligence (BI) stolen each year due to espionage.

Airports & Hotels

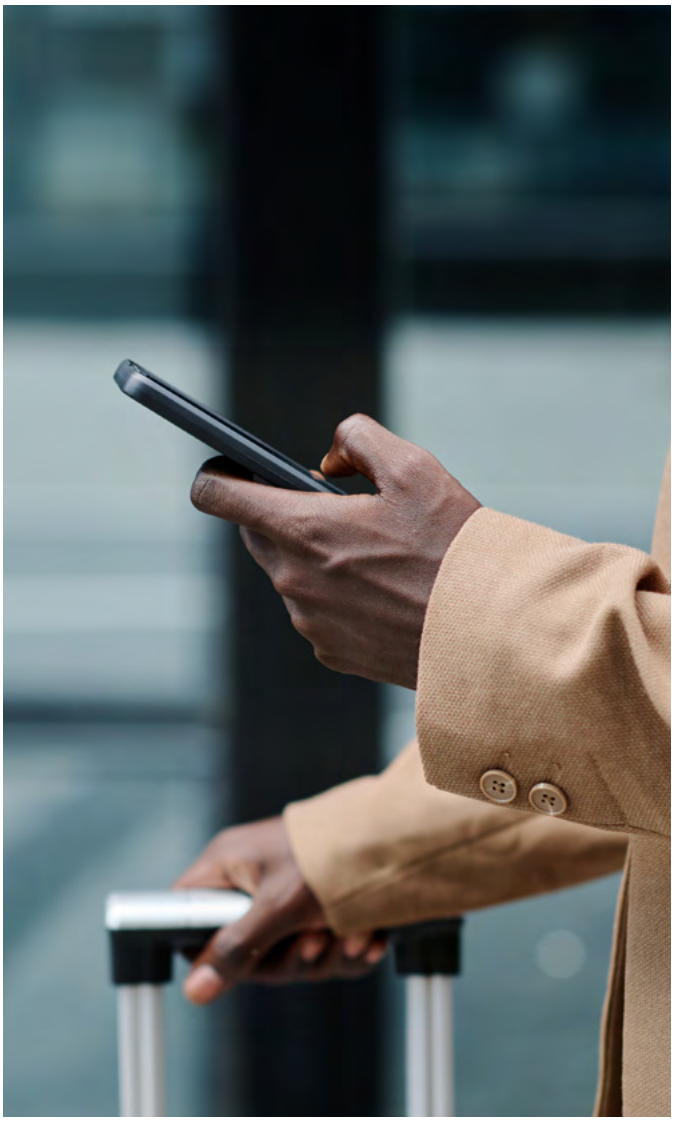
High-risk locations where business travellers face increased vulnerability to surveillance and data theft.

23

Minimum number of foreign states engaged in targeting US corporations for proprietary information (FBI statistics).

Business travellers are at a heightened risk for surveillance and data theft, particularly when travelling to high-risk locations. Business travellers navigate through airports and hotels which are hotspots for intrusion, are more vulnerable to the interception of communications, and can operate in more exposed environments without the rigorous data protection measures they may be used to. Moreover, business travellers are often in possession of sensitive information and materials, so are more likely to be considered high-value targets for espionage. External factors – such as travel fatigue and lack of familiarity with travel destinations – are also likely to make them more vulnerable to acts of espionage.

This report will examine the actors and business travel locations which pose the most credible threats, the different methods and techniques employed, and how a business traveller can mitigate these threats before travel, during travel, and after travel.



Target Industries

The most targeted industries of economic espionage are those that have significant strategic and economic importance. The defence and aerospace sectors are prime targets due to their essential role in national security and access to sensitive, classified information.

Other sectors such as advanced engineering, bioengineering, pharmaceuticals, energy, nanotechnology, semiconductors, artificial intelligence (AI) and telecommunications are also at a higher risk due to their strategic value.

However, while such sensitive industries are more at risk of being targeted, all business travellers could be potentially impacted by economic espionage and surveillance. Criminals, rival companies and state actors can all stand to gain by accessing confidential business information. Individuals or companies with access to information with less intelligence value may also be targeted through indiscriminate forms of surveillance when travelling to high-risk destinations.

KEY ACTORS & HIGH-RISK LOCATIONS

China: Elevated Legal and Intelligence Risks to Foreign Organisations

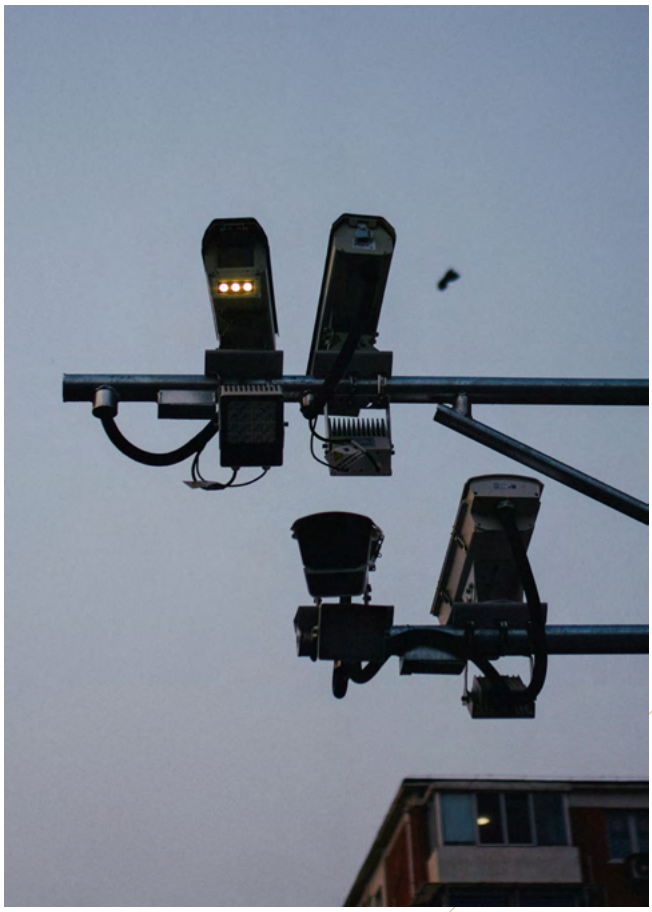
In 2021, the US Department of Justice (DOJ) reported that 80 per cent of all economic espionage prosecutions and 60 per cent of all trade secret theft cases were connected to China. The Chinese government views rapid improvement in strategically vital sectors as fundamental to ensure competitiveness with the United States, as well as with regional rivals like Japan and South Korea.

IP theft, and the illegitimate appropriation of other specialised information, benefit both the Chinese state and the country's private sector in multiple ways. Firstly, it can substantially lower research and development (R&D) costs, lower overall production costs and help to cheaply secure or maintain a competitive advantage.

Secondly, it creates a system of judicial-legal interdependence whereby perpetrator companies are incentivised to closely cooperate with state bodies in exchange for protection from legal repercussions.

The threat to business travellers in China is twofold. Firstly, Chinese intelligence agencies aggressively conduct espionage by targeting foreign companies and business travellers. Secondly, Chinese authorities leverage domestic security laws to extract information from companies and individuals operating in China or travelling through Chinese territory.

The latter efforts are legitimised by a comprehensive legal framework that Beijing has constructed over the last decade. In the summer of 2023, revisions to the National Counter-Espionage Law came into effect. The amended text expanded both the activities classified as "espionage", but more importantly, bolstered the scope of the authorities' powers to investigate them. For example, authorities were granted the freedom to access suspects' electronic devices and personal data and to summon suspects based on simple verbal orders as well as written ones.



The law's approval facilitated a series of raids on foreign companies' Chinese offices, often on unclear pretexts. Additionally, China's new Law on the Guarding of State Secrets came into effect in the Spring of 2024. The law broadens previous legislation by also guarding "work secrets", a poorly defined category of information that may cause "adverse effects" to Chinese national interest if shared.

The legislation also creates multiple and overlapping layers of monitoring bodies, from the Communist Party to local authorities and to "designated" actors operating on an ad hoc basis. As lower-level actors will be allowed to decide what constitutes "secrets", the law ensures that monitoring bodies will have almost complete discretion over controls and surveillance, making it difficult to assess the cases in which the law is likely to be applied.

The broad and arbitrary categorisation of sensitive information, and the increased monitoring efforts, will likely contribute to granting Chinese security forces more power to carry out raids and requisitions under the guise of counterespionage operations. Business travellers to China will likely be accused of carrying sensitive information out of the country as a pretext by authorities to gain access to their equipment or to exert pressure on them to disclose sensitive information via arbitrary detention and interrogation. Chinese authorities may also use the new law to increasingly impose exit bans on foreign executives in the country.

Due to the advanced and highly effective nature of Chinese espionage techniques, companies may remain completely unaware that their sensitive information has been compromised. This was the case of the US Chamber of Commerce, which in 2010 had its internal networks compromised by Chinese hackers, Four Asia policy experts who had travelled to China were used as a "beachhead" for the cyberintrusion. The cyber theft was carried out over a period of months, until it was discovered by the FBI. Later, an office printer and a thermostat in a corporate apartment were found to still be communicating with a China-based internet address.

In 2022, the UK's domestic intelligence service MI5 was undertaking seven times as many investigations relating to Chinese espionage compared to 2018. The current director of the FBI, Christopher Wray, has warned that Chinese economic espionage is being conducted "on a massive scale", and that it has become a "central component of [China's] national strategy".

Due to the risk posed by commercial espionage in China, large consultancy firms have undergone or are in the process of undergoing efforts to fully decouple their data in China – instead ensuring that their data in China is fully localised and completely isolated from global IT systems to prevent unauthorised access or breaches.

> The Chinese government views rapid improvement in strategically vital sectors as fundamental to ensure competitiveness with the United States, as well as with regional rivals like Japan and South Korea.

The broad and arbitrary categorisation of sensitive information, and the increased monitoring efforts, will likely contribute to granting Chinese security forces more power to carry out raids and requisitions under the guise of counterespionage operations. Business travellers to China will likely be accused of carrying sensitive information out of the country as a pretext by authorities to gain access to their equipment or to exert pressure on them to disclose sensitive information via arbitrary detention and interrogation. Chinese authorities may also use the new law to increasingly impose exit bans on foreign executives in the country.

Due to the advanced and highly effective nature of Chinese espionage techniques, companies may remain completely unaware that their sensitive information has been compromised. This was the case of the US Chamber of Commerce, which in 2010 had its internal networks compromised by Chinese hackers, Four Asia policy experts who had travelled to China were used as a "beachhead" for the cyberintrusion. The cyber theft was carried out over a period of months, until it was discovered by the FBI. Later, an office printer and a thermostat in a corporate apartment were found to still be communicating with a China-based internet address.

In 2022, the UK's domestic intelligence service MI5 was undertaking seven times as many investigations relating to Chinese espionage compared to 2018. The current director of the FBI, Christopher Wray, has warned that Chinese economic espionage is being conducted "on a massive scale", and that it has become a "central component of [China's] national strategy".

Due to the risk posed by commercial espionage in China, large consultancy firms have undergone or are in the process of undergoing efforts to fully decouple their data in China – instead ensuring that their data in China is fully localised and completely isolated from global IT systems to prevent unauthorised access or breaches.

KEY ACTORS & HIGH-RISK LOCATIONS

Hong Kong: Reduced Legal Safeguards and Expanded Security Oversight

For decades, Hong Kong has served as a key hub for global business, having been governed under the "one country, two systems" constitutional principle since the 1997 handover from the UK to China. Since the Chinese government's crackdown following the 2019 protests, however, Hong Kong's legal and business environment has changed rapidly.

In 2020, the passing of the National Security Law either criminalised or increased penalties for a series of activities deemed to be potentially "subversive". As in China, authorities were granted substantial freedom to monitor and access information carried by suspects, including foreign nationals.

Due to the increasingly high-risk profile of Hong Kong for commercial espionage, multiple major international audit and consultancy firms now ask their staff to use burner phones when visiting Hong Kong, a measure that has been advised for years by companies working in the aerospace and semiconductor industries.

KEY ACTORS & HIGH-RISK LOCATIONS

Russia: Extensive Surveillance and Lawful Interception Capabilities

Russia carries out espionage activities against Western businesses and business travellers as part of its broader campaign of "hybrid warfare" and to gain a competitive advantage over its Western adversaries.

Russia's over-reliance on fossil fuels, relative international isolation and lack of economic diversification make the theft of foreign technology highly desirable for the Kremlin in its bid to reduce Russia's dependence on foreign technology. This has only increased since the beginning of the war in Ukraine and the imposition of sanctions which have further isolated Russia.

While China formally denies IP and BI theft and its involvement in state-sponsored espionage, Moscow's efforts are formally recognised by the government and explicitly linked to national security questions and its strategic opposition to Western states. After the 2022 invasion of Ukraine, the Russian government implemented a decree allowing local companies and individuals to utilise patents from "unfriendly countries" without compensating the patent owners, setting the compensation rate at 0%.

Moreover, Russia has had a long-standing system of Operative Search Measures (SORM) which allows various state agencies to lawfully and freely intercept emails or text messages, and to analyse Internet usage. Russia's telecommunications surveillance system ensures there is no expectation of privacy for operators within its borders, putting business travellers at risk of extensive state monitoring and data collection.

As part of the measures established by the legislation, Internet Communications Organisers (IOC) are expected to store all communications data and content generated by Russia-based Internet users for a set period of time depending on the type of data

In 2022, the US Embassy in Moscow issued an official alert stating that US citizens entering Russian territory had their electronic devices – including mobile phones – searched upon arrival. Access to devices, even for brief periods of time, likely allows Russian officials to "vacuum" them for information. Russian-based private companies, like Elcomsot, have developed phone-breaking software that bypass the standard security measures installed on mobile phones and other forms of electronic devices.

This technology, which is likely widely used by Russian intelligence, combined with Russia's other methods for surveillance, has created a high-risk environment for business travellers.

KEY ACTORS & HIGH-RISK LOCATIONS

France: State-Backed Economic Intelligence Practices

France has long adopted a policy of encouraging cooperation between state intelligence and private businesses to obtain a competitive advantage over international rivals. The extent and pervasiveness of French economic espionage demonstrate how it is not limited to authoritarian states.

During the early Cold War, French intelligence targeted American and other Western businesses in an effort to benefit its own private sectors. These operations, which were described as "aggressive and massive" primarily focused on security-related sectors, including aviation and telecommunications. Alleged efforts include Air France first class seats being reportedly bugged with listening devices by Directorate-General for External Security (DGSE) operatives, to target foreign business executives travelling to France.

The rise of the threat from international terrorism has forced Paris to invest more of its intelligence resources in counterterrorism operations. However, acts of state-sponsored have continued, with more attention directed towards the cyber domain.

In 2013, a US National Intelligence Estimate placed France alongside Russia and Israel as one of the main users of cyberespionage targeting international private companies or their employees. In the same year, the DGSE's structure was rendered public via a government decree, showing that one of its four subsections, the Economic Security Service (ESS), was dedicated to public-private cooperation in intelligence gathering and the exploitation of the information obtained.

The collection of foreign economic information has long been a policy of the French state. While its operational tempo has likely decreased compared to the heights of the 1980s, DGSE operations have continued. In 2022, the former head of the intelligence agency was indicted for a 2016 attempt at extorting a Franco-Swiss businessman, who was reportedly detained at a Paris airport by DGSE agents and threatened.

> In 2013, a US National Intelligence Estimate placed France alongside Russia and Israel as one of the main users of cyberespionage targeting international private companies or their employees.

KEY ACTORS & HIGH-RISK LOCATIONS

Commercial Competitors: Covert Collection for Competitive Advantage

Corporate actors are also commonly involved in espionage. While this may be carried out on behalf of or in collusion with state actors, it is often conducted independently by a business to obtain a competitive advantage over rivals. Numerous companies employ a range of covert tactics to access sensitive information and technology, often utilising advanced techniques and substantial resources more reminiscent of a state actor.

In 2017, the private car hire company Uber was reported to have spied on other companies via a dedicated internal unit known as the Strategic Services Group (SSG). In a letter by a former senior employee, Uber was accused of using a variety of methods to gather intelligence on self-driving technology by competitor Waymo.

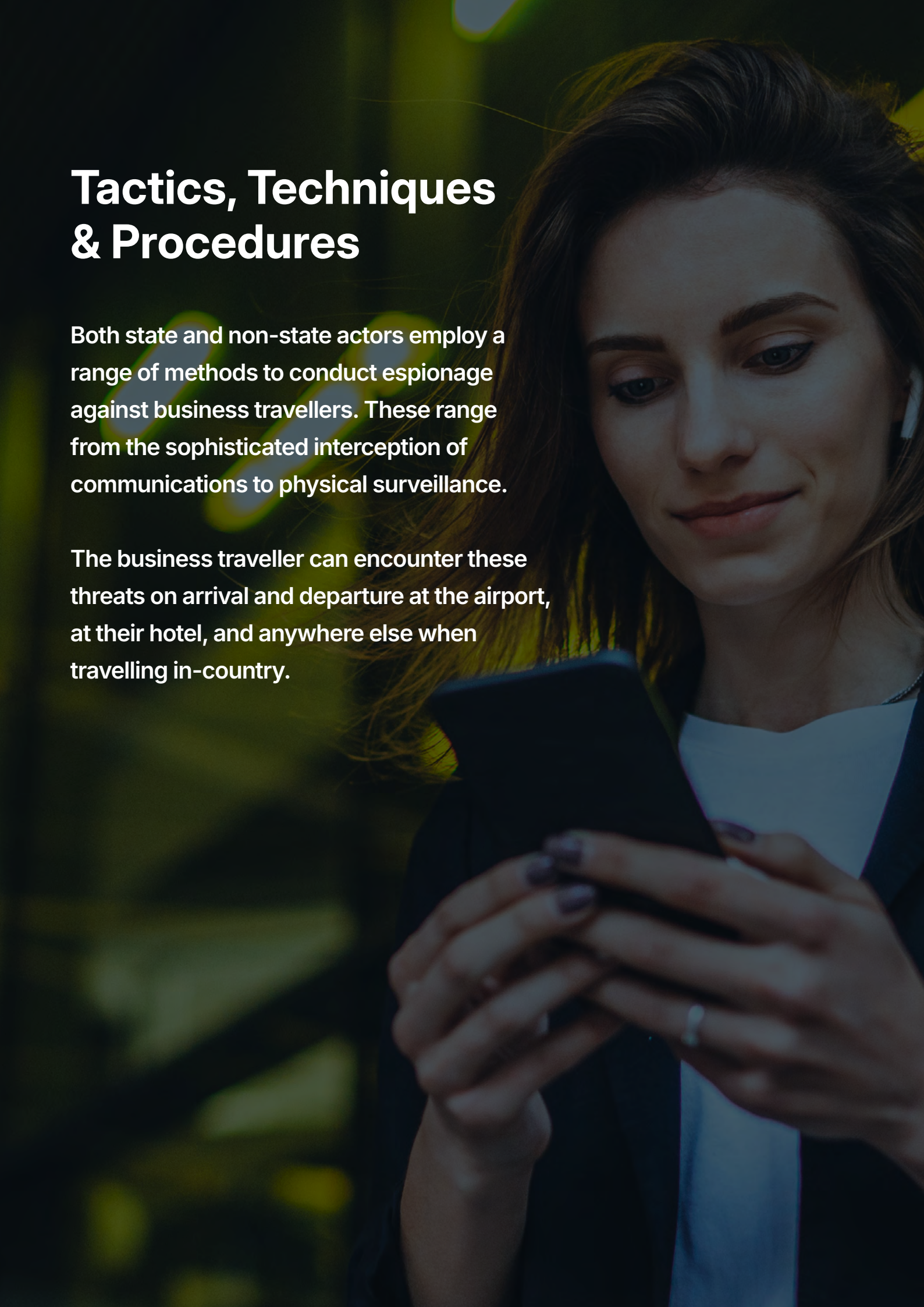
SSG members reportedly followed and videotaped Waymo's experimental vehicles during testing, "impersonated drivers" and "infiltrated" events and facilities used by the competitors' executives. These operations were reportedly carried out alongside cyber operations to gather data on rival technology and internal research on self-driving vehicles.

In 2014, a British private investigator was sentenced to more than two years in prison in China for illegally gathering information for the major pharmaceutical company GaxoSmithKline (GSK). The UK citizen was accused of using a variety of methods, including tailing targets and photographing them, in order to obtain sensitive information on Chinese nationals. The detective had been hired by GSK to investigate a reported sex tape of the company's head of operations in China, which had been sent to other company executives.

Tactics, Techniques & Procedures

Both state and non-state actors employ a range of methods to conduct espionage against business travellers. These range from the sophisticated interception of communications to physical surveillance.

The business traveller can encounter these threats on arrival and departure at the airport, at their hotel, and anywhere else when travelling in-country.



TACTICS, TECHNIQUES & PROCEDURES

Airport: Device Seizure and Rapid Data Extraction Risks

SEIZURE/CONFISCATION OF DEVICES

Business travellers can have their sensitive data accessed upon arrival to a country, by border security agencies and intelligence agents operating in an airport. As a condition of entry, authorities can demand physical access to devices such as laptops or phones. Typically, when crossing international borders legal protections against warrantless search and seizure do not apply. In the US, for example, the Fourth Amendment's constitutional protection against unreasonable search and seizures by the government is given legal exemption at international borders.

Even with temporary device seizures, advanced phone-breaking software and data extraction tools can rapidly retrieve extensive amounts of potentially sensitive data within minutes. Using such tools, security services can bypass device passwords, encryption and other security measures on phones, laptops and tablets, to "vacuum" vast amounts of data to be subsequently collated, processed and analysed.

TACTICS, TECHNIQUES & PROCEDURES

Hotel: Vulnerability to Intrusion and Monitoring

BUGGING/EAVESDROPPING DEVICES

Miniature, inconspicuous microphones and cameras can be hidden in everyday items in hotel rooms such as smoke detectors, fire alarms, light fixtures, electrical outlets, furniture, docking stations, air-conditioning vents, coffee pots, landline phones and clock radios. In fact, any speaker can be turned into a microphone, such as the speakers on a television. Such devices can be permanently placed in hotel rooms and remotely activated, or planted in anticipation of a particular business traveller's stay.
Intrusion

INTRUSION

Individuals can gain physical access to a business traveller's hotel room while it is vacant, seeking to examine any belongings, plant eavesdropping devices and/or attempt to extract data directly from any devices. Intruders may also replace commonly used phone chargers with identical devices which have malicious software installed, enabling future cyber attacks.

Anywhere: Remote Interception of Communications and Conversations

REMOTE INTERCEPTION

Governments and malicious actors can remotely monitor communications and access sensitive data through numerous methods:

Lawful interception

It is legal in many states for authorities to intercept communications, and/or collect the metadata from communications. Legislation may compel network providers to record communications and collect data, which can then be accessed by a state's intelligence agencies.

Stingrays

International mobile subscriber identity-catchers (IMSI-catchers, or Stingrays) simulate wireless carrier cell towers, tricking mobile devices into connecting to them instead of legitimate cellular networks. These can be used to conduct location tracking, intercept calls/texts, harvest data and the delivery of malware (such as through a malicious carrier update).

Wi-Fi

Man-in-the-middle attacks can use fake Wi-Fi networks that may appear legitimate, such as a network that ostensibly claims to be a hotel or airport business lounge Wi-Fi network, to lure connections and expose users to surveillance and cyberattack.

Bluetooth

Bluetooth has multiple vulnerabilities that can be exploited, with "Bluesnarfing" and "Bluebugging" enabling unauthorised access to Bluetooth-enabled devices.

PHYSICAL SURVEILLANCE

Real-time physical observation of business travellers can be conducted by highly trained and covert operatives to gather intelligence. Operatives may seek to physically overhear sensitive conversations, or may just be recording movements, meetings, locations and activities.

ELICITATION

Personnel trained in elicitation techniques can subtly engage with business travellers, seeking to acquire valuable information from casual conversation. This most typically happens in locations such as a hotel bar, restaurant, conference or business function, but can happen anywhere, including over the internet or phone.

HONEY TRAPS

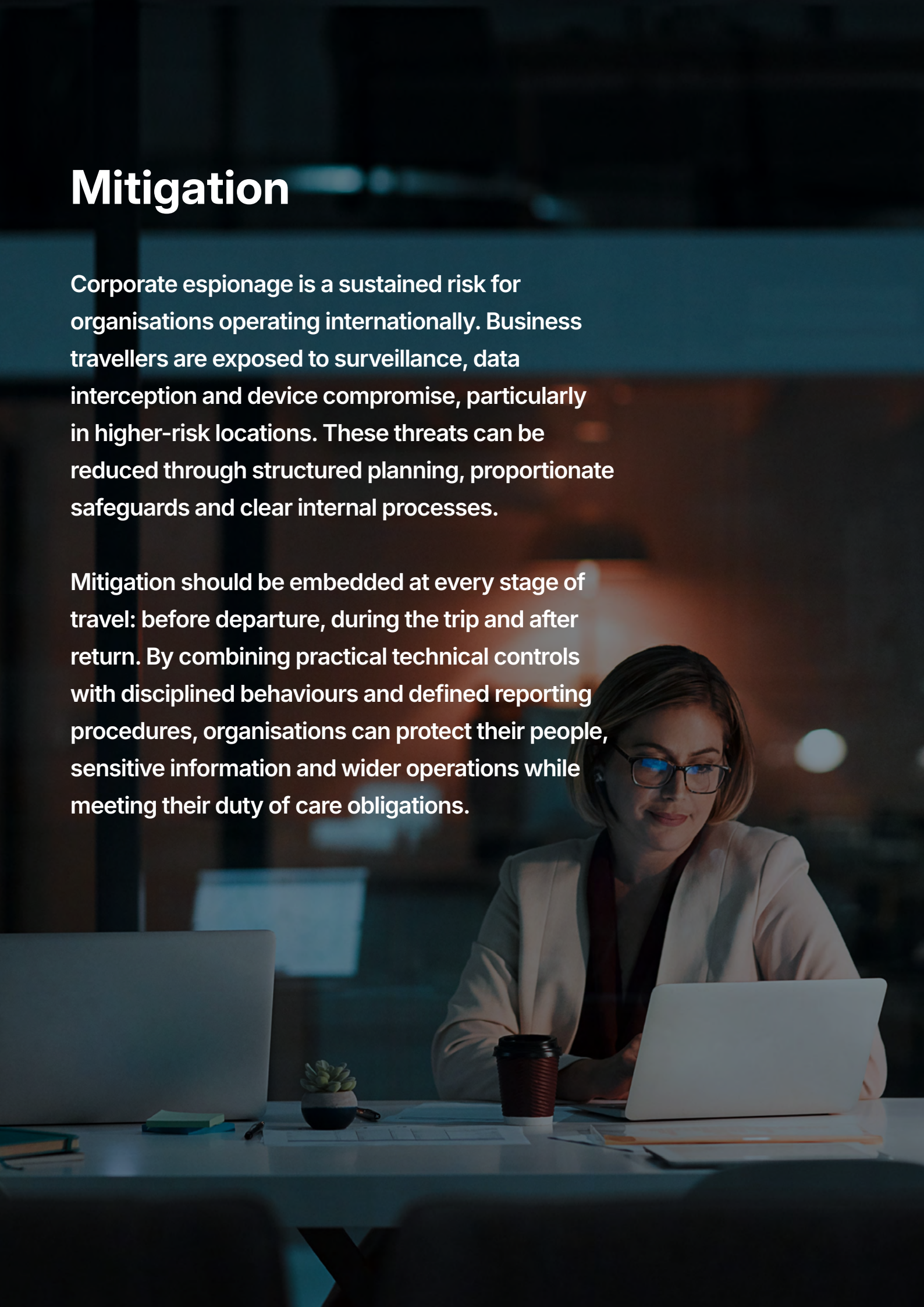
The exploitation of personal or sexual relationships has been conducted by multiple intelligence agencies. Trained operatives or accomplices can deceptively manipulate a target to engage in sexual relations. This tactic can firstly be deployed as a method to gain trust, to gain information through conversational elicitation techniques or to gain access to the target's room.

Secondly, honey traps can be used to blackmail the target for confidential information. There have also been cases, such as in Russia, of authorities arresting victims on charges of sexual assault following encounters with honey traps, charges which can then be used to pressure a target to disclose information or collaborate with intelligence services.

Mitigation

Corporate espionage is a sustained risk for organisations operating internationally. Business travellers are exposed to surveillance, data interception and device compromise, particularly in higher-risk locations. These threats can be reduced through structured planning, proportionate safeguards and clear internal processes.

Mitigation should be embedded at every stage of travel: before departure, during the trip and after return. By combining practical technical controls with disciplined behaviours and defined reporting procedures, organisations can protect their people, sensitive information and wider operations while meeting their duty of care obligations.



MITIGATION

Pre-Travel: Limiting Data, Defining Red Lines and Assessing Risk

KNOWLEDGE

Understand the specific threat environment of the location being visited. Be informed of the most typical threats of espionage in the specific country, and how to mitigate against those.

Legal Compliance

Make sure you are informed about the legal and legislative landscape, including laws regarding data protection, technology use and business practices to avoid inadvertently violating any regulations. Learn about the country's IP laws and how they are enforced from a reliable source such as the UK Intellectual Property Office (IPO). Some countries, such as Saudi Arabia, Russia and China require import licenses for encrypted data – make sure you understand the import control laws of the country and what licenses may be required.

Risk Assessment

Produce or acquire a risk assessment for the trip, specific to the destination, the traveller's specific risk profile, and the sensitive data or information that will be taken or disclosed. Have an established process for reporting incidents, such as a suspicious encounter or missing/stolen laptop, and pre-planned measures to carry out in place if such incidents take place. Identify the physical assets that will be brought and the specific data they hold, and assess what level of protection measures they require. Assess the risk and impact of the assets and/or data being compromised.

RED LINES

Establish red lines for what information you and your company are willing to share, and with who, to achieve the objective of the business trip. Specifically set out what information cannot, under any circumstances, be talked about, shared or even brought into the destination country.

LOANER DEVICES

Strongly consider setting up the use of loaner devices. Loaner devices are devices temporarily given to the business traveller, such as a laptop or mobile phone, specifically for use during the trip. However, a major vulnerability of these is that they may be associated with a sensitive site, business or employee if repeatedly used by a business.

Even if they are scrubbed of sensitive data, a loaner device's association with a high-value target could be a starting point for other forms of surveillance.

BURNER PHONES

A burner phone is a low-cost, disposable mobile phone that allows users to make calls and send texts without a long-term contract or personal identification. These are typically sold with pre-paid credit and are a superior alternative to loaner devices. The major advantage of a burner phone is that they are not associated with an individual or company.

However, the use of a burner phone may lead hostile actors to attribute it to a particular business or location. If possible, burner phones should be purchased inside a destination country by a "fixer" and always paid for in cash. If this is not possible, burner phones can be purchased within a physical store rather than online and paid for in cash to avoid leaving a digital footprint.

DATA REMOVAL

Ensure all devices have had all data/files that are not essential to the trip removed.

PROTECT DEVICES AND ACCOUNTS

Devices and accounts should be protected with strong passwords (unique to each account and device), biometric identification (such as fingerprint recognition), and 2-step verification if possible.

APPLICATIONS AND SETTINGS

Ensure that all software and applications are fully updated, antivirus software activated, USB autorun is disabled, and automatic connection to Wi-Fi networks disabled. Only use trusted applications from official providers.

VPN

If legal in the destination country, set up the use of a Virtual Private Network (VPN). A VPN routes internet traffic through a remote server, masking the user's IP address and making the user harder to track. Make sure you are informed on how the VPN works, and what to do if you encounter issues with its use.

ENCRYPTION

Consider the use of device-wide encryption, if legal/the appropriate licenses are acquired. If illegal, authorities may use device encryption as an opportunity to confiscate the device.

REMOTE WIPING

Ensure that, if possible, devices can be remotely wiped of data if they are compromised. Burner phones should never be taken to the office or sensitive sites, as their presence could link them to specific businesses or industries, making it easier for foreign intelligence services to attribute the device to your organisation, which could lead to other forms of surveillance.

MITIGATION

During Travel: Maintaining Security Discipline in Dynamic Environments

ARRIVAL

Check in at a pre-arranged point with someone upon arrival and inform them of any itinerary changes.

HOTEL

Hotel safes can be used for the storage of valuables, but should not be used for storing sensitive information as capable actors can gain access. Always carry sensitive information on your person and never leave it unattended.

BUG SWEEP

There are measures that can be taken to sweep a room for bugs or cameras – however, always assume eavesdropping and act accordingly.

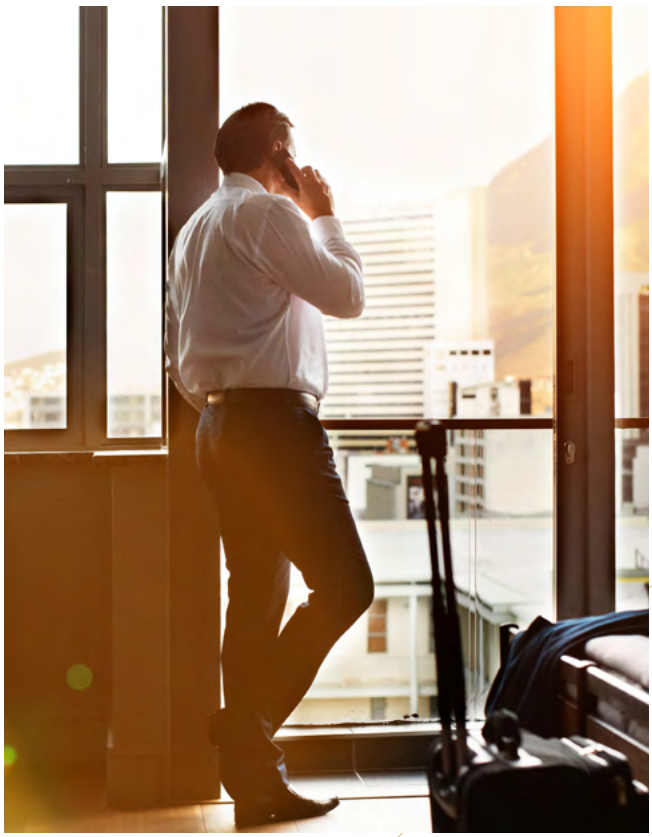
Detectors

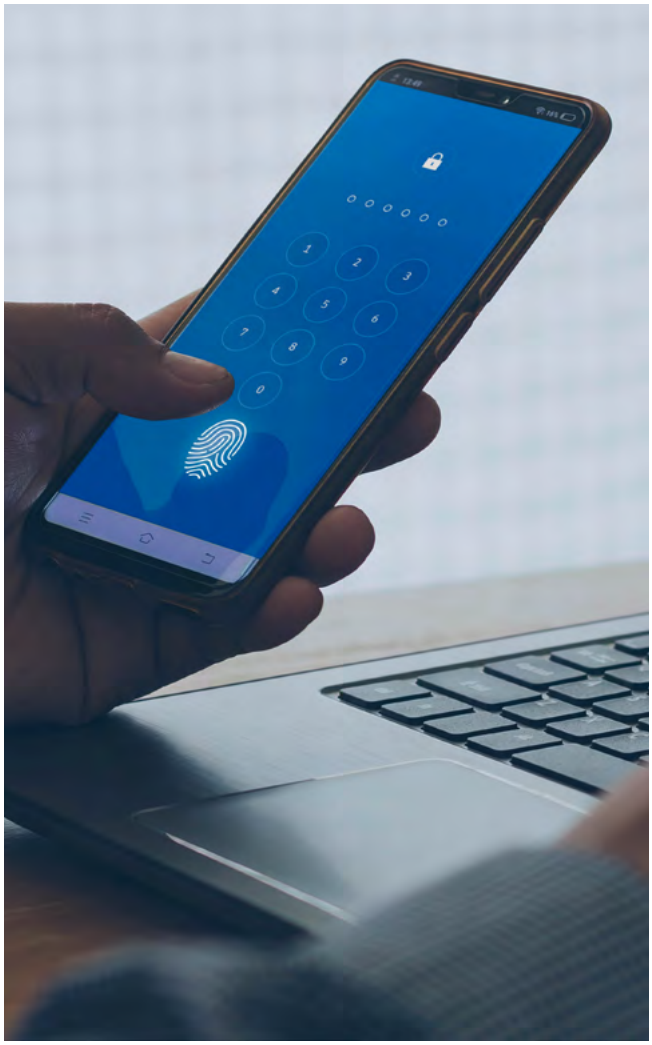
Phone applications such as Hidden IR Camera Detector or camera detector devices can be used to detect hidden monitoring devices, however these do not have comprehensive efficacy.

Physical Inspection

It may be possible to find physical evidence of covert monitoring. Examine objects that are typically used, such as smoke detectors, fire alarms, light fixtures, electrical outlets, furniture, docking stations, air-conditioning vents, coffee pots, landline phones and clock radios.

Examine the walls for any discolouration which indicates new paint/plaster. Examine any objects for stripped screws. Pick up the room's landline phone and check for any unusual static or sound. Close the curtains, turn off the lights, and then use a phone flashlight to reveal slight reflections – camera lenses reflect light.





REPORT

Using the pre-established reporting process, report any suspicious approaches or activity (online or in person) as soon as possible.

WI-FI

Avoid or restrict the use of any public, airport or hotel Wi-Fi. Hostile actors will often establish fake or “Evil Twin” networks to intercept data from unsuspecting users.

FARADAY BAGS

Consider using Faraday bags for phones and devices. These provide a shielded enclosure that blocks electromagnetic fields, stopping radio frequency signals from entering or leaving the bag. This prevents the stored electronic device from receiving or transmitting data via Wi-Fi, Bluetooth, GPS, cellular networks and other forms of wireless communications.

MESSAGING

Use an end-to-end encrypted messaging platform to communicate, such as Signal. While service providers may still be able to access metadata and such encryption is not impossible to penetrate, end-to-end encryption offers strong protection against unauthorised surveillance.

COUNTER ELICITATION

Be vigilant of elicitation techniques. If pressed to go beyond pre-established red lines, be polite but firm in refusing to divulge information.

MITIGATION

Post Travel: Detecting and Containing Potential Compromise

REPORT

Sometimes suspicious incidents may only be recognised post-travel, or suspicious approaches may take place post-travel. Ensure all such incidents are reported.

RESET PASSWORDS

If there is any suggestion whatsoever of account/device tampering, reset passwords and account credentials. If travelling to a high-risk location, this measure should be applied in all instances out of an abundance of caution.

RETURN LOANER DEVICES

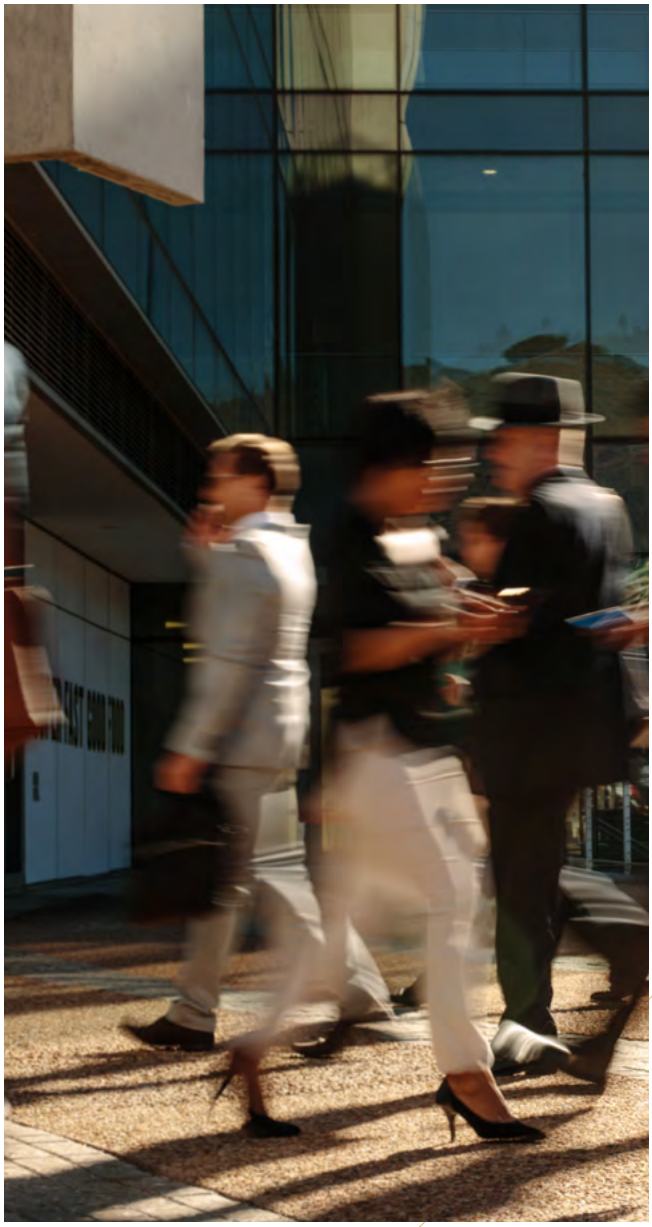
Return any loaner devices used and if used, devices should be checked for any signs of tampering, and any unusual device behaviours (such as unusual battery or system performance) should be reported.

DISCARD BURNER PHONES

Wipe the phone of any data and discard phones securely. If possible, phones should be discarded within the country of purchase. This can involve physically breaking the device or using specialised tools to ensure that all data is irretrievable. Never reuse a burner phone.

POST-TRAVEL ASSESSMENT

To improve procedures and support provided for future travel, a post-travel assessment of encountered risks, incidents, deployed mitigation measures and systems should be conducted. The assessment should gather feedback from all personnel involved to evaluate the effectiveness of current protocols and identify any security gaps. Regular reviews of these assessments should be integrated into the organisation's standard operating procedures to ensure ongoing improvement in travel security measures.



ABOUT SOLACE GLOBAL

Solace Global Risk is a leading provider of comprehensive risk management solutions, serving clients globally with a commitment to excellence. With a worldwide presence and a team of seasoned experts, Solace Global Risk empowers organisations to navigate complex risk landscapes with confidence and resilience. Visit solaceglobal.com

Solace Global

+44 (0)1202 308 810
info@solaceglobal.com
www.solaceglobal.com