PREPAREDNESS FOR CBRN(e) ATTACK
EXECUTIVE SUMMARY

SUMMARY

This issue of Constellis’ Kidnap for Ransom Insight Report covers global kidnapping incidents and trends over the months of March and April 2018, as well as the start of May. The information is derived from multi-source analysis of kidnap for ransom activity and where known, the outcome or resolution of the event. The report covers current kidnap for ransom hotspots at the regional, national and provincial level with particular focus on areas where K&R activity is increasing.

Statistical analysis of data for March and April 2018 is included on page 15, which graphically displays K&R trends by region, victims by nationality and employment sector, as well as identifying the Top 10 countries for kidnapping of foreign nationals over the reporting period.

The Global Piracy Update offers an overview of the piracy threat by region, providing trend analysis for March and April of 2018. It also offers sample cases occurring through those months, providing an illustration of the identified trends.

The Cyber Security section examines current issues affecting companies and individuals in the realm of IT security. This edition will look at the increasing threat of cybercrime to mobile devices. Mobile malware has seen exponential growth over the past year, with cyber-criminals exploiting the popularity of mobile internet-connected devices to fraudulently generate millions of dollars. As with PC cybercrime, attacks on mobiles are mostly financially motivated. Despite improved security of devices and enhanced vetting of online app stores, the number of malware attacks on mobile devices spiked towards the end of 2017, with over 16 million detections recorded. At its current trajectory, it is forecasted that mobile malware will be a multibillion-dollar industry by 2020.

The Focus Article offers an insight onto organisations’ preparedness for a Chemical, Biological, Radiological, Nuclear and Explosive (CBRN(e)). A number of recent intelligence briefings seem to indicate the terrorist threat will diversify in methodology and will be particularly dynamic in nature. With terrorists certainly having a clear intent and capability for highly dramatic attacks, a CBRN(e) attack in the form of a dirty bomb is not out of the realm of possibility. In an era of ‘high-impact high-probability events’, organisations thus need to guarantee that their current organisational resilience plans will be effective in the occurrence of such an incident.
GLOBAL OVERVIEW

AMERICAS

During the period of March-April 2018, the Americas accounted for about a quarter of all incidents recorded by Constellis globally. Although observing a small decrease in the number of foreign victims with respect to the previous reporting period, regional figures remain well above bimonthly averages recorded in 2017. Mexico continues to lead the region’s statistics as the exponential increase in violence levels has also been reflected in the incidence of kidnapping in the country. According to Alto al Secuestro, an NGO specialising in the monitoring of the kidnapping problem in Mexico, at least 10,898 kidnapping events have been reported so far during the current administration (December 2012-March 2018). This figure, the highest ever recorded in Mexican history, is attributed to an overall failure of the security strategies planted by President Pena Nieto, including those especially focused on kidnapping. Much of this failure has been linked to the pervasive corruption within the government apparatus, by which the extensive funds dedicated to security were diverted or not used effectively. With general elections next July, security is at the forefront of the political campaigns. In this regard, candidates themselves are at the centre of the problem, with many of them targeted in recent months in politically-motivated kidnappings and murders.

CASES:

Following the kidnapping and murder of three Italian nationals in January in Jalisco state, a similar incident took place in the same area in March. On 19 March, three local film students were kidnapped by a group of armed men while shooting a short film near the city of Guadalajara. The assailants reportedly identified themselves as members of the state’s prosecutor office and took them to an unknown destination. Their families never received a ransom call. It was not until 23 April that Mexican authorities confirmed the students’ deaths. Investigations revealed that the victims were ‘interviewed’ and tortured before they were killed, after which their bodies were dissolved in acid. The authorities said there were no indications that the students had connection to any criminal gang. It was then concluded that the victims might have found themselves inadvertently caught in an ongoing cartel conflict, in which members of the Cartel Jalisco Nueva Generación (CJNG) may have confused the students with members of a rival drug cartel. While it was rumoured that the Italians were involved in criminal activities that may have made them a target for the cartel, the students’ case illustrates the threat cartel violence presents to common citizens on a daily basis in certain areas of the country. The U.S. Department of State assesses Guadalajara as a high-threat location for crime, including cartel activity.

While virtual kidnapping schemes are typically associated with Latin American countries, these incidents are also recorded in North America. In a trend identified since 2017, Chinese students have been the target of such schemes throughout Canada. While declining by the end of the year, following strengthened law enforcement combined with an education campaign by Chinese diplomatic authorities, this has once again resurfaced. Since April 2018, numerous cases have been reported in a number of Canadian regions, including Ontario and British Columbia.

CASES:

In separate incidents in early May, two Chinese students in Vancouver were targeted by phone by criminals posing as members of the Chinese consulate. The callers reportedly requested cooperation as part of a police investigation or threatened the victims to prosecute them for an alleged crime in China. Victims were then convinced to send videos to their relatives in China, indicating they had been kidnapped. The students were also convinced to switch off or destroy their phones, avoid social networks and relocate to a motel. Meanwhile, the criminals demanded a ransom from their relatives who could not reach the alleged victims. The local police confirmed that a “substantial” amount was obtained by the perpetrators in these two cases, but did not specify the sum. According to police records, 20 such crimes were reported in Vancouver in 2017 and two so far in 2018. Three of those cases reportedly resulted in cash transfers. The police believe the suspects are operating from China.

In Colombia, while reaching a historical milestone with the political participation of the Revolutionary Armed Forces of Colombia (FARC) in the March legislative elections, the country continues to experience violence derived from conflict on other fronts. Hostile activity is particularly concentrated in border areas with Venezuela and Ecuador. To the northeast, since March 2018, the remaining guerrilla group, the National Liberation Army (ELN), has resumed its attacks against government targets and infrastructure. Additionally, the group is currently waging a turf war with the remnants of the Popular Liberation Army (EPL), also known as ‘Los Pelusos’, for the control over drug trafficking routes in Norte de Santander, a major Colombian coca-producing region. Meanwhile, in the southwest, FARC dissident groups have continued their criminal activities, engaging rival groups and authorities. This particular focal point has had consequences beyond the security domain, affecting Colombia in its diplomatic relations with Ecuador and thus, potentially affecting the peace process with the ELN.

CASES:

Two journalists for Ecuadorean newspaper El Comercio and their driver were abducted on the Colombia-Ecuador border on 26 March. It is not clear where exactly the incident took place, with both the Colombian and Ecuadorean authorities claiming it occurred outside their country borders. The perpetrators of the kidnapping were identified to be members of the FARC dissident Oliver Sinisterra unit, which is led by an Ecuadorean man known as ‘El Guacho’. Nine days after the kidnapping, a Colombian television channel released the first proof of life of the Ecuadoreans. The 22-second video showed the three chained hostages pleading with the Ecuadorean government for their release. In the video, the victims also inform of their captors’ demands, consisting of the release of three men imprisoned in Ecuador and that the Ecuadorean government cancels an anti-terrorism agreement with Colombia. On 11 April, the kidnappers released a communiqué announcing the death of the three hostages, blaming them on the governments of Colombia and Ecuador, which allegedly refused to negotiate and instead chose a military response. It is reported that the last communication between the Ecuadorean government and Guacho was on 7 April, when Ecuadorean authorities had sent him a video of one of the FARC prisoners and just affirmed the release process was at its final stages. The Ecuadorean authorities confirmed the deaths on 13 April, a day after Colombian channel RCN presented photos of three bodies allegedly belonging to the victims. The bodies have not yet been recovered. Later, on 17 April, El Guacho’s group kidnapped an Ecuadorean couple in the same area. The group has followed the same negotiation tactics in this case, having the same demands. The couple remain missing at the time of writing. In the aftermath of both cases, Ecuador’s government announced it will no longer host negotiations between the Colombian government and the ELN.
An important increase in the number of cases of kidnapping targeting foreign nationals was observed in Europe during the reporting period. This almost three-fold increase was brought about mainly by a number of incidents recorded as part of the Turkish government’s pursuit of Turkish nationals linked to the Gülen movement. Locally known as FETÖ, the movement is accused of having orchestrated the July 2016 failed coup. In the frame of these covert operations by the Turkish Secret Services (MIT), over 80 Turkish nationals alleged to be members of FETÖ have been kidnapped since the coup during operations carried out in over 18 countries, including European countries such as Kosovo and Bulgaria. “Arrested” individuals are known to have been brought back to Turkey for imprisonment. It is unclear if any of these operations took place with the knowledge or acquiescence of local authorities.

Other cases that contributed to incidence levels observed in Europe over March and April were linked to common criminality. Although limited in comparison to other regions in the world, these type of incidents are not uncommon in Europe. Having said that, most reported cases are resolved with the arrest of the perpetrators, commonly during rescue operations mounted by local security forces.

CASES:

On 29 March, it was reported that six Turkish nationals were kidnapped in Pristina, Kosovo, by the Turkish Secret Service (MIT) and covertly taken to Turkey on a charter flight. The six were alleged to have links to schools funded by Fethullah Gülen. The operation sparked a political crisis in Kosovo. While the Kosovo Ministry of Interior stated that the residence permits of the six persons had been revoked after their arrest for “security reasons”, both the Prime Minister and President claimed they had not been informed of the operation. In the aftermath of the incident, Kosovo’s Prime Minister, Ramush Haradinaj, dismissed the Minister of Interior and other top security chiefs over their involvement in the operation. Later, a senior official in the Kosovo government told the media that the Kosovar authorities had been under “tremendous pressure” from Turkey in recent weeks to take action against Gülen schools and their staff.

In Spain, on 30 March, police in the locality of Arona, Tenerife, rescued a kidnapped couple, an Italian man and a Brazilian woman. During the operation, the perpetrator, a man of Italian nationality, was also arrested. According to reports, the victims had been held at gunpoint inside their own house and the attacker demanded €12,000 in bitcoin for their release. The kidnapper later released the man, to allow him to go into town to make the transfer, threatening to kill his partner, still held at home, if he did not return with proof of the transfer. Instead of complying, the victim reported the incident to the authorities, who immediately responded and instructed the man to arrange the meeting with the kidnapper. The assailant, believing he was going to receive the proof of payment, was arrested at the meeting point. It is not clear if the victims knew their captor.
The Middle East has continued to show low levels of reporting of kidnappings involving foreign nationals, a trend observed since 2016, but which has been more pronounced since the beginning of 2018. This however, is not an indication of a reduced threat. It is rather an indication of a larger targeting of local nationals, who typically apply lesser levels of security measures and whose abduction does not spark as much attention from the local authorities. A number of countries in the Middle East, such as Iraq, Syria and Yemen, are commonly identifiable for their high levels of kidnapping as a result of high levels of criminality in a context of armed conflict. Conversely, the Middle East is home to some of the countries considered among the safest in the world, outside a geopolitical context. This is the case of the United Arab Emirates, where crime rates are relatively low and instances of crime are unlikely to affect foreign travellers. While violent crime very rarely affects western expatriates, crimes among the immigrant labour population occur relatively frequently. These include instances of kidnap for ransom, which are commonly linked to personal and economic disputes.

Likewise in Iran, crime, especially violent crime, does not pose a significant security concern, with kidnapping for ransom remaining a rare occurrence in the country. Foreign travellers are most likely to be affected by non-violent crimes of opportunity, such as petty theft. Nonetheless, a threat of illegal detention remains in the country, particularly to nationals of countries with strained diplomatic relations with the Iranian regime. In this regard, dual nationals are at a heightened risk as the Iranian authorities do not recognise dual nationality, which also means that consular access may not be granted.

**CASES:**

- On 3 May, Dubai authorities said that three Asians were being processed for the kidnapping of an Asian driver and another man. The accused, dressed in military uniforms, showed at the victims’ residence in the area of Rashadiyah, and requested the victims to accompany them to the district police station. The accused reportedly based their request on the grounds that the victims were living in a families-only area and as such, they would be fined 60,000 dirhams (USD 16,300). The victims obliged, but instead of going to the police station, the criminals kept them hostage inside the car. The victims were reportedly beaten throughout their ordeal and driven around the area for five hours until they managed to pay the men 40,000 dirhams (almost USD 11,000) for their release.

In Iran, on 13 March, a foreign national of unknown nationality was rescued in a police operation a week after he was abducted by gunmen in the city of Mashad. The kidnappers reportedly demanded a ransom of €100,000 from the hostage’s relatives, who then notified the authorities. An unknown number of kidnappers were arrested during the operation.
Africa remains the region with the highest number of kidnapped foreign nationals in Constellis statistics, accounting for over 50% of all recorded incidents during March-April 2018. While experiencing a relative decrease in numbers over the second half of 2017, the region seems to have reverted to the high levels recorded over the first half of that year. Kidnapping activity in the reporting period continued to be primarily led by piracy incidents in the Gulf of Guinea. The number of victims in these incidents accounted for over 33% of the total number of foreign victims recorded in the region. While so far in 2018 the threat remains more acute off Nigerian waters, it has extended as far as Ghana to the west and Equatorial Guinea to the south. The territorial extension, the increasing number of incidents registered (both actual and attempted), and the evolving tactics observed this year, may point towards an increased capability by Nigerian pirates, undoubtedly linked directly to large ransom payments obtained in most cases. Meanwhile, in neighbouring Cameroon, the security situation in the western territories continues to deteriorate in the context of the Anglophone crisis. Separatist militants in this region have increasingly taken to kidnapping, with over 50 people kidnapped in the region since the beginning of the crisis in September 2017. Although originally intended as a tactic for political leverage, it is increasingly claimed that these groups are also using kidnapping for economic gain. Moreover, while initially only government officials and members of the security forces were kidnapped by these groups, their targeting has expanded to include foreign nationals and civilians, setting a dangerous trend to be monitored closely over the coming months.

CASES:

- On 15 March, five construction workers, including two Tunisian engineers, were kidnapped in the Southwest region of Cameroon by members of separatist armed group Ambazonia Tigers. The victims were kidnapped while working on a road construction project for a Tunisian construction company in the town of Fianco. The abductors demanded a ransom of 50 million CFA (USD 93,700), which was allegedly paid by their employer. However, the victims were not released, reportedly due to a disagreement within the militant group. As a result, on 20 March, the Cameroonian army carried out a security operation, which resulted in the rescue of four of the hostages. Unfortunately, the fifth hostage, one of the Tunisian engineers, was killed by his captors during the assault. In the weeks prior to the incident, separatists had threatened to attack foreign companies in their territory.

- On 4 April, a teenager was kidnapped near Kano while travelling to school on a motorcycle. The kidnappers told the teen’s father that he would be released once their demands were met. As a result of the incident, the Congolese and British governments, declined to have links to international syndicates. Most victims (both local and foreign) and on rare occasions other foreign nationals such as expatriate workers or tourists. Past recorded ransom demands in the area have ranged between USD 200 and 500,000 per hostage, although the amounts paid are said to be much lower. A number of hostages have been murdered by their kidnappers when families could not pay the ransom. Numerous armed groups have been responsible for kidnappings in the region, including the Democratic Forces for the Liberation of Rwanda (FDLR), the Nyatura, various Mai-Mai militia groups, and other foreign militant groups. In some instances, Congolese armed forces or other armed groups said to be acting in collaboration with Congolese army or police personnel, have been accused for these incidents.

- In DRC, rebel activity continues to dominate the country’s security concerns. These groups, mainly concentrated in central regions and the eastern border areas, are widely-known to commonly engage in violent criminal activity. Kidnapping has particularly become an important source of finance for armed groups in the east since 2015, when this practice started to increase rapidly. According to the Kivu Security Tracker, a joint project of Human Rights Watch and the Congo Research Group, a total of 355 people have been kidnapped for ransom in eastern Congo’s North and South Kivu provinces since May 2017. Over 30% of the incidents were recorded in Rutshuru, Nyiragongo, and Goma, which are areas surrounding the Virunga Park. While the vast majority of victims comprise local villagers, kidnappers have also targeted aid workers (both local and foreign) and on rare occasions other foreign nationals such as expatriate workers or tourists. Past recorded ransom demands in the area have ranged between USD 200 and 500,000 per hostage, although the amounts paid are said to be much lower. A number of hostages have been murdered by their kidnappers when families could not pay the ransom. Numerous armed groups have been responsible for kidnappings in the region, including the Democratic Forces for the Liberation of Rwanda (FDLR), the Nyatura, various Mai-Mai militia groups, and other foreign militant groups. In some instances, Congolese armed forces or other armed groups said to be acting in collaboration with Congolese army or police personnel, have been accused for these incidents.

- In Nigeria, on 14 April, unknown gunmen abducted a German engineer in Kano. The incident took place early in the morning, when five armed men on motorcycles fired at the vehicle taking construction staff to a work site. The vehicle had been escorted by a police sergeant, who was killed by the assailants. The German national remains missing at the time of writing and no information has been released regarding the perpetrators or ransom demands. This incident occurred six days after a Syrian youth was kidnapped and his father killed, also in Kano. The teenager was abducted alongside his Congolese driver after their vehicle was ambushed by unknown armed men in the park on 11 May. A park ranger was killed in the attack and many others injured. Park authorities, as well as the Congolese and British governments, declined to say how the two British nationals were released. It was previously reported that the kidnappers had demanded USD 200,000 for their release. The driver was released shortly after the abduction. The identity of the perpetrators was neither disclosed, with initial media reports mentioning the FDLR, the Ugandan Allied Democratic Forces (ADF), the Mai Mai, and Congolese soldiers as possible perpetrators. As a result of the incident, the Virunga Park management has temporary halted tourist activities in the park. Since prior to the incident, the UK Foreign Office advised against travelling to the area as a result of high levels of armed and criminal activity.

- In South Africa, high-profile kidnappings continue to be reported. On 13 April, a Polish businesswoman was freed after her family reportedly paid a €2 million ransom to her kidnappers. Barbara Wadolowska was found by police unharmed near OR Tambo International airport after being held captive for nearly a week. Wadolowska, whose kidnapping reportedly sparked a secret international police operation, was kidnapped outside her hotel in Sandton, Johannesburg. Between January and April 2018, at least seven prominent foreign businesspeople have been kidnapped in South Africa for ransoms over 20 million rand (over half a billion dollars). Most of these incidents have been carried out by sophisticated criminal groups, believed to have links to international syndicates. Most victims since 2017, when this trend started to escalate, have belonged to the South Asian community. However, this incident is an indication that these groups could potentially be expanding their targeting.
Reporting of kidnapping activity in Asia remained within established parameters for 2018 and 2017, with the region accounting for 11% of all recorded victims of foreign origin. Kidnapping activity linked to Philippine extremist militant group Abu Sayyaf Group (ASG) has remained limited since the crackdown launched by governments in its areas of operation, particularly by the governments of the Philippines and Malaysia. Having said that, incidents targeting local nationals are being increasingly recorded in recent months, signaling a possible resurgence of the group, known through time for its great resilience. Linked to these developments, Asian anti-piracy centre ReCAAP issued a warning on 1 May, cautioning on possible ASG attacks on vessels off East Malaysia and southern Philippines, aiming at the kidnapping for ransom of crew. Elsewhere in the Philippines and Malaysia, kidnapping incidents targeting foreign nationals continue to be mostly linked to regional syndicates. These groups mostly target fellow nationals in kidnap for ransom bids, or incidents linked to personal or financial disputes.

**CASES:**

- On 29 April, suspected ASG militants lead by local leader Mujir Yada abducted four people, including two policewomen, in a village near Patikul, Sulu, on their way back from a leisure trip. The two police officers were released by the group on 15 May in two separate events. The Philippine authorities did not elaborate on the conditions of their release, but it is likely a ransom was paid. The group had initially demanded a P5 million (USD 95,500) ransom for the two cops and P300,000 (USD 5,700) for each of their companions. The two companions were said to have been freed in the conditions of their release, but it is likely a ransom was paid. The group had initially demanded a P5 million (USD 95,500) ransom for the two cops and P300,000 (USD 5,700) for each of their companions. The two companions were said to have been freed in the operation on 12 April. Dorg Yun Hao had been held hostage in a room at the Okada Manila casino since 5 April after he had run up a USD 96,000 gambling debt that he could not repay. His captors reportedly sent a video to his relatives, showing the victim being beaten, and demanded them to pay Dong's debt. Profiting a distraction by his captors, the victim was able to send a phone message to his girlfriend, who contacted police.

With the Taliban’s 2018 offensive in full swing, the security threat profile of the country has further deteriorated since its announcement on 25 April. In the code-named ‘Al Khandaq’ operations, the Taliban have carried out attacks in nearly all of Afghanistan’s 34 provinces and have so far overrun at least five district centres across western, northern, and southern Afghanistan. In this context, a number of kidnappings have been attributed to the Taliban as part of their political campaign and possibly also for ransom. Given the opportunity, future high-profile Taliban kidnappings of foreign nationals in Kabul and elsewhere in the country are a strong possibility.

**CASES:**

- On 6 May, Taliban militants abducted seven Indian engineers and their Afghan driver near the city of Pul-e-Khumri, in the northern province of Baghlan. All victims were employees of an Indian engineering company working on a project for the construction of a power sub-station in Baghlan for Afghan power company Da Afghanistan Breshna Sherkat (DABS). It is currently unknown if the group has issued any demands for the release of the abducted engineers. Although authorities had said tribal elders and local influential figures were mediating with the Taliban to free the group, it was later reported the negotiations stalled for unknown reasons. At present, the motives for the kidnapping remain uncertain. While some sources have claimed the abduction took place because the Taliban mistook the workers for Afghan government employees, it is likely that the incident has taken a political tint of greater magnitude. One theory states the engineers are being held as bargaining chips with the Afghan government on account of the Taliban’s perception that electricity is being denied to the province’s districts where they have control or influence, a long standing issue in the country. On another notion of greater magnitude, it is believed that the hostages have become victims of geopolitical developments involving the governments of Afghanistan, India, Pakistan and the US.

- Meanwhile in India, two policemen were arrested on 8 April, accused of the kidnapping of a local businessman on 11 February. The detainees, alongside six other officers and a lawyer, reportedly demanded an initial ransom of USD 4.9 million for the release of the businessman, which was finally settled with the alleged transfer of 200 bitcoins (worth about USD 1.8 million) by the victim. The businessman reported the incident to the police on 23 February. The authorities are currently investigating allegations that the businessman had stolen the said bitcoins from someone else. Following the large surge in the value of bitcoin, cases of abduction and fraud linked to this virtual currency have increased in India. This was the second known kidnapping involving ransom in bitcoin in Gujarat in less than one month.
Statistics for March-April 2018 are drawn from Constellis’ record of 105 kidnapped foreign nationals. Over January-February 2018, Constellis recorded a total of 136 foreign nationals kidnapped across the world.

For the kidnapping of foreign citizens in MAR-APR 2018:

- **AFRICA** 51.4%
  - Nigeria 15.2%
  - Cameroon 13.3%
  - South Africa 5.7%
  - Gabon 5.7%
  - Cameroon 3.7%

- **AMERICAS** 25.7%
  - Mexico 14.3%
  - Venezuela 8.2%
  - Colombia 8.2%
  - Costa Rica 3.7%
  - Haiti 3.7%

- **ASIA** 10.5%
  - Pakistan 18.2%
  - Philippines 18.2%
  - Vietnam 18.2%
  - Azerbaijan 3.7%
  - Thailand 3.7%

- **EUROPE** 10.5%
  - Kosovo 54.5%
  - Spain 27.3%
  - France 9.1%
  - Russia 9.1%

- **MIDDLE EAST** 1.9%
  - Turkey 50%
  - Iran 50%

- **REST OF THE WORLD** 25.7%
  - Venezuela 2.9%
  - Gabon 2.9%
  - Libya 3.8%
  - Ghana 4.8%
  - Kosovo 5.7%
  - South Africa 5.7%

Statistics for March-April 2018 are drawn from Constellis’ record of 105 kidnapped foreign nationals. Over January-February 2018, Constellis recorded a total of 136 foreign nationals kidnapped across the world.
MAR-APR 2018

**KIDNAPPED FOREIGN CITIZENS**

**REGIONAL ORIGINS OF VICTIMS**

<table>
<thead>
<tr>
<th>Region</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>North African</td>
<td>2.9%</td>
</tr>
<tr>
<td>North American</td>
<td>2.9%</td>
</tr>
<tr>
<td>Unknown</td>
<td>4.8%</td>
</tr>
<tr>
<td>Middle Eastern</td>
<td>4.8%</td>
</tr>
<tr>
<td>African</td>
<td>5.7%</td>
</tr>
<tr>
<td>South Asian</td>
<td>9.5%</td>
</tr>
<tr>
<td>Southeast Asian</td>
<td>9.5%</td>
</tr>
<tr>
<td>European</td>
<td>23.8%</td>
</tr>
<tr>
<td>Latin American</td>
<td>23.8%</td>
</tr>
<tr>
<td>Central Asian</td>
<td>12.3%</td>
</tr>
</tbody>
</table>

**MOST VICTIMISED SINGLE NATIONALITY**

<table>
<thead>
<tr>
<th>Nationality</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turkish</td>
<td></td>
</tr>
<tr>
<td>Salvadoran</td>
<td></td>
</tr>
<tr>
<td>Swiss</td>
<td></td>
</tr>
<tr>
<td>Indian</td>
<td></td>
</tr>
<tr>
<td>Italian</td>
<td></td>
</tr>
<tr>
<td>Ukrainian</td>
<td></td>
</tr>
<tr>
<td>Filipino</td>
<td></td>
</tr>
<tr>
<td>Ecuadorian</td>
<td></td>
</tr>
<tr>
<td>American</td>
<td></td>
</tr>
<tr>
<td>Guatemalan</td>
<td></td>
</tr>
</tbody>
</table>

**MOST VICTIMISED OCCUPATIONAL SECTOR**

<table>
<thead>
<tr>
<th>Region</th>
<th>Occupational Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>Maritime</td>
</tr>
<tr>
<td>Americas</td>
<td>Businesspeople</td>
</tr>
<tr>
<td>Asia</td>
<td>Dependents</td>
</tr>
<tr>
<td>Europe</td>
<td>Education</td>
</tr>
<tr>
<td>Middle East</td>
<td>Unskilled</td>
</tr>
</tbody>
</table>

**DISCLAIMER:** These statistics herein presented are the result of a compilation of kidnapping incidents involving foreign nationals only, which have been reported in the media and other open sources. The information contained and its results are therefore partial as result of the incomplete nature of open-source material. Thus, this report should be taken only as a reference of general trends, taking its limitations into consideration.
Piracy and armed robbery registered an increase in Q1 2018 with 66 reported incidents, in comparison to 43 in Q1 2017 and 37 in Q1 2016. However, worldwide incident totals for March and April 2018 declined compared to January – February 2018. Hostile activity remained concentrated in the Gulf of Guinea, particularly in Nigeria’s territorial waters, followed by Southeast Asia. Criminal boardings continued to account for the majority of incidents reported globally. These, however, decreased 36% in March and April, with 14 recorded incidents. On the other hand, hijackings increased, with four reported attacks in comparison to two in the previous reporting period. Terrorism-related attacks remained relatively rare, with the threat, most pronounced in the Gulf of Aden. Additionally, although outside of the reporting period, on 1 May, Asian anti-piracy centre ReCAAP issued an unusually specific warning, cautioning on possible kidnapping attacks on vessels off Eastern Malaysia by Philippine terror group Abu Sayyaf Group (ASG). Between March 2016 and April 2017, ASG kidnapped at least 59 seafarers from 13 vessels in the region.

The Gulf of Guiana accounted for 43% of all incidents recorded in Q1 2018, with all four hijackings recorded in the period taking place there. It is important to note this was an outstanding escalation since no such incidents were reported in 2017. Nigerian waters particularly remained a piracy hotspot, recording 75% of all incidents registered in the region. The risk of kidnapping of crew is expected to remain high to all types of vessels in this region, particularly off Brass and Bonny. Of note, an increasing number of incidents are being reported outside of Nigeria’s exclusive economic zone (EEZ). In Q1 2018, over 50% of recorded hijackings in the region occurred outside the EEZ, suggesting that Nigerian pirates have expanded their area of operations. In particular, maritime security conditions continue to deteriorate in Benin, where incidents recorded thus far this year represent the first significant piracy activity in the area since February 2015. Despite support from international partners, the Benin Navy is highly unlikely to be able to completely deter perpetrators in the short term.

The downward trend in Southeast Asia continued throughout March and April. There were 12 recorded piracy and robbery incidents in the region during the period, representing a 20% decrease from January and February. However, piracy and robberies in the first four months of 2018 increased by 23% from the same period in 2017. Despite the relatively low number of incidents, the threat of piracy in the region remains credible, with low-level attacks such as robberies, remaining as the primary security concern. Vessels are advised to continue to implement strict anti-piracy measures particularly in the Straits of Malacca, off eastern Sabah and in the southern Philippines. Pirates and robbers also continue to pose a threat to commercial interests in Indonesia and the Singapore Strait, with night attacks on passing or anchored vessels relatively common. While attacks off Bangladesh have fallen significantly in recent years, armed robberies continue to be reported especially at Chattogram anchorages and approaches. Early detection continues to deter much of piracy throughout the region.

**CASES:**

- On 3 April, Houthi rebels launched a missile attack on the Saudi Arabian-flagged MT Abqaiq, a very large (300,000 DWT) crude carrier carrying over 2 million barrels of crude oil. A coalition warship reportedly repelled the attack. The ship sustained minor material damage and continued its journey to Ain Sukhna, Egypt. The rebels said they had actually targeted a coalition warship in response to an airstrike on Hodeidah on 2 April that killed at least a dozen civilians. The missile type used in the attack has not been disclosed. While a risk of terrorist attacks employing mines, waterborne IEDs, RPGs and missiles, on commercial interests remains, merchant ships are unlikely to be directly targeted. Application of extant security measures are assessed as sufficient in the area.

- On 24 April, five men armed with guns and machetes boarded the Malaysian fishing boat JHF 2529 15 nm southwest of Tanjung Laboh, Malaysia. The attackers hijacked the vessel and sailed towards Indonesia. A RM 30,000 (USD 7,600) ransom was demanded for the release of the three crew members. The Malaysian Maritime Enforcement Agency (MMEA), with the help of Indonesian authorities, released the boat and its crew on 25 April. According to the MMEA, this is one of seven similar cases reported close to the Malaysia-Indonesia maritime border since the beginning of 2017.
Mobile phones and internet-connected devices have grown in complexity over the past decade, evolving into sophisticated computer devices. Today these devices enable users to perform a wide range of tasks, including storing personal information, shopping, banking and making payments, in addition to providing a platform for interaction through social media. With the avenues of possibilities for mobile devices continuously expanding, avenues for exploitation by cyber-criminals have risen hand-in-hand. McAfee, in its Q1 2018 ‘Mobile Threat Report’, noted an exponential growth in mobile malware since 2015, with attacks reaching over 20 million toward the end of 2017 and into early 2018. With the boom of mobile malware observed last year, and the ever-increasing number of mobile subscribers globally (currently in the region of 5 billion), mobile malware could create billion-dollar revenues for its authors by 2020, should the rate of attacks continue at their current trajectory. Furthermore, with research firm Gartner also reporting a massive increase in ‘Internet of Things’ (IoT) devices, numbering almost 8.5 billion worldwide last year; opportunities for exploitation will also continue to grow rapidly. 

As with threats to regular computers, mobile devices have been targeted in a variety of cyber-attacks, most of which are financially motivated. Threats which have all seen increases from last year include:

- Spyware, which monitors and records information about a user’s actions without their knowledge;
- Botnets, which can take control of a device and have complete access to its contents;
- Banking Trojans, which emulate authentic mobile banking apps to steal users’ money;
- Ad-clicker Trojans, which seem to provide a service of some kind but fraudulently manipulate mobile ads to generate revenue.

All of these threats can be inserted onto a device via several means, such as malicious emails or SMS and fake updates. They can also be embedded into legitimate or fraudulent apps, into websites or into other downloads.

With the high popularity of cryptocurrencies, cryptocurrency-mining malware has also seen considerable growth in the mobile market, with the number of detections spiking significantly since October last year. Such malware, once transmitted onto a device, uses it to mine cryptocurrency without a user’s permission or knowledge. Given that cryptocurrency mining is a computationally intensive operation, cyber criminals seek to spread the load to as many devices as possible to combine their processing power. Some of these programs have actually been known to hijack a smartphone’s processor so aggressively that they cause the device to overheat, damaging its battery. Devices can become infected by crypto-mining malware in the same way as other threats, i.e. via spam emails or as potentially unwanted apps via an app store.

Indeed, attacks via mobile application stores, such as the Apple App Store or Google Play, have seen the most growth over the past few years, infecting millions of devices. Attackers have seen these market places as an attractive platform to exploit due to the relative vulnerability of app vetting systems employed by such stores. Google Play last year removed over 4,000 apps from its store, which were deemed malicious. However, it did not notify users, many of whom may have harboured fraudulent applications long after they were removed from the store. Frequently, these malicious apps, posing as legitimate ones, gain access to the device’s phone number to subscribe to a number of paid services, charging unknowing users every week or month.

Ransomware has also often been bundled-in with otherwise seemingly legitimate apps. As with ransomware attacks against PCs, this phenomenon saw a sharp increase in the mobile sector over 2017, remaining a significant threat to date. Unlike its PC-based counterparts, mobile malware is typically limited to restricting users’ access to their device’s functions, as opposed to encrypting data on it. However, some more sophisticated attacks have incorporated the ability to encrypt information on SD cards. Similar to PC ransomware, mobile attacks can display ransom notes directing victims where to send payment to release their device’s functionality. In early 2017, an attack dubbed ‘Charger’ targeted Android devices from the Google Play Store. It demanded a 0.2 Bitcoin ransom, threatening to release users’ personal information to the black market if this was not paid.

With McAfee reportedly detecting over 16 million mobile malware attacks in Q3 2017 alone (almost double the number of cases for all of 2016), mobile providers have improved the security of devices and enhanced their vetting procedures for applications on their online marketplaces. There has also been an increase in the use of encrypted communication apps, both amongst businesses and members of the public. These allow data to be passed only between intended individuals, mitigating the threat of communications being intercepted maliciously. Nevertheless, such recent security advancements, user awareness is still critical in mitigating exposure to mobile cyber-crime. To avoid infection, users are advised to secure their devices with mobile security solutions, keep devices’ software up-to-date, and only download applications from trusted sources.

**CASES:**
- **Grabos**: An Android malware hiding behind free music player apps, discovered in late 2017/ early 2018. It was later found to exist in 144 trojanized apps on the Google Play Store and downloaded by an estimated 17.5 million users. The malware generated money by stealing users’ information and creating custom notifications, which would deceive users into installing additional applications. This is known as a ‘pay-per-download’ scam, generating income for the author for every install.
- **LokiBot**: A banking Trojan that, in addition to harvesting the user’s credentials by simulating a mobile banking app, simulated other popular apps such as Skype and WhatsApp. ‘LokiBot’ had the ability to display fake notifications from these apps, as well as using the infected device to send malicious SMS to contacts in the phonebook to spread itself. Upon detection, ‘LokiBot’ transformed itself into a ransomware, locking the phone’s screen and demanding a ransom in a message accusing the user of viewing child pornography. This Trojan is thought to have targeted over 100 financial institutions globally.
A number of recent intelligence briefings seem to indicate the terrorist threat will diversify in methodology and will be particularly dynamic in nature. In the backdrop of this information, and taking into account a possible migration of tactics from the Middle-East, Indonesia and Africa, this briefing explores a series of considerations in the occurrence of a Chemical, Biological, Radiological Nuclear and Explosive (CBRN(e)) attack in the Western world.

In October 2017, European intelligence agencies warned of chemical attacks on public transport hubs or places of mass public congregation. They also identified that there is concrete intelligence to indicate a heightened risk of an improvised explosive device (IED) with chemical or toxic gases. For example, in issue 15 of its Dabiq magazine released in July 2016, the Islamic State (IS) called on its Jihadists to keep their operations simple and effective and to use a weapon to cause the ‘most damage and panic’. Terrorists certainly have the intent and capability and, as has often been demonstrated, they are interested in carry out attacks that are highly dramatic in nature and that generate significant worldwide press coverage. In this context, a CBRN(e) attack in the West is not out of the realm of possibility. The full range of CBRN(e) weapons are potentially available to terrorists but the capability to obtain and deploy depends on the skill level and resources of the group. However, chemical release and dirty bombs are probably easiest to expedite with the right training and equipment.

After careful assessment of these new threats, a number of governments have identified the necessity to improve contingency plans. For example, the UK’s National Police Chiefs’ Council and the National Fire Chiefs’ Council recognised after the Glasgow Airport attack and the failed Tiger Tiger bombs in 2007 that the country was slightly behind the curve. Thankfully, after intensive work and significant uniformed services collaboration, the UK has become much better tactically, technically and logistically at determining the developing threats. The Borough Market response is testament to that.

There are however, two areas for immediate concern that need to be identified when undertaking security risk audits in the private sector. The first is the actual difficulty there would be in dealing with a CBRN(e) incident in crowded public places such as mass transit hubs, large sporting events or visitor attractions. The second issue is the heightened sensitivity of crowds and reaction to actual or perceived incidents. The Oxford Circus false alarm and subsequent crowd rushes in late 2017 was a good example of mass hysteria, where certain celebrities with a massive social media following contributed to the general panic in real-time. A person’s legitimate and understandable fear can be magnified out of proportion when it is projected instantaneously over social media.

The reason for highlighting these issues now is that a CBRN(e) incident (actual or perceived) could have a larger effect, beyond the crowds located directly in the hot zone. Mass hysteria and the considerable confusion that results would certainly further stretch emergency services and complicate the response. This would allow a determined and well planned attack to ‘multiply’ its effectiveness. This conundrum is currently perplexing many security and business continuity directors as they consider what takes priority within their organisations: people (staff, visitors, contractors, customers), physical assets (buildings, equipment); information (paper, electronic, critical records); or processes (critical procedures, invacuations/evacuations/lockdowns).

Risk management audits should examine existing risk assessments, business continuity management plans, crisis management plans, workplace violence policies, access control policies, training programmes and so on, with the aim of identifying and addressing any weaknesses. All these are facets of effective risk management, and when priority decisions are made in relation to people, physical assets, information and processes, they should inform a comprehensive organisational risk management plan. That plan should enable key incident decision-makers within the organisation to handle everything from social media storms, protests and rioting, right up to a coordinated well-planned terrorist attack using CBRN(e).

Fortunately, there is a plethora of information to assist with this planning, including the excellent counter-terror protective security advice for crowded places provided by counter terrorism agencies such as the UK’s National Counter Terrorism Security Office (NaCTSO). This resource material exists because it has been recognised that we are currently in an era of ‘high-impact high-probability events’, which will call for elevated consequence decision making by people not used to making such decisions. The key question that organisations need to ask themselves is whether or not they are sufficiently resilient to cope with a high-impact high probability event such as a CBRN(e) attack, and if not, take appropriate action to ensure that they are well prepared and capable in the future.

In summary, the threat is dynamic and continually diversifying. This means that organisations must maintain constant vigilance and keep one step ahead of the threat through scenario planning and establishing appropriate counter-measures and responses.
ABOUT CONSTELLIS

Constellis is a leading provider of risk management, humanitarian, social intelligence, training and operational support services to government and commercial clients throughout the world. Operating in over 45 countries, Constellis’ 20,000 employees bring unparalleled dedication and passion for creating a safer world by upholding the highest standards of compliance, quality, and integrity.

Constellis’ forward thinking services span a broad range of synergistic solutions, from the boardroom to the project site, encompassing risk governance, organisational resilience, business continuity management, crisis management, travel security, global tracking, training, protective security, life support, logistics and specialist support such as K9 services and UAV systems.

At Constellis, our number one mission is to secure success for our customers. Constellis combines the legacy capabilities and experience of ACADEMI, Triple Canopy, Centerra, Olive Group, OmniPlex, AMK9, Edinburgh International, Strategic Social and all of their affiliates. The consolidation of companies under the Constellis name allows our clients to rely on one single partner and project experience that spans the globe.

For more information about Constellis, please visit our website at: www.constellis.com