THREATS TO ENERGY INFRASTRUCTURE
breaching users’ devices with cryptomalware, hackers are able to hijack the device’s processing power to mine cryptocurrency without the victim’s knowledge or approval. Due to cryptomining being a computationally intensive process, cryptomalware can severely degrade the performance of an infected device, as well as requiring a large amount of electricity. This can have a severe financial impact on breached organisations, with losses in productivity due to poor computer performance, as well as extremely high energy bills.

The Focus Article offers an insight onto the threats to energy infrastructure. Among all sectors that constitute a nation’s critical infrastructure, the energy sector is uniquely important because it possesses an enabling function across all other sectors. This not only means that its incapacitation or destruction would have a serious effect on a nation’s economy and security, but also makes it a high-profile target for threat groups. In the context of a complex operating environment with ever-evolving threats, both physical and virtual, it is necessary to utilise comprehensive approaches to security. Moreover, as an increasing number of critical infrastructure assets are privately owned, these approaches need to reflect the shared responsibility between the state and individual owners and operators.
GLOBAL OVERVIEW

AMERICAS

During July-August 2018, the Americas accounted for 55% of the total pool of foreign kidnapping victims recorded by Constellis globally, a noticeable increase from levels observed in previous months. This was the result of a series of mass kidnappings of migrants recorded in Mexico, which made the international headlines for their magnitude. These however only reflect the tip of a much-larger issue. According to figures by the National Commission of Human Rights (CNDH), as many as 71,415 migrants were kidnapped in the country between 2007 and 2014. Meanwhile, the Mexican National Institute of Migration (INM) affirms they assisted 1,227 migrants who were victims of kidnapping in Mexico between 2012 and 2017. Most of these abductions (79%) were reported in Tamaulipas state, followed by Tabasco and Chiapas. Having said that, it is well known that the majority of these incidents go unreported. This is especially the case for illegal migrants, who fear approaching the authorities, given their irregular status in the country. It is for this reason, and because of their large numbers, that organised criminal groups in Mexico target them. According to recent studies, as a result of the exponential growth of this business, the cartels have subcontracted this activity to minor groups, who pay them a percentage of the profits as right-to-operate fees.

CASES:

- On 27 August, Mexican authorities rescued 22 Central American migrants who had been held for ransom at a small property in the southern state of Chiapas. The rescue took place after another kidnapped migrant escaped and reported the incident to the police on 21 August. The escapee stated that the group, comprising people from Ecuador, Guatemala, El Salvador, and Honduras, were kidnapped by human smugglers who had promised to transport them to the US border in exchange of a payment of 15,000 pesos (USD 800).

- On 26 days. The kidnappers had reportedly demanded a ransom of 160,000 pesos (USD 8,500) for each of the migrants, and sent torture videos to their relatives in order to extort the money.

- Colombia, in the context of increasing illegal immigration from Venezuela, is beginning to develop similar criminal patterns. On 1 August, in a security operation in Tolima department, Colombian authorities rescued 11 Venezuelans and arrested the man who had kidnapped them. The suspect, posing as a sergeant of the Colombian Army, had approached the victims at a locality in Santander department, not far from the border with Venezuela, promising work in Tolima. The man then took them to a farm and demanded a payment of COP 1.2 million (USD 405). Those who could not pay were forced to work. Preliminary reports indicate the rescued victims had all been lured in July.

- On 1 August, Italian businessman Elio José Simonelli Datellis, owner of several warehouses and a car body shop, in the city of Maracay, was kidnapped as he arrived at one of his businesses. Three kidnappers died in the clash. The victim was murdered as he tried to escape during a clash between the kidnappers and police.

While crime in Panama is moderate by regional standards, the threat remains significant. Similarly, whilst kidnapping in the country remains limited, it has shown a clear increasing trend since 2013. Although the majority of incidents comprise express kidnappings, in recent months a number of foreign nationals have been targeted in conventional kidnappings. While in the past these crimes were attributed to foreign gangs, local groups have now shown dominance, although still holding important links to transnational criminal organisations.

CASES:

- On 11 July, Panamanian police rescued a kidnapped Colombian trader in Arraijan district, western Panama. Two Panamanian suspects were arrested during the operation. The Colombian national had been kidnapped from a shopping mall in the same district on 9 July. According to reports, the kidnappers had demanded a ransom of USD 1 million from the victim’s father. The sum was later decreased to USD 500,000 and finally to USD 300,000. Two other suspects were arrested in follow-up operations in the region.
During the period of July-August 2018, Europe reverted to previous reporting levels experienced over 2017 and toward the beginning of this year. Although reporting of kidnappings in the region has somewhat increased in recent years, the incidence remains limited in comparison to other regions of the world. This is particularly the case for Western Europe, where effective law enforcement and judicial systems deter the proliferation of this phenomenon. There, the great majority of cases reported in the media conclude in the rescue of victims and arrest of perpetrators. While trends differ country by country, kidnapping in Europe generally takes place along two main trends: the kidnapping of wealthy individuals (or those perceived to be wealthy) and their dependents; and the kidnapping of individuals linked to the criminal world.

**CASES:**

- On 26 July, the 85-year-old grandfather of the wife of Serbian tennis player Novak Djokovic was found tied to a lamppost at a cornfield in central Serbia after he was taken hostage the previous night. Miloslav Radisavljevic was abducted by two armed men who broke into his house in the city of Ljig and robbed him of approximately EUR 220 (USD 255) and a cell phone. According to a Serbian news outlet, the kidnappers contacted one of the victim’s sons, demanding a ransom of EUR 2 million (USD 2.3 million). It is unclear if a payment took place for his release, with Ljig authorities labeling the incident as an “attempted abduction”. Two suspects were arrested in the days following the incident.

- On 14 August, a man was abducted by a group of suspected drug traffickers in Seville, Spain. The victim was said to have been conducting a drugs deal with the suspects, who set up a fake police raid to take him hostage. The victim was robbed of EUR 180,000 (USD 209,000) on the spot and a ransom of EUR 200,000 (USD 232,000) was later demanded from his wife. In spite of the issued threats, the wife reported the incident to the police, who rescued the victim the next day and arrested ten suspects.

- In Cyprus, two ten-year-old Greek nationals were abducted from their school in Larnaca on 25 September. The perpetrator approached the boys pretending to be a teacher who needed help bringing some books from his car. A large-scale search operation by air and land was initiated by the Cypriot authorities after the incident was reported. The victims were found on the same day at a location not far from the school and the perpetrator was apprehended. Subsequent investigations determined the kidnapping had a financial motivation.

Other methods such as virtual kidnapping and express kidnapping are also beginning to be reported in Europe, mostly conducted by foreign criminal groups. Notably in recent months, the targeting of Chinese nationals in virtual-kidnapping-style scams and loan-shark kidnappings has been observed. These trends, which are prevalent in Asia, have been expanding throughout the world targeting the Chinese diaspora.

**CASES:**

- On 21 September, six Chinese nationals were tried at a Portuguese court, accused of illegally lending money to compatriots for gambling at casinos at very high interest rates and then violently extorting the payment of the loans. The gang members were arrested after one of their victims reported having been held against his will by the accused. Lei Zoang said he was forced into a car and taken to a house, where he was kept tied up for several days until he paid his debt. The man reported he was physically and psychologically tortured. It is not clear when the event took place and what was the amount of the debt.

- On 11 July, the Shanghai police stated they were investigating a virtual kidnapping that targeted a Chinese student in Germany. The student was called by a stranger who claimed to be a Chinese police officer and demanded information on her family because they were allegedly suspected in a criminal case. Using the information provided by the student, the criminal called her mother in China, and claiming to have kidnapped her daughter in Germany, demanded 2 million yuan (almost USD 300,000) as ransom. It is unclear if any payments were made.
MIDDLE EAST

Over the reporting period, the Middle East maintained similar reporting levels to those recorded over May-June 2018. In this period however, a spike in kidnappings was observed in Iraq, where a socio-political crisis is being met with serious security challenges. These challenges include the perceived reorganisation of Islamic State (IS) remnants over previously declared “liberated” areas. While the group continues to be a threat at national level with much of Iraq continuing to be affected by insurgent activity, rural areas in Ninawa and northcentral Iraq are currently the primary base of IS’s operations, enjoying a large degree of freedom of movement in the desert regions of Anbar and along the Syrian border. Regrouping of IS cells is also being observed in Syria, particularly in the country’s northeast. According to most recent estimates published by the US state department, more than 30,000 IS fighters remain across Iraq and Syria combined, posing a serious threat to the region.

CASES:

- The body of Iraqi journalist Wisam Hassan al-Obeidian, who had been kidnapped by IS insurgents overnight on 17 September, was found in a village in northern Tikrit the next day. Al-Obeidian was kidnapped alongside his uncle by militants disguised in Iraqi army uniform at a fake checkpoint along the Hawija-Kirkuk highway, near the Riyadh district of Kirkuk. Al-Obeidian’s uncle was reportedly able to escape his captors shortly after the incident. The victim died having been shot in the head while being blindfolded.

- On 8 July, a video emerged featuring Japanese journalist Jumpei Yasuda, who was kidnapped in Syria by Jabhat al-Nusra militants in June 2015, soon after he crossed the Turkish-Syrian border. According to the journalist’s words, the video was filmed on 17 October 2017. Although the journalist expresses in the video he is fine, the person who handed the video to Japanese media, allegedly on behalf of Hay’at Tahrir al-Sham (former Nusra Front) reportedly said that Yasuda’s health had recently been deteriorating. A second video was released on 1 August. This latest video however, bears little in common with the previous recording, posing a serious threat to the region.

- According to local media, the UN has avoided a public announcement on the kidnapping of two employees by Houthi militants in Yemen. The first incident reportedly took place on 12 July, when Houthi militias kidnapped World Food Program (WFP) employee Nasser Hanaf, in Hodeidah. This was followed by the kidnapping of Adel al-Salhi, who works for the International Organization for Migration (IOM), on 5 September in Sanaa. Relatives of the victims have confirmed the incidents and affirmed they have not been able to communicate with them since their abduction. According to some local reports, both victims are foreign nationals, although their nationality has not been specified. This information has not yet been verified.

In Yemen, the Houthi rebels are known to frequently take hostages and commit serious abuses against people in their custody. While most detentions have a political motivation or are aimed at exchanging hostages for Houthi fighters held by opposing forces, there have been documented cases where civilians have been held unlawfully to extort money from relatives. According to Human Rights Watch, in many such cases the Houthi captors threaten victims and their relatives with rape and other methods of physical and psychological torture in order to extort the demanded ransoms, which may reach millions of Yemeni riyals (thousands of US dollars) for common citizens. In this context, aid workers, activists and journalists have found themselves common targets for the rebels.

In Turkey, the kidnapping threat remains largely criminal. On 26 August, three members of a kidnapping and extortion gang were arrested in Istanbul, suspected in the kidnapping for ransom of a Libyan national. Yaseen Algeharari was kidnapped in Istanbul on 24 August after he went to meet his Tunisian girlfriend, who he met on social media. At the woman’s apartment, he was met by three Syrian males who took him away and held him hostage at a basement in the area. The kidnappers then demanded a ransom of USD 100,000 from the victim’s cousin who had travelled with him to Istanbul. The cousin reported the incident to the Turkish police, who advised to proceed with the negotiations. The kidnappers had agreed to be paid in two instalments, the first of USD 20,000. Within five hours, the police located the victim and arrested the kidnappers.
In Africa, the figures of foreign nationals kidnapped in the region over July-August were largely driven by events at sea in the Gulf of Guinea. While piracy activity has seen a relative lull since May due to weather conditions, two hijackings, one in August (19 victims) and one later in September (12 victims), suggest that piracy attacks involving the kidnapping of crew may begin resurfacing in the coming months. On land and offshore, Nigeria remains the top kidnapping hotspot in the region. While the criminal kidnapping threat in Nigeria was previously concentrated in the Niger Delta region, in recent years it has expanded into central states, linked to the ethnic violence prevalent in the region. The proliferation of arms resulting from the conflict has also brought about a notable increase in violent crime. While kidnapping and other violent crime in this area is commonly attributed to Fulani nomads, recent reports suggest that the kidnapping problem in central Nigeria has bypassed ethnic lines, also targeting members of the herding communities. The states of Kaduna and Zamfara, as well as territories adjacent to the capital, Abuja, have been particularly affected by this expanding threat. At least 17 foreign nationals have been taken hostage in highly violent kidnapping events in central territories adjacent to the capital, Abuja, have been particularly affected by this expanding threat. At least 17 foreign nationals have been taken hostage in highly violent kidnapping events in central Nigeria since 2017. Moreover, Nigeria’s middle belt, particularly in the eastern states, is threatened by incursions of jihadist group Boko Haram.

CASES:

In Libya, the high kidnapping threat to foreign nationals was recently evidenced with the abduction of a Romanian oil worker in south-western Libya. The Romanian engineer was abducted on 14 July alongside three Libyan colleagues. The incident took place at Station 186 of the al-Sharara oilfield, which has been the target of previous threats and attacks, the most recent in November 2017. Two of the Libyan engineers were reportedly released soon after. Subsequent to the incident, oilfields in neighbouring areas were shut as a precautionary measure, with all foreign workers evacuated. On 17 July, Libya’s National Oil Corporation (NOC) called for the release of Sharara exports due to the drop in production caused by the incident. In late August, a video was posted on social media showing the two hostages for the first time. In the video, the Romanian engineer appeals to the relevant government authorities and corporations to begin negotiations with the kidnappers. Two masked hostage-takers are also shown, stating they are not terrorists and do not intend to demand money for the release of the hostage. They say their goal is only to get Libyan authorities to find a solution to the crisis in the country. The men however warn that if their appeal is not heard, they will sell the hostages to terrorists. The identity of the perpetrators is currently unknown. Both victims remain missing.

In South Africa, the kidnapping of wealthy businessmen has become a highly profitable activity for criminal syndicates that are becoming more brazen in their actions. South African intelligence agencies have recently declared they suspect that units of the same syndicate are involved in the recent spate of high-profile kidnappings in the country. Their assessment is based on the fact that all recent incidents have had the same modus operandi and similar pattern of victim targeting. This syndicate, highly professional and organised, is believed to have a strong connection to the Mozambican criminal underworld and to partner with foreign regional criminals. Mirroring activity trends in Mozambique and Madagascar, it typically targets businessmen of south Asian origin who are considered wealthier, and for whom hefty ransoms are typically demanded. At least 10 such victims have been kidnapped in the country so far in 2018, and according to local media, over 40 businessmen have been kidnapped in South Africa in the last three years. As a result of the profitability of this syndicate’s business model, a number of copycat groups have begun to emerge in South Africa, according to national authorities. These groups, not having the necessary infrastructure, are not able to hold victims for long periods of time and thus demand lower ransom amounts.

CASES:

- In the most recent case, businesswoman of Indian origin Liyaqat Parker, was kidnapped by five unknown and armed men from his business in Cape Town, South Africa, on 9 July. Sources close to the investigation affirmed that a ransom of 50 bitcoin (approximately USD 330,000) had been demanded by the kidnappers for his release. Parker was released in the northern suburbs of Cape Town on 17 September, after 70 days in captivity. It is reported that rather than police facilitating the release, it was private investigators who coordinated the payment of the undisclosed ransom. The family however denied any payment took place.

- In Madagascar, Abdul Aziz Mansour, a French businessman of Indian origin, was kidnapped on the evening of 19 July from the Tsaralalana area of Antananarivo. His vehicle was found abandoned in Ilotso after the incident. Mansour was released after nine days in captivity, allegedly with the payment of a large undisclosed ransom. It is reported that the family refused the involvement of the police in the case. According to the Collective of French nationals of Indian Origin of Madagascar, this was the ninth abduction of a French person of Indian origin recorded in the country since the beginning of 2018.
Over July and August, Asia observed an increase of almost 50% in the number of foreign kidnap victims. This increase was driven by a series of kidnappings recorded in Cambodia. Although most visits to Cambodia are trouble-free, the country has considerable rates of both petty and violent crime. Criminals in the country perceive foreigners as wealthy and will target them for crimes motivated by financial gain. While kidnapping in the country is limited, Cambodian authorities have pointed to a recent increase in its incidence. According to Cambodian police, at least 50 people have been kidnapped for ransom in Phnom Penh in the last six months. Ransom amounts demanded by kidnappers are also reported to have risen dramatically, reaching the hundreds of thousands of dollars. It is however assessed that this problem originates from abroad, with kidnapping gangs being mainly comprised of foreigners, particularly Chinese nationals.

**CASES:**

- **On 22 August,** a Phnom Penh court charged five Chinese men for kidnapping a Chinese businessman for ransom. The incident took place on 16 August, when the victim went to a casino in Chamkar Mon and borrowed USD 15,000 from the accused after he lost all his money. When the victim could not repay the debt, the men kidnapped him and took him to a rental house in Tuol Kork district, where the victim was severely beaten before his family was contacted the next day. The men threatened to kill the victim if the debt was not paid. Under police guidance, the family paid the money on 18 August. Cambodian police arrested the loan sharks after the victim was safely released.

- **On 28 July,** Malaysian police rescued a kidnapped Indian man in Johor city, and arrested three Pakistani nationals guarding the victim. The police raid took place after reports were made by the victim’s relatives both in India and in Malaysia. The kidnappers reportedly demanded a ransom of RM200,000 (over USD 49,000) and threatened to kill the victim if this was not paid. It is not clear when the abduction took place and under what circumstances.

- **On 11 September,** two Indonesian fishermen were kidnapped by armed men believed to be ASG militants in the waters off Semporna, in Sabah, Malaysia. The two victims and two other men were on their docked fishing trawler when the attack took place, during curfew hours at approximately 0100hrs local time. According to reports, the vessel was boarded by at least two masked men carrying M16 rifles and who spoke Suluk, a dialect used in the Philippines’ Sulu province. The other two crew members, who escaped the abduction by hiding in the engine room, reported the incident to the police. Reportedly, on 18 September, the perpetrators contacted the victims’ relatives, demanding a ransom of RM 4 million (USD 967,000). No deadline was reportedly given for the ransom payment to be made. Given that the vessel flew the Malaysian flag, and judging by the language spoken, it is likely that the kidnappers were Indonesian or at least their counterparts. Based on anecdotal information, Malaysians in the region have thought the fishermen were Malaysian. Based on information received by leaders, the fishermen were from Tawau district and were working on a trawler that is believed to be owned by a Chinese company. While the victims were not taken by the kidnappers, it is believed that the kidnappers were seeking to extort money from the owner of the trawler.

In September, the first kidnapping in the Sulu Sea was registered after almost two years. The incident, attributed to the Abu Sayyaf Group (ASG), has highlighted the extant threat posed by the group. It also questions its possible regrouping following the heavy crackdown pursued by the Duterte administration in the Philippines and increased security measures imposed by the governments of Indonesia, Malaysia and the Philippines in the shared maritime area. According to local reports, it is believed that a number of ASG commanders who had gone underground during this period have re-emerged and are reconstructing their regional networks in order to carry out further cross-border kidnappings.

**CASES:**

- **On 11 September,** two Indonesian fishermen were kidnapped by armed men believed to be ASG militants in the waters off Semporna, in Sabah, Malaysia. The two victims and two other men were on their docked fishing trawler when the attack took place, during curfew hours at approximately 0100hrs local time. According to reports, the vessel was boarded by at least two masked men carrying M16 rifles and who spoke Suluk, a dialect used in the Philippines’ Sulu province. The other two crew members, who escaped the abduction by hiding in the engine room, reported the incident to the police. Reportedly, on 18 September, the perpetrators contacted the victims’ relatives, demanding a ransom of RM 4 million (USD 967,000). No deadline was reportedly given for the ransom payment to be made. Given that the vessel flew the Malaysian flag, and judging by the language spoken, it is likely that the kidnappers were Indonesian or at least their counterparts. Based on anecdotal information, Malaysians in the region have thought the fishermen were Malaysian. Based on information received by leaders, the fishermen were from Tawau district and were working on a trawler that is believed to be owned by a Chinese company. While the victims were not taken by the kidnappers, it is believed that the kidnappers were seeking to extort money from the owner of the trawler.

- **In Afghanistan,** three expatriates were found dead in Kabul on 2 August shortly after they were kidnapped by unknown gunmen. The group, comprising an Indian, a Malaysian and a FYROM national was abducted in the early morning of the same day near Puli-e-Charkhi in the PD9 area of the city. Their bodies were later found riddled with bullets inside a car parked at the Mussahi district of Kabul province. According to international media, the three men, employees of a French food service provider, had been travelling to work at Kabul airport with a local driver who was not taken by the kidnappers. No group claimed responsibility for the incident. Given past patterns of violent activity targeting foreign nationals in the city, it is highly likely the incident was a kidnapping gone wrong, rather than an attack aimed at the murder of the expatriates.
Statistics for July-August 2018 are drawn from Constellis’ record of 160 kidnapped foreign nationals. Over May-June 2018, Constellis recorded a total of 127 foreign nationals kidnapped across the world.

**Region**

<table>
<thead>
<tr>
<th>Region</th>
<th>Number of Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>88</td>
</tr>
<tr>
<td>Africa</td>
<td>37</td>
</tr>
<tr>
<td>Asia</td>
<td>25</td>
</tr>
<tr>
<td>Middle East</td>
<td>6</td>
</tr>
<tr>
<td>Europe</td>
<td>4</td>
</tr>
</tbody>
</table>

**Statistics for Jul-Aug 2018**

- **Americas** 55%
  - Mexico (63) 71.6%
  - Colombia (12) 13.7%
  - Panama (5) 5.7%
  - Peru (2) 2.3%
  - Venezuela (2) 2.3%
  - Costa Rica (1) 1.1%
  - US (1) 1.1%
  - Canada (1) 1.1%
  - Trinidad & Tobago (1) 1.1%
  - Gabon (19) 51.4%
  - Libya (5) 13.5%
  - Nigeria (4) 10.8%
  - Madagascar (3) 8.1%
  - Angola (2) 5.4%
  - CAR (2) 5.4%
  - Mozambique (1) 2.7%
  - South Africa (1) 2.7%
  - Cambodia (10) 40%
  - Philippines (5) 20%
  - Afghanistan (4) 16%
  - Malaysia (4) 16%
  - Azerbaijan (1) 4%
  - Mongolia (1) 4%
  - Ukraine (2) 50%
  - Lebanon (1) 16.7%
  - Turkey (1) 16.7%
  - UAE (1) 16.7%

- **Africa** 23.1%
  - Gabon (19) 51.4%
  - Libya (5) 13.5%
  - Madagascar (3) 8.1%
  - Angola (2) 5.4%
  - CAR (2) 5.4%
  - Mozambique (1) 2.7%
  - South Africa (1) 2.7%
  - Cameroon (5) 25%
  - Algeria (5) 25%
  - Mozambique (1) 2.7%
  - South Africa (1) 2.7%
  - Gabon (19) 51.4%

- **Asia** 15.6%
  - Cambodia (10) 40%
  - Philippines (5) 20%
  - Afghanistan (4) 16%
  - Malaysia (4) 16%
  - Azerbaijan (1) 4%
  - Mongolia (1) 4%
  - Ukraine (2) 50%
  - Lebanon (1) 16.7%
  - Turkey (1) 16.7%
  - UAE (1) 16.7%
  - Thailand (4) 16%

- **Middle East** 3.8%
  - Iraq (3) 50%
  - Lebanon (1) 16.7%
  - Turkey (1) 16.7%
  - UAE (1) 16.7%

- **Europe** 2.5%
  - Ukraine (2) 50%
  - UK (1) 25%
  - Portugal (1) 25%

- **Rest of the World** 18.1%
  - Malaysia (4) 2.5%
  - Afghanistan (4) 2.5%
  - Philippines (5) 3.1%
  - Panama (5) 3.1%
  - Libya (5) 3.1%
  - Cambodia (10) 6.3%

* (Number of Victims)
JUL-AUG 2018

KIDNAPPED FOREIGN CITIZENS

REGIONAL ORIGINS OF VICTIMS

- Latin American (83) - 51.9%
- African (1) - 0.6%
- Unknown (4) - 2.5%
- Middle Eastern (8) - 3.8%
- European (9) - 5.6%
- South Asian (11) - 6.9%
- Central Asian (17) - 10.6%
- Southeast Asian (27) - 16.9%

MOST VICTIMISED SINGLE NATIONALITY

- Cuban (1) - 11.8%
- Indian (1) - 11.8%
- Georgian (1) - 11.8%
- Colombian (1) - 11.8%
- Salvadoran (1) - 11.8%
- Guatemalan (1) - 11.8%
- Filipino (1) - 11.8%

MOST VICTIMISED ORIGIN BY REGION

<table>
<thead>
<tr>
<th>Region</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>Central Asians</td>
</tr>
<tr>
<td>Americas</td>
<td>Latin Americans</td>
</tr>
<tr>
<td>Asia</td>
<td>Southeast Asians</td>
</tr>
<tr>
<td>Europe</td>
<td>Middle Eastern</td>
</tr>
<tr>
<td>Middle East</td>
<td>Southeast Asians</td>
</tr>
</tbody>
</table>

MOST VICTIMISED OCCUPATIONAL SECTOR BY REGION

<table>
<thead>
<tr>
<th>Industry</th>
<th>Number of Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unskilled</td>
<td>77</td>
</tr>
<tr>
<td>Unknown</td>
<td>20</td>
</tr>
<tr>
<td>Businesspeople</td>
<td>19</td>
</tr>
<tr>
<td>Maritime</td>
<td>19</td>
</tr>
<tr>
<td>Tourists</td>
<td>8</td>
</tr>
<tr>
<td>Construction</td>
<td>6</td>
</tr>
<tr>
<td>Journalists</td>
<td>3</td>
</tr>
<tr>
<td>Oil &amp; Gas</td>
<td>3</td>
</tr>
<tr>
<td>Professionals</td>
<td>2</td>
</tr>
<tr>
<td>Education</td>
<td>2</td>
</tr>
<tr>
<td>Dependents</td>
<td>1</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.
The Gulf of Aden continued to record low piracy levels. This is in part due to the southwest monsoon season, alongside the effectiveness of security measures. On the other hand, terrorist-related incidents increased over July and August. Of concern, on 22 July the Landing Craft Alpha Kirawira came under mortar fire approximately 1NM offshore Barawe, Somalia. Onboard security personnel returned fire and the vessel reached Barawe Port safely. The vessel has been carrying AMISON supplies for several years and was most likely targeted by Al Shabaab attacks on vessels are rare. Meanwhile, security conditions off Yemen’s coast remained volatile. Incidents in July included a Houthi attack on two Saudi Arabian-flagged tankers off Hodeidah and a Small Arms Fire (SAF) attack on a bulk carrier southwest of the Hanish Islands. On 23 August, the Saudi-led coalition foiled a Houthi attack on commercial vessels, involving the use of explosive-laden speedboats. No further details were disclosed. Commercial vessels are at considerable risk of collateral damage, with those affiliated with the war parties facing a high risk of attacks.

Maritime security incidents in the Gulf of Guinea decreased markedly in the July-August 2018 period compared to the previous two months. Criminal boardings accounted for the majority of recorded incidents. A hijacking off Gabon and four armed attacks were also reported. The overall decrease in hostility is not uncommon, as the frequency of maritime incidents has declined over the summer months in the past. This is mainly due to prevailing weather conditions between May and October, which hinder the navigation of small vessels offshore. Notably, August was the first month since August 2017 when no offshore incidents were recorded in the Nigerian Exclusive Economic Zone. Nonetheless, data suggests pirates have adapted their modus operandi, perpetrating attacks closer to the coast or within inland waters. Despite low activity over July and August, the piracy threat in the region remains severe. An increase in piracy is expected following the end of the rainy season in September.

The piracy threat throughout Southeast Asia remains significant, despite a downward trend observed in recent years. A total of 40 incidents were recorded between January and June 2018, the lowest figure since 2009. The majority of incidents recorded in the first half of 2018 (37) were criminal boardings. Most attacks involved up to six mostly unarmed assailants, with violence relatively uncommon. Vessels, predominantly bulk carriers and tankers, were largely targeted whilst at anchor, with a majority of attacks being opportunistic in nature. Over July and August 2018, nine criminal boardings and a hijacking were recorded. While criminal boardings will likely remain the primary threat to commercial operations in the region, an underlying risk of violent piracy remains. Also of concern, the Abu Sayyaf Group (ASG) piracy threat endures. On 3 July, Sabah authorities announced they decided to extend the sea curfew over the Eastern Sabah Security Zone (Esszone), which was first imposed four years ago, until 13 September. The decision was based on continuous cross-border threats, including attacks by kidnap-for-ransom groups and the ASG. Although security approaches, such as military actions and amnesty programmes, have diminished ASG’s ability to target commercial vessels in the Sulu and Celebes seas, continuous attacks reported on fishing vessels and a kidnapping of crew recorded on 11 September, clearly indicate ASG continues to pose a credible threat in the region.

### CASES:

**On 24 July, two very large crude carriers operated by Bahri, Saudi Arabia’s national shipping company, were attacked by Houthi rebels approximately 68NM west of Hodeidah. One vessel sustained minor damage, with no injuries or oil spill reported. No further details surrounding the attack were disclosed. As a result, on 25 July Saudi Arabia announced it would temporarily halt all oil shipments through the Bab al-Mandeb Strait. These were resumed on 2 August. The incident highlighted the enduring insecurity in the Strait. At least, seven attacks on vessels in the area were linked to the Yemeni conflict between 2016 and 2017. At least three attacks have been attributed to the Houthis since the beginning of this year, with only one targeting a vessel not affiliated with the war parties.**

**On 19 August, two Malaysia-flagged fishing boats with 11 crew were stopped approximately 3NM off Pulau Langun in Langkawi, Malaysia, by two vessels with a total of 12 Thai nationals aboard. The Malaysians were robbed and captured. On the same day, Malaysian authorities intercepted one of the boats belonging to the attackers, rescuing seven victims and arresting four Thai suspects, including three policemen. The other suspects escaped, taking the remaining four fishermen to Thailand. The victims were subsequently released by Thai authorities and repatriated on 20 August. Reports surrounding the incident have been conflicting, with Thailand claiming the attackers were in fact patrolling Thailand’s territorial waters to prevent illegal fishing. Yet, the policemen involved in the incident were working for Muang Satun Police Station, which has no authority to intercept fishing vessels at sea. Seven Thai officers have reportedly been suspended, amid ongoing investigations into the matter.**
As cryptocurrencies continue to proliferate and gain in popularity, cybercriminals are increasingly utilising cryptomalware to surreptitiously ‘mine’ cryptocurrency from victims’ devices. Recent studies have indicated that this activity, also known as ‘cryptjacking’, has seen exponential growth. Only in the first half of 2018, the number of detections showed a 956% increase over the same period last year, replacing ransomware as the top detection. Targets from this type of fraud range from single users, to large multinational organisations and governments. It has been estimated that in the UK, in July 2018 alone, approximately 30% of large businesses were the victims of cryptomining attacks. Moreover, according to research by Citrix and OnePoll, 59% of UK businesses have detected cryptomining attacks on their systems at some point.

Cryptomining itself is not an illegal activity. It involves solving complex computational problems to verify digital transactions, rewarding miners with new cryptocurrencies as well as ‘minting’ new cryptocoins. While many users have taken to cryptomining to turn a profit, the process for their funding, instead of running advertisements. Cryptojacking attacks also utilise this method, setting up cryptomining scripts to run on websites without the domain owner’s knowledge or permission. Unlike other forms of malware, cryptomining is intended to run undetected for as long as possible; to ensure maximum profits for the attacker. A single device is generally not powerful enough to mine cryptocurrencies profitably, so cybercriminals seek to attack multiple devices simultaneously. This way, they can pool the collective power of all the devices they have breached to mine more cryptocurrency. Cryptomining is not limited to computers, but can also target mobile devices.

There are a number of methods by which cyber criminals breach devices with cryptomining. These include server exploits, malvertisements, phishing attacks with malicious links in emails or on webpages, as well as targeted hacking attacks to remotely access a victim’s device and cryptopack it. Moreover, it was recently found that over 100,000 app downloads from a popular ‘App Store’ had been reported as containing hidden cryptomining mining malware. The use of cryptomalware to fraudulently mine cryptocurrency is not unique to hackers. A recent phenomenon has arisen whereby websites are progressively leaning toward using browser-based cryptocurrency miner. In the case of the ‘The Pirate Bay’, whenever a user visited the website, a secret cryptomining script was found to be running browser-based cryptomining miner. In the case of the ‘The Pirate Bay’, whenever a user accessed the website, a secret cryptomining script ran in the background, utilising the CPU power of the user’s device to mine the cryptocurrency. Other cryptomining attacks also utilise this method, setting up cryptomining scripts to run on websites without the domain owner’s knowledge or permission. Earlier this year, it was found that thousands of websites, including those of popular sites such as The Pirate Bay, were found to be running browser-based cryptocurrency miners.

Apart from victims not reaping any of the benefits from mining cryptocurrency, their devices suffer a severe impact on performance by unknowingly running cryptomining. As mining is a computationally-intensive process, devices may run slowly or are not be able to function normally. Furthermore, they increase the rate at which they consume electricity. While not often significantly detrimental to single users (other than a drop in their device’s performance), large organisations that have been breached may endure a significant financial impact, with higher electricity bills, a reduction in productivity due to a slow-down in computer performance and needing to replace processors on compromised machines ahead of the computer’s normal lifecycle. There are a number of preventative measures users and businesses can take to minimize the risk of being breached by cryptomining. These include;

- Disabling JavaScript to block cryptomining scripts from running on malicious websites
- Installing an ‘ad-blocker’ or anti-cryptomining extensions on web browsers
- Blocking certain domains or avoiding visits to known mining websites
- Monitoring CPU usage for suspicious spikes
- Ensuring cyber security protocols and training for staff are up-to-date

### CASES:

- ‘WannaMine’ is a cryptomalware that was discovered in October 2017. Propagating through the same ‘Eternal Blue’ exploit also used by the ‘WannaCry’ ransomware, ‘WannaMine’ hijacks devices’ processors to mine cryptocurrency. This cryptomalware is extremely difficult to detect, given that it doesn’t download any applications onto the compromised machine, instead using inbuilt Windows tools. ‘WannaMine’ was found to have infected dozens of organisations when it was discovered, severely compromising operations for days and weeks in some cases. Demonstrating that it remains a significant threat, a major, undisclosed Fortune 500 multinational suffered a serious WannaMine breach in September 2018, with over 1,000 machines infected on the first day of the attack.

- ‘Coinhive’ has been identified as the top malware threat, as it is a browser-based cryptomining malware that only needs a user to visit a website for the cryptomining script to run and start mining cryptocurrency using the user’s device. It was recently estimated that the ‘Coinhive’ mining script was being run on 32,000 websites, either intentionally or by hackers. Furthermore, during August 2018, it was reported to have affected 17% of organisations worldwide. Several websites of high profile governments and organisations were reported to have been breached, including English Councils, Blackberry and the Los Angeles Times. The script runs as long as a user is visiting the website.
Among all sectors that constitute a nation’s critical infrastructure, the energy sector is uniquely important because it provides an enabling function across all other sectors. Its incapacitation or destruction could therefore have a serious effect on a nation’s economy and security in broad terms. As such, this sector faces a variety of threats, ranging from terrorism and criminality, to espionage and social activism, all of which can be physical or virtual (through cyberattacks).

Terrorist organisations have always been interested in targeting critical infrastructure, particularly energy facilities, not only for the magnitude of the consequences but also because of its symbolism. According to recent studies, terrorist threats targeting the energy sector have risen sharply in the last two decades, already accounting for about 23% of total terror attacks by 2013. These attacks have primarily taken place in the Middle East, Africa and Latin America. Pipelines are one of the main targets for these attacks, as they are very easily sabotaged. Having said this, larger infrastructure such as petrochemical complexes and oil installations, being high-profile targets, may also be attractive to militants. It is believed that a number of minor attacks are carried out to assess a target’s response capabilities and vulnerabilities in preparation to potential larger attacks.

While Islamic terrorist groups have targeted critical infrastructure in the past and certainly possess the capabilities to do so, it is in fact separatist, nationalist and Marxist groups, who have typically shown a greater proclivity to attack targets of this nature.

Moreover, criminal activity targeting the energy sector, particularly the oil and gas industry, poses considerable challenges for states, reducing state revenue and affecting foreign direct investment. This also provides funds for wider violent activity, which may well include terrorism. Carried out at different scales, in many cases being part of larger criminal enterprises and intermingled in wider criminal cycles, these activities are particularly persistent in countries suffering from poor rule of law, poor socio-economic conditions and a pervasive criminal culture. They have a direct serious impact on national security and the economy, also furthering state fragility. Smuggling is of particular concern to the industry, being an attractive criminal activity due to its low barriers to entry and not perceived critical for law enforcement. In recent times, organised crime and militant groups in some countries have increasingly been involved in oil smuggling, profiting from porous borders and their existing criminal networks. These groups commonly use existing corruption networks to sell large quantities of unreported product on the black market. The direct theft of oil from ships and pipelines, also known as bunkering, is however the most pressing current concern both in economic and security terms. This activity, being highly complex and requiring a certain degree of technical knowledge, is typically carried out by well-resourced groups. Although piracy-related bunkering has decreased in recent times, result of the security focus on this problem, it is an enduring concern as piracy groups retain their intent and capabilities. The kidnapping of personnel is also of particular concern. Regarded as better paid than people working in other industries, employees in the energy sector, especially in the oil and gas industry, are commonly targeted for kidnapping and extortion.

Activism is a growing concern for the energy sector in both developed and developing countries as environmentalist and social groups have shown themselves increasingly hostile to its activities, carrying out attacks on personnel and facilities. A number of governments have in recent years warned of the rising threat to critical infrastructure from domestic pressure groups described as “extremists” and of the growing use of criminal and terrorist-type means to force companies to forgo operations. A number of these organisations, particularly larger ones with significant financial and legal resources, are also striving to undermine the strategies and operations of energy companies. The use of media to damage company reputation is also increasingly common.

Cyber threats are not only new but constantly evolving, with far-reaching consequences; becoming today’s most pressing concern across all critical infrastructure sectors. A wide range of hostile actors use the cyber space to target a nation’s critical infrastructure, including foreign states, criminals, “hacktivist” groups and terrorists. While governments, businesses and individuals are devoting greater resources to becoming more cyber-vigilant, cyber-attacks are very difficult to prevent. Critical infrastructure currently relies heavily on IT networks and other cyber support to operate, making it highly vulnerable to cyber intrusions. Some of the latest attacks have involved malware targeting industrial automation control systems, which block or delay the flow of information or make unauthorized changes to programmed instructions, resulting in malfunctioning of infrastructure. The power sector has been seen to be particularly vulnerable to this type of attacks.

The complex operating architecture of today’s critical infrastructure, in addition to the ever-evolving nature of threats, renders it extremely challenging to protect and secure. Holistic approaches to security are thus necessary in such a context. While the primary obligation of securing critical infrastructure lies heavily on the state, in a world where an increasing number of these assets are privately owned, there is a shared responsibility between the state and individual owners and operators.
**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

---

**CONTACT**

For more information on this report please contact:

BEATRIZ SANCHEZ-GARRIDO
Information Analysis Manager
beatriz.sanchez-garrido@constellis.com

For all enquiries on Constellis’ advisory & consulting services please contact:

MARK ALLISON
Vice President, Crisis & Risk Services
Mobile: +44 7791 495 057
mark.allison@constellis.com

Crisis Response Emergency Numbers:

**NORTH/SOUTH AMERICA**
+1 713 916 6401

**EUROPE, AFRICA, ASIA, AUSTRALIA**
+44 (0) 20 7 240 3237

**GENERAL INQUIRIES**
+971 800 100 100

THE INFORMATION IN THIS REPORT IS PROVIDED "AS IS" WITHOUT ANY WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. CONSTELLIS, MAKES NO REPRESENTATION OR WARRANTY THAT THE INFORMATION CONTAINED IN THIS REPORT WILL BE TIMELY OR ERROR-FREE. IN NO EVENT SHALL CONSTELLIS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL OR ANY OTHER DAMAGES, ARISING OUT OF OR IN CONNECTION WITH THE USE OF OR RELIANCE ON INFORMATION AVAILABLE WITHIN THIS REPORT. IN USING THIS INFORMATION, YOU ARE USING IT AT YOUR OWN RISK AND AGREE TO THE LIMITATIONS AND DISCLAIMERS PROVIDED HERE.