„Ohne mich würde niemand die Pink Panther kennen“

Andrea Scholz deckte das internationale Netzwerk der „Pink Panther“ auf. Die Juwelendiebe aus Serbien, Montenegro, Kroatien und Bosnien sind für die weltweit wohl spektakulärsten Raubüberfälle mit einem Schaden im Wert von geschätzten 500 Mio. USD verantwortlich. Gemeinsam mit Europol, Interpol und ihrem Team aus Mitgliedern der deutschen Antiterroreinheit (GSG9), dem BKA, MEK und Spezialverbänden verfügt sie über einmalige Einblicke.

“If it weren‘t for me, no-one would have heard of the Pink Panthers” – Andrea Scholz exposed the international network of the “Pink Panthers”. The jewel thieves from Serbia, Montenegro, Croatia and Bosnia are responsible for the most spectacular robberies worth an estimated 500 million dollars. Collaboration with Europol, Interpol and a team comprising members of the German counter-terrorism unit (GSG9), the German federal office of criminal investigation (Bundeskriminalamt, BKA), mobile task forces (MEK) and special forces has provided her with unique insights.

„Ohne mich würde niemand die Pink Panther kennen“

Bild/Image: istock.com/Cactusimage

Frau Scholz, wie werden große Raubfälle vorbereitet? Welche Ressourcen sind notwendig und was wird getan?

Grundsätzlich gibt es keine Zufälle in diesem Milieu. Weshalb ich seit Beginn meiner Tätigkeit in diversen Risikobereichen auch den Leitspruch von Voltaire übernommen habe: „Zufall ist ein Wort ohne Sinn, nichts kann ohne Ursache existieren.“ Täter wählen sich ihre Objekte gezielt aus und entscheiden dies nicht am Morgen während des Frühstücks. Es gibt zahlreiche sogenannte Aufklärer, die diverse Einrichtungen „besuchen“, sich die Abläufe genauestens ansehen. Registriert wird alles, was sicherheitsrelevant ist und Zugang zum lohnenden Objekt verschafft. Dabei sind banale Dinge, die für Mitarbeiter oder echte Kunden gar nicht auffällig sind, möglicherweise entscheidend für die spätere Entscheidung, in dieses Objekt einzubrechen oder es zu überfallen.

Große Ereignisse benötigen zudem eine Menge Manpower und Know-How. Die eingesetzten Finanzmittel zur Beschaffung von Fluchtfahrzeugen, Pässen, Reisen und Waffen wird kalkuliert und gegen den zu erwartenden Gewinn verrechnet. Eine Kosten-Nutzen-Analyse wie in jedem gut geführten Unternehmen auch. Erst wenn der Gewinn lohnenswert erscheint, wird eine Tat weiter vorbereitet. Ansonsten wird abgebrochen und ein „einfacher zu überwindendes“ Objekt ausgewählt. Aufgeklärt wird alles: mechanische, elektronische und personelle Absicherungen. Gibt es Schwachstellen, wird an diesen angesetzt. Für die Durchführung wird ein Minimum an Zeit kalkuliert, da meist eine Alarmauslösung zur Folge hat, dass man den Tätern schnell auf die Spur kommt. Um das zu verhindern, wird auch alles für die Zeit nach dem Raub bestens organisiert.

Die Fluchtmittel und eventuell genutzte Maskierungen werden auf der Flucht weggeworfen. Teilweise erfolgt auch ein Wechsel der Kleidung. Ware und Täter bleiben nur für wenige Zeit gemeinsam fassbar. Nach wenigen Minuten, maximal Stunden, geht die Ware einen zuvor gut ausgeklügelten Transportweg – geschmuggelt oder legal mit gefälschten Transportdokumenten. Die Täter nehmen einen ganz anderen Weg.

Wenn ein Raub gelingt – was waren die entscheidenden Faktoren für den Erfolg?

Grundsätzlich die vorhandenen Absicherungen. Zuerst die, die zur Sicherung der Ware installiert wurden, später dann auch die, die von Tätern zu ihrem eigenen Schutz aufgebaut wurden. Entscheidend ist immer der Zeitfaktor: Wie lange dauert es bis die begehrliche Ware entwendet werden und man selbst sicher entkommen kann? Schwachstellen werden gnadenlos analysiert und sogar getestet. So wird auch schon lange vor der Tat nächtlicher Alarm ausgelöst und gewartet was passiert. Sind mechanische und elektronische Absicherungen sehr gut, dann ist eventuell der Faktor Mensch das schwächste Glied in der Absicherungskette und Möglichkeiten mittels Social Engineering oder Kidnapping werden evaluiert.

Täter haben alle Zeit der Welt, um an ihr Ziel zu gelangen. Es ist schlicht egal, ob jemand über Monate observiert werden muss, nur um eine wichtige Schlüsselposition zu knacken.

Wie kann man sich ‚den Mensch dahinter‘ vorstellen?

Der Mensch dahinter sieht aus wie „du und ich“. Menschen mit Familie und Kindern, die lachend Urlaub am Meer verbringen. Organisierte Tätergruppen weisen überwiegend eine strenge hierarchische Struktur auf. Da sind die, die Taten ausführen, Aufklärer, die Sicherheitseinrichtungen und Opferverhalten auskundschaften, Transporteure, Helfer, Hehler und Auftraggeber. Letzterer ist niemals in direktem Kontakt mit den unteren Ebenen. Kommunikationswege werden über alle erdenklichen Kanäle geführt und umgeleitet. Bei ganz wichtigen Gesprächen wird das persönliche Gespräch immer noch als Mittel erster Wahl genommen.

Jeder der Beteiligten hat seine Aufgabe und ist auf seinem Gebiet über Jahre hinweg gewachsen: Wir haben es teilweise mit richtig guten Experten zu tun, die auf dem normalen Arbeitsmarkt mit ihrem Fachwissen als Spezialisten für Alarmanlagen oder Glasbeschaffenheit ein enorm gutes Gehalt verdienen würden.

Hilflos ausgeliefert ist man diesen Tätern dennoch nicht. Es gibt Mittel und Wege wie man sich schützen kann. Zum einen mittels installierter Absicherungsmaßnahmen wie sinnvoller Mechanik, Elektronik und Videotechnik, aber auch, und das ist der weitaus wichtigste Faktor, mittels aufgeklärtem und geschultem Personal. Wer weiß wie Täter arbeiten, wird mehr Sicherheitsbewusstsein erlangen und wissend agieren können. Schulungen zur Erlangung dieses Wissens sind ständig an die neuen Vorgehensweisen anzupassen und regelmäßig durchzuführen, um im Ernstfall zu wirken.

Ms Scholz, how do perpetrators prepare for major robberies? What resources do they need and what do they do?

Basically, nothing is left to chance in this setting. Which is why I chose a saying by Voltaire as my motto when I started working in various risk areas: “Chance is a word void of sense; nothing can exist without a cause.” Perpetrators select their objects systematically, rather than making random decisions during breakfast. There are numerous “scouts” who “visit” various facilities to thoroughly study the procedures, doing reconnaissance. They register all security-relevant details required to get access to the object of desire. Even the most trivial details that wouldn’t be noticed by employees or real customers may be decisive for the subsequent decision to break into or rob a particular facility.

In addition, major undertakings require a lot of man-power and know-how. The financial means required to buy getaway vehicles, passports, tickets, weapons and the like are calculated and offset against the anticipated profit: a cost/benefit analysis as in any other well-managed enterprise. Only if the profit seems worth the trouble will the preparations for the criminal act be continued. Otherwise, the project will be abandoned, and some other object that can be “entered more easily” will be chosen. A full reconnaissance is made with regard to mechanical, electronic and personal security measures. If they find any weak spots, this is where they start. A minimum of time is calculated for executing the robbery, for once an alarm is triggered, perpetrators are often caught very quickly. In order to prevent this, the getaway part following the robbery is also perfectly organised down to the tiniest detail.

The means of escape and any disguises that may have been used are discarded during the getaway. Sometimes a change of clothes is involved as well. There is only a very short period of time during which the perpetrators could be caught with the stolen goods. After a few minutes, hours at most, the stolen goods will be on their previously well-thought-out transport route – either smuggled or even shipped legally, with forged transport documents. The perpetrators will take an entirely different route.

If the robbery succeeds – what were the decisive factors for its success?

Basically, it’s the security measures involved. First of all those that were put in place to protect the goods, subsequently also those that were implemented by the perpetrators for their own protection (getaway and time factors to conduct the robbery).

It is always the time factor that is decisive: how long does it take for the desired goods to be stolen and for the perpetrators to escape safely? Weak spots are analysed relentlessly, and even tested. For instance, long before the date of the planned robbery, an alarm may be triggered at night to see what happens. If the mechanical and electronic safety measures are excellent, the human factor may be the weakest link in the chain of security measures, and options involving social engineering or kidnapping will be evaluated.
Perpetrators have all the time in the world to achieve their goal. It simply doesn’t matter whether they have to stake out a person for months just to crack a key position.

What kind of person is behind such a scheme?

The person behind it is just someone “like you and me”. People with a family, with children, who enjoy spending a holiday on the beach. The majority of organised gangs are based on strictly hierarchical structures. There are those who actually perform the criminal acts, then there’s the scouts who stake out safety systems and victim behaviour, also drivers, helpers, fences, and the principal. The latter is never in direct contact with the lower tiers.

Communication is effected and redirected via every conceivable channel. When it comes to extremely important matters, face-to-face meetings still are the measure of choice.
Every member of the team has their task and has perfected their expertise over the years: some of them are outstanding experts who would earn a large salary on the regular job market with their expert knowledge as specialists for alarm systems or the characteristics of glass.

However, we are not completely and utterly at the mercy of such perpetrators. There are ways and means to protect ourselves: on the one hand, by means of security measures such as reasonable mechanical, electronic and video systems, on the other hand, and that is even much more important, through well-informed and well-trained personnel. Anyone who knows how perpetrators work will be able to act with greater confidence and knowledge when it comes to security. For training to be effective in an emergency, courses meant to convey the relevant knowledge must be adjusted to the new practices and conducted on a regular basis.