



September 2024

KÜNSTLICHE INTELLIGENZ

Es ist offensichtlich daß sich die Nutzung von „Künstliche Intelligenz“ (K.I.) nicht nur im staatlichen Kontext, sondern auch auf privater Ebene, immer weiter ausweitet. Mit der Zeit gibt es neue Verwendungsmöglichkeiten und K.I. nimmt daran Teil sich selbst zu verbessern und robuster zu gestalten. Aus diesem Grunde wird ein Teil jedes folgenden Rundbriefes K.I. gewidmet.



Inhaltsverzeichnis:

- 1-2 Künstliche Intelligenz & Logik
- 2-3 Angreifer mit Messer (Maßnahmen K.I.)
- 3-4 K.I. Diagnose bei Verletzungen
- 5-6 Diese Mittel sind nicht erlaubt Gesetze, Vorschriften, und Bürokratie beim Staat
7. Weiteres über K.I. „Der Elefant“
- 7-8 Der Datenhacker und Schutzmaßnahmen
8. Police-App: Bewerbungsauskünfte
9. Sicherheitsunternehmen in Ekuador (Nicht unbedingt sicher)
10. Nordkorea-Erweiterung der Staats-sicherheit

Das Bild mit dem Polizeieichhörnchen war das Resultat einer Bitte an ChatGPT ein deutsches Polizeieichhörnchen das einen Rundbrief liest zu entwickeln. Auf dem ursprünglichen Bild hieß es aber ROUNDBRIFF, und das mußte man dann manuell korrigieren. Dabei sieht man das deutsche Wort POLIZEI auf dem Hemd, aber das englische Wort POLICE an der Hose. Also fragte ich KI warum das so ist, und erhielt folgende Antwort:

Das Bild zeigt eine interessante Mischung von Details, die sowohl deutsche als auch englische Begriffe beinhalten, was möglicherweise auf die kreative Freiheit bei der Erstellung des Bildes zurückzuführen ist. Hier sind einige Gründe, warum diese Diskrepanz auftreten könnte:

1. **Künstlerische Interpretation:** Bei der Erstellung solcher Bilder werden oft künstlerische Freiheiten genutzt, um humorvolle oder verspielte Darstellungen zu schaffen. Es kann sein, dass die Kombination von "Polizei" auf Deutsch und "Police" auf Englisch bewusst gewählt wurde, um einen internationalen oder universellen Charakter darzustellen.
2. **Fehler oder Inkonsistenz:** Ein solcher Unterschied könnte auch einfach ein kleiner Fehler oder eine Inkonsistenz in der Darstellung sein. Da das Bild von einer KI generiert wurde, kann es manchmal zu Missverständnissen oder fehlerhaften Interpretationen bei der Platzierung von Texten kommen.

LOGIK DER K.I. DARSTELLUNGEN

3. **Symbolische Darstellung:** Die Verwendung beider Begriffe könnte symbolisch gemeint sein, um zu betonen, dass das Eichhörnchen eine Figur ist, die internationale Polizeibezüge hat, oder um eine humorvolle Vielfalt in der Darstellung der Uniform zu schaffen.

ANGREIFER MIT MESSER (Maßnahmen laut K.I.)

Mit der relativ hohen Anzahl von Messerstechereien in Deutschland, war es interessant mal K.I. zu fragen wie sich ein Polizeibeamter verhalten sollte, wenn er mit einem Angreifer mit Messer konfrontiert ist.

In diesem Zusammenhang konnte K.I. zusätzlich ein Symbolbild erstellen.



Wenn ein Polizeibeamter von einer Person mit einem Messer bedroht oder angegriffen wird, gibt es eine Reihe von Taktiken und Vorgehensweisen, die er befolgen sollte, um die Situation zu deeskalieren und die Sicherheit aller Beteiligten zu gewährleisten. Diese Maßnahmen basieren auf den Grundprinzipien der Polizeiarbeit und der Einsatzsicherheit. Hier sind einige allgemeine Richtlinien:

1. Situation beurteilen und Abstand halten

- *Einschätzung der Bedrohung:* Der Beamte sollte sofort die Bedrohung einschätzen, indem er die Distanz zum Messerstecher und die Umgebung berücksichtigt.
- *Sicherheitsabstand:* Es ist entscheidend, einen sicheren Abstand (mindestens sieben Meter) einzuhalten, da dies die Reaktionszeit erhöht und die Gefahr eines unmittelbaren Angriffs verringert.

2. Deeskalation und Kommunikation

- *Verbale Deeskalation:* Der Beamte sollte versuchen, die Situation durch verbale Kommunikation zu beruhigen. Dies beinhaltet klare und laute Aufforderungen, das Messer fallen zu lassen, und gleichzeitig beruhigende Worte, um die Spannung zu reduzieren.
- *Selbstschutzmaßnahmen:* Während der Kommunikation sollte der Beamte sich in einer stabilen Position halten, die ihm eine schnelle Reaktion ermöglicht.

3. Anwendung von Einsatzmitteln

- *Nicht-tödliche Einsatzmittel:* Falls möglich und sicher, sollte der Beamte nicht-tödliche Einsatzmittel wie Pfefferspray, Taser oder einen Schlagstock einsetzen, um den Angreifer zu neutralisieren, ohne tödliche Gewalt anzuwenden.
- *Waffe ziehen:* Sollte die Bedrohung als schwerwiegend und unmittelbar eingestuft werden, muss der Beamte bereit sein, seine Schusswaffe zu ziehen und, falls notwendig, gezielt zu schießen, um die Gefahr zu stoppen. Die Anwendung tödlicher Gewalt ist immer die letzte Option und muss verhältnismäßig und rechtmäßig sein.

4. Rückzug und Verstärkung anfordern

- *Rückzugsposition finden:* Wenn möglich, sollte sich der Beamte in eine Position zurückziehen, die ihm mehr Schutz bietet (z. B. hinter einem Fahrzeug oder einer Barriere).

K.I. ANLEITUNG BEI MESSERSTECHER

- *Verstärkung anfordern: Sofortige Anforderung von Verstärkung und Notfallmedizinischer Unterstützung (RTW) über Funk ist entscheidend, um die Situation sicherer zu machen und potenzielle Verletzungen zu behandeln.*

5. Fortlaufende Gefahrenbewertung

- *Situation kontinuierlich bewerten: Der Beamte sollte die Situation kontinuierlich neu bewerten, auf Veränderungen reagieren und Anpassungen an seiner Vorgehensweise vornehmen.*

- *Nach einem Einsatz handeln: Sollte der Beamte das Messer verwenden müssen, ist eine umfassende Berichterstattung, die Sicherung der Beweise und die Einhaltung der rechtlichen Vorgaben erforderlich.*

6. Erste Hilfe leisten

- *Medizinische Erstversorgung: Nach einem Einsatz, insbesondere wenn es zu Verletzungen gekommen ist, muss der Beamte sicherstellen, dass so schnell wie möglich medizinische Hilfe geleistet wird, sowohl für den Angreifer (falls sicher) als auch für eventuell verletzte Personen.*

Diese Vorgehensweise kann je nach den spezifischen Gesetzen und Richtlinien des Landes oder der Behörde variieren, aber sie bietet einen allgemeinen Überblick über das Standardprotokoll, das Polizeibeamte in solchen gefährlichen Situation befolgen sollten.

Eine generelle Anfrage (ohne Fotos) über die Behandlung oder dem Vorgehen bei einer Schußwunde, war ebenso detailliert und glaubwürdig.

Eine Einschätzung der verschiedenen Gefahrenlagen und die Auswahl möglicher Einsatzmethoden- und Mittel durch K.I., kann auf den ersten Blick erfolgsversprechend sein, aber wie es schon in der K.I. Anwendung klargemacht wird, ist K.I. nicht fehlerfrei. Nur menschliche Intelligenz kann einen

möglichen Chaos erkennen und auch abwenden. K.I. ersetzt nicht die menschliche Intelligenz, und das Treffen von Entscheidungen kann man nicht einfach K.I. überlassen.

Die Reichweite von K.I. Anwendungen ist dazu eine Frage der menschlichen Kreativität. Man weiß nicht wie man K.I., im eigenen privaten oder beruflichen Bereich anwenden kann, bis man es versucht. Dabei gibt es dann Überraschungen.

K.I. DIAGNOSE BEI VERLETZUNGEN

Ein Unfall auf dem Laufband eines Fitnesszentrums führte z.B. zu folgenden Verletzungen:



Ohne vorigen Erfahrungen mit ähnlichen Verletzungen meint man zuerst daß ein Termin bei einem Arzt notwendig sei.

Aber was würde K.I. dazu sagen? Kann es nur anhand der Fotos eine Diagnose erstellen und Ratschläge zur Behandlung geben?

Also ladet man dann die Fotos der Verletzungen auf ChatGPT hoch. In diesem Falle kamen die Diagnose und Ratschläge in rund 15 Sekunden. Wie schon in verschiedenen Artikeln berichtet, kann sich eine durch K.I.

DIAGNOSE DURCH K.I.

erstellte medizinische Diagnose gut sehen lassen, und stimmt in den meisten Fällen mit einer echten ärztlichen Diagnose überein.

Einschätzung:

1. Abschürfungen:

- Die Haut ist an einigen Stellen abgeschürft, wodurch das darunterliegende Gewebe freigelegt ist. Dies kann zu leichtem Bluten und Unbehagen führen.

- Die Abschürfungen sind nicht tief in die Haut eingedrungen, was ein gutes Zeichen ist.

2. Blutergüsse:

- Es ist sichtbare Rötung und Blutergüsse um das Knie herum zu erkennen, was auf ein Trauma des darunterliegenden Gewebes hindeutet.

- Die Blutergüsse könnten Schmerzen und Unbehagen verursachen, besonders bei Bewegung des Knies.

Empfohlene Behandlung:

1. Reinigung:

- Erster Schritt ist, die Wunde mit mildem Seifenwasser oder Kochsalzlösung zu reinigen, um Schmutz oder Fremdkörper zu entfernen. Vermeiden Sie es, starke Antiseptika wie Wasserstoffperoxid direkt auf die Wunde aufzutragen, da dies das Gewebe reizen könnte.

2. Antibiotische Salbe:

- Nach der Reinigung eine dünne Schicht einer antibiotischen Salbe wie Neosporin auftragen, um eine Infektion zu verhindern.

3. Verband:

- Die Abschürfungen mit einem sterilen Verband oder einer Mullbinde abdecken. Wechseln Sie den Verband täglich oder wenn er schmutzig oder nass wird.

- Da das Knie bei Bewegung wahrscheinlich stärker beansprucht wird, sollten Sie einen Verband verwenden, der flexibel ist und sich mit der Haut bewegt, um Reizungen zu vermeiden.

4. Schmerzbehandlung:

- Schmerzmittel, die ohne Rezept erhältlich sind, wie Ibuprofen oder Paracetamol, können bei Schmerzen und Entzündungen helfen.

- Das Auflegen eines Eisbeutels auf den verletzten Bereich für 15-20 Minuten mehrmals am Tag kann ebenfalls Schwellungen reduzieren.

5. Überwachung:

- Achten Sie auf Anzeichen einer Infektion wie zunehmende Rötung, Wärme, Schwellung oder Eiterbildung. Falls diese auftreten, suchen Sie einen Arzt auf.

- Stellen Sie sicher, dass die Wunde sauber und trocken bleibt, um die Heilung zu fördern.

6. Schonung:

- Vermeiden Sie es, zu viel Druck oder Belastung auf das verletzte Bein, insbesondere auf das Knie, auszuüben, um die Heilung zu unterstützen.

Diese Maßnahmen sollten dazu beitragen, dass die Abschürfungen und Blutergüsse innerhalb weniger Tage bis zu einer Woche heilen. Falls sich der Zustand verschlechtert oder nicht verbessert, ist es möglicherweise notwendig, einen Arzt aufzusuchen.

Zwei Wochen nach diesem Unfall besuchte ich einen Arzt, und seine Diagnose und Behandlungsvorschläge deckten sich mit der „kostenlosen“ 15 Sekunden Diagnose von ChatGPT. Man muß dazu aber noch erwähnen, daß diese K.I. Diagnose nur mit einem ChatGPT Abonnement möglich ist.

Das auf ChatGPT hochgeladene Foto kann man weder löschen noch zurückfordern. Bei Routinefragen oder Anfragen ohne Verbindung zu Verschlußsachen, kann K.I. das Leben im privaten und, je nach Vorschriften oder gesetzlichen Regelungen, auch im dienstlichen Bereich vereinfachen. Unter den geschätzten mehr als 100 K.I. Anwendungen, sind auch solche die nicht öffentlich zugänglich sind, aber

K.I. ANWENDUNGEN...

für verschiedene staatlichen Dienste mit Zugang zu internen Daten aktiv sind.

DIESE MITTEL SIND NICHT ERLAUBT BÜROKRATIE, GESETZE & VORSCHRIFTEN

Erfahrungsgemäß sind diese staatlich betriebenen Systeme weit wirksamer und erfolgreicher bei der Erkennung und Überwachung von kriminellen oder staatsgefährdenden Personen, und der Verhütung von Straftaten, als allgemein veröffentlicht wird. Firmen die vertraglich solche Systeme für staatliche Dienste bereitstellen, haben den Vorteil daß sie die dazu benützten Algorithmen nicht preisgeben müssen, da diese in einer Wettbewerbsgesellschaft als Geschäftsgeheimnis eingestuft sind. Dadurch haben auch die unter Vertrag gestellten staatlichen Sicherheitsdienste keinen Zugang zu den Algorithmen. Das erübrigt rechtliche Klagen an die Sicherheitsdienste selbst, um die Veröffentlichung der Algorithmen zu erzwingen.

Während einer Präsentation in Deutschland über die Fähigkeiten eines dieser Systeme, inklusiv echter Beispiele verschiedener Recherchen über staatsfeindliche Aktivitäten in Deutschland, wurde mir gesagt: *Ach das ist toll, aber wird dürfen hier so etwas nicht verwenden.*

Viele dieser neuen K.I. betriebenen Systeme sind in Deutschland, und manchen anderen E.U. Ländern, entweder gesetzlich nicht zugelassen, oder dürfen nur in limitierter Form verwendet werden. Das Letztere war oder ist der Fall in einem der deutschen Bundesländern. Bei einer Vorführung vom Einsatz von Palantir im dortigen Bundesland, sah ich sofort mehrere Datenlücken die eine effektivere

Nutzung von Palantir einschränkten. Warum die Lücke? *„Diese Daten dürfen wir nicht verwenden“.* Solche oder ähnliche Zustände waren allen Berichten zufolge auch beim geplanten Angriff auf das Taylor Swift Konzert erkennbar. Die Polizei erhielt den eigentlichen Hinweis auf die geplante Terroraktion von amerikanischen Sicherheitsdiensten, deren Befugnisse weniger eingeschränkt sind.

Ein weiteres Hindernis bei der effektiven Bekämpfung von Terrorismus und schwerer Kriminalität, ist die ausufernde Bürokratie. Was aber ist Bürokratie, und wie weiß man wenn man es mit ihr zu tun hat?

In dem chilenischen Humorheft CONDORITO, fragte ein Mädchen einen Buben wie man wissen kann wenn man in einer Bürokratie ist. Die Antwort: *Wenn alle guten Vorschläge abgelehnt werden.*

Dazu der ständige Verweis auf Vorschriften, Regeln oder Gesetze, die in außergewöhnlichen Situationen kontraproduktiv sein würden, und auch Menschenleben kosten könnten.

Ein kleines Beispiel das ich persönlich von dem Leiter einer Observationsgruppe eines US Dienstes erfuhr, zeigt daß die Bürokratie in nationalen Sicherheitsdiensten lebt oder floriert. Die Observationsgruppe hatte den Auftrag eine sehr wichtige Person im Bezug auf die nationale Sicherheit zu beobachten. Die Gruppe positionierte sich deshalb in der Nähe des Hauses in dem diese Person wohnte, um sie dann beim Verlassen des Hauses mobil weiter zu observieren.

Zwei Wochen lang rührte sich nichts. Niemand kam, niemand ging, und man hörte auch nichts. Der Observationsgruppenleiter schlug dann vor, einfach mal die Mülleimer vor dem Haus zu

BÜROKRATIE BEIM STAAT

durchsuchen, um auf Grund des Inhaltes vielleicht einen besseren Überblick über die Lage zu bekommen.

Diese vorgeschlagene Mülldurchsuchung wurde von oberer Ebene abgelehnt. Die Dienstvorschriften und das Gesetz würden es nicht zulassen. Die leitende Person dieser Observationsgruppe ignorierte die Absage, und die Gruppe durchsuchte dann die Mülleimer. Was sie darin fanden machte es dann offensichtlich, daß die Zielperson gar nicht mehr dort war oder wohnte.

Es wäre interessant mal zu überlegen, wieviele Monate oder Jahre die Gruppe ohne diese Entscheidung noch dort gewesen wäre. Der Irrsinn bei diesem nicht weiter erwähnten Sicherheitsdienst scheint bis aus Kleinste verbreitet zu sein. So mussten Beamte auch nach mehr als einem Jahrzehnt seit der Einführung von E-mail, ihre Schreiben über den normalen Postverkehr an die anderen Dienststellen schicken. Auf dienstlichen Visitenkarten stand keine E-Mail Anschrift und auch keine Webseitenadresse. Zur selben Zeit waren andere nationalen Sicherheitsdienste fortschrittlicher und E-Mail Kontakt gehörte zur Tagesordnung.

Beim rückständigen Sicherheitsdienst war auch festgelegt, daß je nach Dokument oder Schreiben, eine andere Papierfarbe benützt werden mußte.

Schickt der Beamte ein Schreiben in der falschen Farbe per Schneckenpost an das regionale Hauptquartier, so läuft das Dokument dort zuerst durch verschiedene Instanzen, bis es beim Endempfänger angekommen ist. Dann wird es wegen der falschen Farbe zurückgeschickt. Aus eigener Erfahrung, dauert der ganze Ablauf, vom ursprünglichen Abschicken an das

Hauptquartier, bis zum Wiedererhalt der Anweisung (über den Postweg) das Schreiben auf dem richtigen Papier zu verfassen, 20 bis 30 Tage.

Auch auf bundesstaatlicher Ebene ist die Bürokratie ebenso weit verbreitet. Besonders bei den Einstellungspraktiken wird die Vernunft manchmal außer Acht gelassen. Die Überprüfung von Bewerbern unterliegt z. B. gesetzlichen und auch dienstlichen Vorschriften. (Das ist auch in Deutschland der Fall)

So wird im Auswahlverfahren bei Bewerbern für akademische Stellen an manchen staatlichen Universitäten, genau festgelegt was man fragen darf und welche Kontakte des Bewerbers man anschreiben kann.

Andere Informationsquellen, wie z.B. das Internet, sind verboten. Dabei kann es dann vorkommen daß mehrere oder verschiedene Medien über kriminelle Vorfälle, dubiose Machenschaften, und Skandale über den Bewerber berichten. Diese Informationen darf man in dem Einstellungsverfahren weder erwähnen noch irgendwie dokumentieren. Die möglichen Auswirkungen kann man sich erdenken.

Mit der fortschreitenden K.I., die inzwischen bei Bewerbungen beim Staat und auch auf privater Ebene angewendet wird, wird es immer schwieriger die relative Angemessenheit der Methoden zu beurteilen.

Dazu sind die möglichen Nutzungsbereiche von K.I. nur durch die eigene Kreativität begrenzt. Manchmal kommt man aber einfach nicht auf den Gedanken mal etwas über K.I. nachzufragen.

WEITERES ÜBER K.I....

Das Resultat bei der Anforderung an K.I. gestützte Anwendungen, richtet sich nach der Genauigkeit der Anfrage. Je detaillierter die Anfrage die man eingibt, desto eher widerspiegelt das Result den erwarteten Ausgang.

Unten ein Beispiel einer einfachen Anfrage (auf Englisch) einen Elefanten mit Polizeimütze zu zeigen:



Der obere Elefant hatte aber nicht die gewünschte Erscheinung. Deshalb wurde nachgehakt mit "Ich möchte daß der Elefant echt aussieht."



Dieses zweite Bild war genau das Erwünschte.

Mit jeder Antwort von KI kommt die Anweisung, daß wenn man mit dem Bild oder dem Resultat nicht zufrieden ist, man die Anfrage mit zusätzlichen Angaben oder Beschreibungen wiederholen kann.



DATENHACKER

(Bild: Anfrage über ChatGPT)

HACKERGRUPPE USDoD

Im April 2024 behauptete die Hackergruppe USDoD, sie habe 2,9 Milliarden persönliche Datensätze von NationalPublicData.com gestohlen, einem Unternehmen, das sich auf das Sammeln und Aggregieren öffentlicher Datensätze spezialisiert hat.

Diese Datensätze sind nun im Dark Web aufgetaucht und viele von ihnen sind authentisch. Dieser Datendiebstahl, zählt „soweit“ als einer der größten in der Geschichte, und hat sensible persönliche Informationen von zig Millionen Menschen kompromittiert. Aufgrund dessen gibt es weit verbreitetes Bedenken über den fortschreitenden oder potenziellen Identitätsdiebstahl.

NationalPublicData.com ist aber nur eine von vielen Datenbanken mit höchst persönlichen Informationen. Die Hackerangriffe erstrecken sich auf alle privaten und staatliche Bereiche, und man sollte davon ausgehen, daß alle Datenbanken gehackt werden, man weiß nur nicht wann.

NPD BREACH (HACK)

Nach dem letzten Hack kann man über die <https://npdbreach.com/> Webseite überprüfen ob man selbst betroffen ist.

Unten eine eigene Recherche

Search the National Public Data Breach
Were you affected?

First Name: HARALD | Last Name: SCHWEIZER | ZIP code: 93614

OR

Social Security Number (SSN)

OR

Phone Number

SEARCH

1 Result Found

Name	Address	ZIP Code	SSN	Phone
HARALD SCHWEIZER	Redacted	93614	Redacted	Redacted

Result Logs

Oh weh, ich bin davon betroffen

Als Gegenmaßnahme kann oder soll man bei Banken und Kredit-Debitkarten bei Zahlungsaktivitäten eine sofortige Benachrichtigungen erfordern. Um einen Identitätsbetrug zu unterbinden, kann man in den USA auch jegliche Kreditanfragen sperren. Das erschwert eine Kreditaufnahme im eigenen Namen durch Unberechtigte. Dazu sollte man auch öfters die Kennwörter bei Bankkarten- und Kontos ändern.

Internetbetrug kann man an das FBI melden (<https://www.ic3.gov/>). Bei einem eigenen Vorfall den ich dort anzeigte, verlief alles im Sand. Keine Rückfrage, keine Benachrichtigung über Ermittlungsergebnisse...garnichts. Dies ist aber bei der Masse an Vorfällen gut zu Verstehen.

Übersicht der Anzeigen mit Verlusten



<https://www.ic3.gov/>

Weitere Auskünfte über Cyberkriminalität auf <https://www.fbi.gov/investigate/cyber>



<https://www.policeapp.com/>

Interessenten am Polizeiberuf in den USA können sich mit dieser Anwendung (APP) über Stellenangebote, bevorstehende schriftliche- und Sportprüfungen, und allgemeine Einstellungsbedingungen informieren.

Die APP zeigt zudem die Prüfungstermine der verschiedenen Polizeien oder regionalen Prüfungszentren. Dabei sind Polizei oder ähnliche Vollzugsbehörden in allen Bundesstaaten repräsentiert.

<https://www.policeapp.com/Police-Departments/>

Nationale Polizeivollzugs- oder Ermittlungsdienste wie z.B. das FBI, USSS, HSI, ATF, usw. sind nicht aufgeführt.

SICHERHEITSFIRMEN IN EKUADOR



Kompromittierter Staat

In Ecuador ist die Zahl privater Sicherheitsfirmen mit der Zunahme der Kriminalität gestiegen, doch mehrende Hinweise auf eine kriminelle Unterwanderung der Branche deuten darauf hin, dass sie ebenso Kriminellen wie dem privaten Sektor und der Regierung dient

Mit der steigenden Kriminalität sind private Sicherheitsunternehmen zu wichtigen Partner der Regierung im Kampf gegen die organisierte Kriminalität geworden. Um deren Arbeit zu erleichtern, wurden die Waffengesetze geändert um ihre Schutzaufgaben effektiver zu machen, und die Polizei besser unterstützen zu können. Neue Sicherheitsunternehmen beteiligen sich an dieser neuen Einkommensquelle und die erweiterten Befugnisse solcher Unternehmen eröffneten der organisierten Kriminalität einen idealen Weg, unter einem legalen Deckmantel, ihre eigenen bewaffneten Sicherheitsunternehmen zu gründen, oder bestehende zu unterwandern.

Dadurch können ihre „Mitarbeiter“ nicht wegen illegalem Waffenbesitz angeklagt werden, und während der Transportierung von Kokain und anderen Drogen, bleiben sie als Sicherheitsunternehmen bei Polizeikontrollen weitgehend unbehelligt.

Ein Beispiel ist der jüngste Fall von Carlos Joel G.C., alias „Carlitos“, einem Drogenhändler aus Guayaquil, der laut dem Innenministerium eine der

„größten und ausgeklügeltsten Organisationen“ des Landes leitete. Carlitos nutzte eine Flotte gepanzerter Fahrzeuge, um Kokain zu Garnelenfarmen rund um die zahlreichen Flussmündungen Guayaquils zu transportieren. Von dort transportierten Schnellboote die Drogen, oft in Mengen von mehreren Tonnen, zu Frachtschiffen rund um die Hafenterminals der Stadt.

Ein entscheidender Aspekt dieser Operation, so die Behörden, waren Carlitos' legal registrierte private Sicherheitsfirmen, die es ihm ermöglichten, seine Operationen unbemerkt vom Radar der Behörden durchzuführen.



Mit Schrotflinte bewaffneter Sicherheitsmann vor einem Restaurant in Guayaquil. (in den 80er Jahren aufgenommen)

<https://insightcrime.org/news/ecuador-criminals-taking-advantage-private-security-firms/>

Nachrichten aus Nordkorea

DAILY NK

Anmerkung: Alle Artikel werden mit Genehmigung von Daily NK von Dr. Schweizer auf Deutsch übersetzt. Die deutsche Version ist meist eine verkürzte Zusammenfassung des Originals, mit eigenen zusätzlichen Bemerkungen für die Rundbriefleser. Bei manchen Artikel in Daily-NK wird kein Autor angegeben, da Anonymität zur Eigensicherung beiträgt.



Quelle: Daily NK

Kims allsehendes Auge: Der 100-Millionen-Dollar-Spionagekomplex verändert Nordkorea

Mun Dong Hui

In einem umfassenden Schritt zur Stärkung der Regimesicherheit verdoppelt das nordkoreanische Ministerium für Staatssicherheit seine Auslandseinsätze und erweitert die Überwachung im Inland um 50 %, unterstützt durch eine neue Hightech-Einrichtung im Wert von 100 Millionen US-Dollar.

Eine anonyme Quelle in Pjöngjang sagte gegenüber Daily NK kürzlich, dass die Erweiterungsbemühungen einem Befehl von Machthaber Kim Jong Un folgten, der „die Bedeutung der Sammlung, Analyse und Zusammenstellung von

Geheimdienstinformationen aus dem In- und Ausland betonte“.

Nordkorea scheint die Absicht zu haben, das Ministerium für Staatssicherheit zu erweitern, um die Stabilität des Regimes durch hartes Vorgehen gegen interne und externe Bedrohungen zu festigen.

Nach Kims Erweiterungsbefehl verdoppelte sich das Auslands Spionageabwehrbüro des Ministeriums, während das Team für die Spionageabwehr im Inland um 50 % wuchs. Als Reaktion auf die zunehmenden Bedrohungen des Kommunikationsnetzwerks des Landes wurde dem Kommunikationsbüro des Ministeriums eine neue Abteilung für das Management der Kommunikationssicherheit unterstellt.

„Die Behörden werden in der Zweigstelle Sicherheits- und Datentechnologie und -ausrüstung einsetzen, die die des israelischen Mossad oder der amerikanischen CIA übertrifft“, behauptete die Quelle.

„Im Gebäude planen sie, Gesichts- und Fingerabdruckerkennungssysteme, Kartenleser für den Eingang und intelligente Videoüberwachungsgeräte zu installieren, während sie außerhalb des Gebäudes elektronische Zäune und Wände sowie Herzschlagdetektoren aufstellen wollen.“

<https://www.dailynk.com/english/kims-all-seeing-eye-the-100-million-spy-complex-reshaping-n-korea/>

Daily NK arbeitet mit einem Netzwerk von Quellen zusammen, die in Nordkorea, China und anderswo leben. Ihre Identität bleibt aus Sicherheitsgründen anonym. Weitere Informationen über Daily NKs Netzwerk von Berichtspartnern und Informationsbeschaffungsaktivitäten finden Sie hier auf unserer FAQ-Seite.

<https://www.dailynk.com/english/faq/>