

Wie Ex-CIA, MI5 und Mossad an Israels Völkermord profitieren

Das Transkript gibt möglicherweise aufgrund der Tonqualität oder anderer Faktoren den ursprünglichen Inhalt nicht wortgenau wieder.

Dimitri Lascaris (DL): Wenden wir uns nun der Milipol-Konferenz für innere Sicherheit zu. Mir gefällt, dass man der Veranstaltung diesen Namen gegeben hat, der noch aus der Bush-Ära stammt: Homeland Security (Heimatschutz). Die Messe fand vom 16. bis 19. November in Paris statt. Hier sehen Sie die Website der Milipol-Messe. Sie versteht sich als führende Veranstaltung für Heimatschutz und Sicherheit. Sie wird alle zwei Jahre unter der Schirmherrschaft des französischen Innenministeriums in Zusammenarbeit mit mehreren nationalen und internationalen Institutionen und Regierungsbehörden organisiert. Im Jahr 2023, als sie zum letzten Mal vor der Veranstaltung in diesem Monat stattfand, versammelten sich auf der Veranstaltung über 1100 Aussteller und über 30.000 Besucher. Rami, warum erzählen Sie uns nicht einfach, wie Sie davon erfahren haben und wie Sie teilnehmen konnten? War dies schwierig oder stand die Veranstaltung grundsätzlich jedem offen?

Rami Yahia (RY): Dimitri, ich ging hier in meiner Wohnung einfach meinen eigenen Angelegenheiten nach. Da sah ich einen Beitrag auf Instagram, in dem im Grunde genommen über dieses Ereignis in Frankreich berichtet wurde. Milipol, ich glaube, es war in den sozialen Medien, vielleicht war es ein Reel von Al Jazeera. Ursprünglich verbot Frankreich allen israelischen Unternehmen die Teilnahme an seinen Militärmessen, richtig? Vor einigen Monaten wurde Elbit Systems der Zugang zu dieser großen Militärkonferenz verwehrt. Und dann hat Frankreich in letzter Minute doch israelischen Unternehmen die Teilnahme an dieser Milipol-Messe erlaubt. Die Begründung dafür war, dass es einen Waffenstillstand in Gaza gibt. Ich meine, jetzt ist es doch fair, nicht wahr? Wir haben ein neues Kapitel aufgeschlagen. Der Völkermord ist laut der französischen Regierung angeblich vorbei, und jetzt können diese Unternehmen wieder teilnehmen. Es wirkt so, als ob Israels Verbrechen nur während des Krieges gelten würden. Erstens geht der Völkermord immer noch weiter, aber kaum gibt es einen fiktiven Waffenstillstand, ist alles wieder normal. Und es gibt auch keine Rechenschaftspflicht. Frankreich sagt also kurzerhand, dass Israel zwar Gräueltaten begangen haben mag, aber angesichts des Waffenstillstands könnten diese Unternehmen wieder problemlos teilnehmen und weiterhin ihre kampferprobten Waffen verkaufen. So bewerben

diese israelischen Unternehmen ihre Waffen. Es gab viele Leute, die sich die israelischen Stände ansahen, weil Israel im Gegensatz zu anderen Ländern tatsächlich Daten vorliegen hat. Dimitri, der erste Stand, den ich besuchte, war der eines lettischen Unternehmens. Sie stellten diese kleinen unbemannten Fahrzeuge her, die dazu dienen, Fracht an die Front zu bringen oder verwundete Soldaten von der Front zu evakuieren. Am Ende fragte ich diesen Mann: „Wird das irgendwo eingesetzt?“ Er antwortete: „Ja, wir haben sechs Divisionen, die unser unbemanntes Fahrzeug in der Ukraine einsetzen.“ Ich fragte: „Wie ist das Feedback? Was sagen die sechs Einheiten?“ Er meinte: „Als wir unseren ersten Testlauf mit dieser einen ukrainischen Einheit durchgeführt haben, sagten sie, unser Fahrzeug sei schrecklich.“ Ich erwiderte: „Oh, das ist ja schlimm.“ Er antwortete: „Ja, aber dann konnten wir diese Daten nutzen, um das Feedback der ukrainischen Soldaten umzusetzen, eine aktualisierte Version herausbringen und unsere Fahrzeuge weiter verbessern. Jetzt wird es von sechs weiteren Einheiten eingesetzt.“ Der Kampfeinsatz von Waffen, Dimitri, liefert also eine unglaubliche Menge an Daten, mit denen man seine Waffen verfeinern und dann noch effektiver exportieren kann. Es macht also durchaus Sinn, dass Israel viel Datenverkehr hat. Sie hatten zwei Jahre Zeit, Dimitri, um die Palästinenser massiv zu überwachen, jeden beliebig zu ermorden, ohne dafür zur Rechenschaft gezogen zu werden, und Waffen im Kampf zu testen, seien es Drohnen, Cybersicherheits-Tools, Raketen, Waffen, was auch immer. Wir werden später noch darüber sprechen, aber jedes einzelne Unternehmen, mit dem ich gesprochen habe, erzählte mir, wie sie ihre Waffen im Kampf getestet haben und dass sie funktionieren. Es fühlt sich also wirklich so an, als gäbe es eine Pipeline von Gaza zum Heimatschutzministerium. Wir werden später noch darüber sprechen. Und Israel und Gaza werden tatsächlich zum Labor, in dem wir testen und dann exportieren.

DL: Ja, diese Änderung der Position der französischen Regierung zur israelischen Teilnahme an der Milipol spiegelte sich vor einigen Wochen auch auf EU-Ebene wider, nachdem dieser kriminelle, betrügerische Waffenstillstand angeblich in Kraft getreten war. Kaja Kallas, die politische Vorsitzende der EU, gab bekannt, dass die EU ihr Assoziierungsabkommen mit dem völkermörderischen israelischen Staat, welches das wichtigste Instrument ist, mit dem Israel jährlich Produkte im Wert von mehreren Milliarden Dollar in die Europäische Union exportieren kann, doch nicht aussetzen werde. Der Hintergrund dafür ist, dass die EU zwei Jahre lang unter Druck stand, etwas zu unternehmen, Sanktionen gegen Israel zu verhängen, doch nichts unternahm, obwohl sie die Russische Föderation und den Iran mit Sanktionen belegt hatte, und in letzter Minute, nur wenige Wochen vor Inkrafttreten des sogenannten Waffenstillstands, kündigte sie an, bestimmte Aspekte des Assoziierungsabkommens mit Israel auszusetzen. Ich weiß nicht, ob sie das jemals getan haben. Wenn ja, dann nur für ein paar Tage. Und sobald der Waffenstillstand in Kraft trat, erklärten sie, sie hätten ihre Meinung geändert, da es nun einen Waffenstillstand gebe, und würden das Assoziierungsabkommen doch nicht aussetzen. Sie haben also während dieser ganzen Zeit nie wirklich Sanktionen gegen Israel verhängt. Übrigens, und das habe ich in dem Bericht behandelt, den wir heute Morgen veröffentlicht haben: Der Geschäftsführer von Amnesty International, der wahrscheinlich renommiertesten Menschenrechtsorganisation im Westen und einer weltweit bekannten Organisation, hat vor zwei oder drei Tagen eine Erklärung abgegeben, dass es die offizielle Position von Amnesty International ist, dass der Völkermord

nicht beendet ist, sondern weitergeht. Das sollte übrigens jedem klar sein, der aufmerksam ist, aber jetzt, da es in die breite Öffentlichkeit Eingang findet, wird die Auffassung, dass er nie beendet wurde, sondern weitergeht, allgemein akzeptiert. Diese Begründung, Rami, die das Macron-Regime vorgebracht hat, um dem völkermordenden israelischen Militär die Teilnahme an dieser Ausstellung zu ermöglichen, hat null, null Glaubwürdigkeit, überhaupt keine. Der Völkermord geht weiter, der Waffenstillstand ist bedeutungslos. Um noch einmal auf den zweiten Teil meiner Frage zurückzukommen: War diese Veranstaltung allgemein für die Öffentlichkeit zugänglich, oder brauchte man eine spezielle Akkreditierung? Wie sind Sie dort hineingekommen?

RY: Ich habe die Veranstaltung am Vortag des letzten Tages entdeckt. Ich glaube, sie begann an einem Dienstag oder Mittwoch. Ich habe mich am Donnerstag online angemeldet und war mir nicht sicher, ob meine Teilnahme sofort akzeptiert wurde. Aber dann habe ich mich am nächsten Morgen an diese Veranstaltung erinnert und dachte: Oh, okay, ich logge mich mal ein und schaue, ob ich eine Zusage bekommen habe. Ich sah, dass mein Ausweis zum Ausdrucken bereit war. Die Veranstaltung findet etwas außerhalb von Paris statt. Und Dimitri, wenn ich hier in Paris etwas gelernt habe, dann ist es, dass man, wenn man eine Veranstaltung außerhalb des inneren Rings von Paris, also außerhalb des sogenannten 75er-Bereichs, organisiert, in der Regel damit rechnet, dass es zu Protesten kommen wird. Also macht man es so weit und abgelegen wie möglich, damit die Leute nicht dazwischenfunken, richtig? Das ist ein bisschen die Begründung, warum die französische Königsfamilie nach Versailles gezogen ist. Es ist ähnlich wie wenn man sich in der Mitte des Bienenstocks befindet. Dort wird es zu heiß und man rechnet mit einer Revolte der Bienen. Die Veranstaltung fand also in Paris Nord statt, ich glaube, der Ort hieß Villepinte. Also nahm ich einen dieser interregionalen Züge. Man nennt sie RER, und ich brauchte etwa 45 Minuten, um dorthin zu gelangen. Ich hatte einen kurzen geschäftlichen Telefontermin und ich lief hin und her und bemerkte, dass an fast jedem Eingang eine Reihe von Polizeiautos stand, und ich fragte mich, ob ich verdächtig wirkte, denn, Dimitri, ich kann mich nicht hinsetzen und ein Gespräch führen, ich mache das gerade für diesen Live-Stream, aber ich laufe am Telefon immer hin und her und im Kreis, und das Telefonat dauerte 30 Minuten. Ich ging mit meiner Jacke durch die Sicherheitskontrolle, wie auch immer; ich hatte nur eine Kamera und ein Mikrofon dabei. Und ich druckte meinen Ausweis aus, es geschah wirklich nichts. Ich zögerte, ob ich einen falschen Namen verwenden sollte, aber ich entschied mich für meinen richtigen Namen, und zum Glück tat ich das, denn...

DL: Sie liefen mit einem Schild herum, auf dem „Rami Yahia“ stand?

RY: Genau. Die Sache ist die: Sobald Sie den ersten Kontrollpunkt passieren, wo Sie Ihren Ausweis ausdrucken, scannt jemand Ihren Ausweis, schaut sich Ihren Namen an und fragt Sie dann nach einem Ausweis.

DL: Wir werden Aufzeichnungen Ihrer Gespräche mit diesen Israelis, verschiedenen israelischen Cybersicherheitsunternehmen, abspielen. Als Sie mit ihnen sprachen, konnten sie daher Ihren Namen, Rami Yahia, sehen?

RY: Ja, Dimitri, und ich werde noch mehr darüber sprechen, aber sie waren überhaupt nicht misstrauisch.

DL: Das sind Cybersicherheitsexperten, die weltweit führenden Spitzel, und sie konnten nicht erkennen, dass sie mit einem Palästinenser sprachen.

RY: Dimitri, sie waren überzeugt, dass ich Israeli war.

DL: Jesus Christ.

RY: Sie waren davon überzeugt – bis zu dem Punkt, an dem ich selbst anfang, es zu glauben. Ich dachte mir: Haben meine Eltern mich angelogen?

DL: Sie sind viel zu nett, um Israeli zu sein, das muss man deutlich sagen.

RY: Und nachdem ich den ersten Kontrollpunkt passiert hatte, an dem mein Ausweis überprüft wurde, gab es dort eine kleine Begrüßungsstation, und ich stellte eine Frage, die hier in Europa extrem wichtig ist. Sie lautet: Darf ich hier auf dieser Konferenz frei filmen? Die Frau und der Mann am Schalter sahen sich an und meinten: Wir haben keine Anweisungen erhalten, die etwas anderes besagen. Ich könne gerne filmen, was ich wolle. Ich meine, Sie werden das Filmmaterial sehen. Ich habe ganz offen viele Sachen gefilmt, darunter das Innenministerium, die GIGN (Einsatzgruppe der Gendarmerie Nationale) und die französische Heimatschutzbehörde. Ich habe gefilmt und hatte keinerlei Probleme.

DL: Es ist komisch. Ich war vor ein paar Jahren in einer ähnlichen Situation – nicht in Frankreich, sondern in Katar. Genau wie Sie habe ich während meines dreitägigen Aufenthalts dort in letzter Minute von einer großen Waffenausstellung erfahren. Ich bin am letzten Tag hingegangen. Ich war überrascht, dass sie mich zugelassen haben. Und noch überraschender war, dass ich stundenlang herumlaufen und alles filmen durfte, einschließlich meiner Gespräche mit Leuten und, wie Sie wissen, hochrangigen Würdenträgern und Generälen, die dort waren. Sobald man einmal hineingekommen ist, ist es überraschend offen, aber hineinzukommen kann schwierig sein. Schauen wir uns also das Video an. Ich glaube, das ist das Video, das wir gleich zeigen werden, als Sie mehr oder weniger reinkamen. Erklären Sie uns doch bitte, was wir da sehen, während wir es uns ansehen.

Ich möchte hier kurz innehalten. Als ich das sah – man sieht oben rechts, dass die Pavillons offenbar nach Ländern geordnet sind; rechts ist also Belgien. Und vergessen wir nicht, dass es sich hier um Heimatschutz handelt. Das ist also so etwas wie innere Sicherheit. Sehen Sie sich diese Typen an. Die sehen aus wie Soldaten im Kampfeinsatz dort rechts, diese Dummies mit ihrer ganzen Ausrüstung. Ich konnte nicht sagen, ob wir auf einer Konferenz zur inneren Sicherheit oder auf einer Konferenz für einen heißen Krieg sind.

RY: Dimitri, es wird noch viel verrückter, denn es geht nicht nur um die Heimatschutzbehörde, sondern auch um private Sicherheitsdienste. Es gibt also Leute, die mit ihren eigenen privaten Sicherheitsfirmen auftreten. Ein Mann meinte, er würde sich um die Sicherheit in ein paar Kneipen und Nachtclubs kümmern. Es gibt Privatdetektive. Ich erinnere mich, dass ich vor ein paar Jahren einen Vortrag an der Concordia organisiert habe und jemand sagte, dass alle Forschungsergebnisse, die in das Militär fließen, und alle Waffen, über die das Militär verfügt, sobald sie eine Generation zu alt sind, an die Polizei und die Heimatschutzbehörde weitergegeben werden.

DL: Fahren wir fort.

RY: Dort in der Ferne sieht man rechts, etwa in der Mitte rechts, den deutschen Pavillon. Alle üblichen Verdächtigen sind dabei.

DL: Was ist das?

RY: Ich bin mir nicht ganz sicher. Aber nachdem ich ein bisschen Zeit dort verbracht habe, sehen Sie diesen kleinen Rucksack? Die drei Antennen? Ich glaube, da ich ein bisschen Zeit dort verbracht habe, weiß ich mehr, als ich sollte. Aber das sieht aus wie eine Drohnen-Störsoftware, die Radioaktivität meldet, also entweder um die von Mobiltelefonen ausgestrahlten Frequenzen zu messen oder um Radargeräte zu stören, und dieser Turm könnte eine Störsoftware oder ein Störgerät für Drohnen sein. Man hat also die Drohne, schießt sie irgendwie ab, jedenfalls hoffe ich, dass es so ist.

DL: Ich glaube, Sie haben Recht, aber ich bin kein Experte. Fahren wir fort. Dort sehen Sie den Schweizer Pavillon, das sogenannte neutrale Land. Das war also der einführende Rundgang durch das Ausstellungsgelände. Sagen Sie uns doch bitte, Rami, als Sie hereinkamen, was war Ihr Gesamteindruck von allem? Gab es etwas, das Ihnen besonders aufgefallen ist?

RY: Dimitri, ich habe schon einige Messen besucht. Die Messen, auf denen ich war, waren alle für den zivilen Gebrauch, für B2B, den Kauf von Waren, Wohnkultur, Buchmessen. Es ist dasselbe. Wirklich, es ist dasselbe, dasselbe Layout. Die Stände sind alle gleich aufgebaut, nur das Endprodukt ist unterschiedlich. Es kam mir wirklich absurd vor, denn man konnte genauso wie auf einer Buchmesse mit den Büchern, Lesezeichen und allem Möglichen herumspielen oder wie auf einer Spielzeugmesse mit den Spielsachen. Dort sind die Waffen alle ausgestellt, man kann eine in die Hand nehmen, zielen, schießen, simulieren, Spaß haben. Und es entstand wirklich dieses absurde Gefühl, dass dies eine echte Industrie ist. Es gibt Menschen, deren gesamter Arbeitsalltag sich um Tod und Zerstörung dreht.

Und ich wollte auch noch sagen, Dimitri, dass ich ziemlich linksorientiert aufgewachsen bin und über diese sogenannten bösen Polizeistaaten wie die Sowjetunion gelesen habe, die einen ständig überwachten und all diese schrecklichen Dinge, die uns durch Propaganda eingetrichtert wurden, und ich erinnere mich, dass ich dort war und dachte: Das ist eine ganz andere Ebene der Überwachung. Ich meine, sie sprechen offen darüber, dass sie Telefone

anhand ihrer Nummer verfolgen können. Im Grunde digitalisieren sie alle diese Karten, auf denen man anhand von Metadaten jederzeit verfolgen kann, wo sich Menschen befinden, so wie uns alles Mögliche über den Kommunismus erzählt wurde, Dimitri, aber was ich dort gesehen habe, war tausendmal alarmierender. Und noch etwas möchte ich erwähnen: Immer wenn ich zu diesen Ständen ging, diesen Militärständen, und wenn man sich ihre Websites ansieht, wusste ich nicht allzu viel über diese ganze Entwicklung der Smart Cities, aber es fühlt sich wirklich so an, als gäbe es eine Schnittmenge zwischen Smart Cities, Cybersicherheit und einfach der Militarisierung des Staates.

DL: Es handelt sich um ein Unternehmen namens Octopus Systems. Ich zeige Ihnen mal ein Bild von der Website dieses gruseligen Unternehmens. Bitte sehr. Sie haben eine Fusion Platform, wie sie sagen. „Octopus vereint riesige Datenströme aus verschiedenen Quellen in einer einzigen KI-gestützten Fusion Platform, der Hunderte von Organisationen aus den Bereichen Verteidigung, innere Sicherheit, kritische Infrastruktur, Smart Cities, Technologie und Finanzen vertrauen. Octopus ermöglicht intelligente Entscheidungen und Maßnahmen in Echtzeit, um proaktiv auf sich entwickelnde Bedrohungen zu reagieren.“ Für jemanden wie mich ist das alles nur Kauderwelsch. Rami, Sie sind viel technikaffiner als ich. Was bedeutet das alles? Und können Sie uns kurz erklären, was die Produkte dieses Unternehmens im Grunde sind?

RY: Ich glaube, Dimitri, Sie sind nicht der Einzige, der Schwierigkeiten hat, die Websites dieser Militärunternehmen zu verstehen. Manchmal hat man wirklich das Gefühl, dass sie absichtlich kryptisch und geheimnisvoll kommunizieren. Ich kann Ihnen beschreiben, was ich verstanden habe. Ich glaube, dieser Mann von der Firma Octopus hat seine Software als Kommando- und Kontrollzentrum beschrieben. Man hat also seine Dateneingabepunkte, sei es eine Kamera, eine Beobachtungsliste, irgendwelche Überwachungsgeräte, Audio, was auch immer man herstellen kann, alle Metadaten, die man erfassen möchte, um eine Person zu identifizieren, man gibt sie in Octopus ein und es erstellt eine Art Porträt dieser Person. Und dann könnte man diese Person mit einer Terroristen-Beobachtungsliste abgleichen, wenn man an einer Grenze ist. Nehmen wir zum Beispiel den Fall, dass jemand hier in Paris an einem Flughafen die Grenze überquert. Der Grenzbeamte hat dann schon ein Bild von Ihnen, denn wenn Sie Ihren Reisepass scannen, ist dort ein Bild von Ihnen, oder manchmal gibt es auch Kameras am Kontrollpunkt, und dann verwendet man einige Metadaten durch Octopus, wo dann ein Porträt von Ihnen erstellt wird, das mit Whitelists oder Blacklists abgeglichen werden kann. Außerdem könne er andere Datenpunkte integrieren, um Ihre Social-Media-Konten abzurufen. In dieser Aufzeichnung, die ich habe, frage ich ihn: Sogar private Konten? Und er antwortet: Ja, wir können Social-Media-Konten und Beiträge von Privatpersonen erfassen. Im Grunde genommen handelt es sich also um eine Kommando- und Kontrollzentrale. Sie haben nicht wirklich Hardware oder Geräte. Man verbindet einfach alle möglichen Geräte mit Octopus, und dann erstellt Octopus eine Art Hintergrundgeschichte zu den Daten, die sie über einen haben.

DL: Das klingt nach einem gruseligen Produkt. Lassen Sie uns doch ein wenig über dieses Unternehmen sprechen, okay? Wie sich herausstellt, ist das Unternehmen zwar israelisch,

aber – wie Sie dort auf dem Bildschirm sehen können – in 28 Ländern physisch präsent. Eines davon ist Kanada. Und laut der Website befindet sich sein Büro ganz in der Nähe meines derzeitigen Aufenthaltsortes. Es befindet sich ein paar U-Bahn-Stationen nördlich von meinem Standort in der Innenstadt von Toronto. Und in einem Artikel vom Dezember 2023 hat das unabhängige Medienunternehmen The Breach – ich glaube, wir haben ein Bild von diesem Artikel. Jedenfalls hat The Breach, das einige gute Berichte zu diesem Thema veröffentlicht hat – da haben wir es –, enthüllt, dass eine Risikokapitalgesellschaft namens Awz, die ihren Sitz hier in Toronto hat, nur zwei Blocks von meinem Standort entfernt, 5,5 Millionen Dollar in Octopus Systems investiert hat. Und da sehen Sie The Breach. Sie haben die Tatsache hervorgehoben, dass der Geschäftsführer von Awz Venture Capital der ehemalige kanadische Premierminister Stephen Harper ist, der dort links abgebildet ist. Und ich denke, man kann mit Fug und Recht sagen, Rami, ich bezweifle, dass Sie mir widersprechen werden, dass er der pro-israelischste Premierminister in der Geschichte dieses Landes ist. Und das will etwas heißen, denn sie waren so ziemlich alle fanatisch pro-israelisch. Ich möchte Ihnen nur zeigen, dass Awz wirklich etwas Außergewöhnliches ist. Ich verfolge sie schon seit einiger Zeit, ehrlich gesagt, ohne dass ich hier näher darauf eingehen werde, warum. Es hat mit rechtlichen Angelegenheiten zu tun, und dabei möchte ich es belassen. Aber ich wusste nicht, dass sie in dieses Unternehmen Octopus Systems investiert hatten. Tatsächlich wusste ich nicht einmal, dass Octopus Systems existiert, bis Rami mir davon erzählte. Und hier sind die führenden Köpfe des Managementteams. In der obersten Reihe, der dritte von links, ist Stephen Harper selbst zu sehen. Er ist Partner und Vorsitzender des Beirats dieser berühmten Risikokapitalgesellschaft. Rechts von ihm, also von uns aus gesehen, sitzt Richard Fadden, der ehemalige Direktor des CSIS, des kanadischen Sicherheitsdienstes. Das ist das kanadische Pendant zur CIA. In der zweiten Reihe, ganz links, ist James Woolsey, ehemaliger Direktor der CIA. Direkt neben ihm sitzt Tamir Pardo, ehemaliger Direktor des Mossad. Dann Buck Revell, ehemaliger stellvertretender Direktor des FBI. Richard Nesbitt, strategischer Berater für Finanzdienstleistungen. Ich glaube, Nesbitt ist so etwas wie ein Titan der kanadischen Finanzwelt. Ich bin mir ziemlich sicher, dass entweder er oder sein Vater eine der größten Investmentbanken Kanadas gegründet hat, die später von der Bank of Montreal übernommen wurde. Und dann unten in der letzten Reihe Jacob Frenkel. Der Name kommt mir bekannt vor, Rami. Er ist strategischer Berater. Wissen Sie, wer dieser Mann ist? Ich bin mir sicher, dass ich diesen Namen schon einmal gehört habe.

RY: Er sagt mir nichts.

DL: Okay. Auf jeden Fall handelt es sich hierbei um eine Art Crème de la Crème der kanadischen, amerikanischen und israelischen Sicherheitsbehörden der obersten Ebene. Diese Firma investiert also 5,5 Millionen Dollar in das Octopus-System. Hören wir uns nun Ihr Gespräch an. Es handelt sich um ein etwa sechsminütiges Gespräch...

RY: Bevor wir dazu kommen, können wir noch einmal betonen, dass die drei wichtigsten Geheimdienste der Welt in diesem strategischen Gremium vertreten sind? Wir sprechen hier vom kanadischen Geheimdienst, dem amerikanischen Geheimdienst, der CIA und dem

Mossad, die alle in dieser Investmentgruppe zusammenarbeiten und in israelische Cybersicherheitsunternehmen investieren. Ich weiß nicht, ob das nur für mich hier schockierend ist, aber diese drei Geheimdienste scheinen wirklich eng miteinander verflochten zu sein. Es gibt kein Geschäftsfeld für den Geheimdienst – ich meine, im Allgemeinen, in einem eher professionellen Sinne, würde man erwarten, dass diese Agenten wie separate Individuen agieren. Wahrscheinlich spionieren Amerikaner Kanadier aus, aber hier arbeiten die drei ehemaligen Leiter dieser Organisationen zusammen, um in israelische Cybersicherheitsunternehmen zu investieren und diese dann wahrscheinlich durch Hintertüren zurück zum kanadischen Geheimdienst, zum amerikanischen Geheimdienst und zum israelischen Geheimdienst zu bringen.

DL: Genau. Und sie arbeiten zusammen, das ist wichtig, wie auch immer, ich bin mir sicher, dass sie dafür ideologische Beweggründe haben, aber sie arbeiten zusammen, um Geld für ihre eigene Bereicherung zu verdienen. Und so handeln all diese Leute, einschließlich des ehemaligen kanadischen Premierministers, mit ihrer politischen Vergangenheit, um sich selbst zu bereichern. Ich bin mir sicher, dass Stephen Harper vor allem deshalb an der Spitze dieser lukrativen Organisation steht, weil er der pro-israelischste Premierminister in der Geschichte Kanadas war. Diese Leute unterstützen also nicht nur ein Apartheidregime oder arbeiten im Dienste eines Apartheid- und mittlerweile auch Völkermordregimes, sondern sie bereichern sich auch persönlich aufgrund ihrer Unterstützung für dieses Regime. Wie gesagt, es handelt sich um einen etwa sechsminütigen Clip. Wenn Sie zu irgendeinem Zeitpunkt während dieser Audioaufnahme möchten, dass ich unterbreche, Rami, sagen Sie mir einfach Bescheid, damit wir Ihre Erklärung hören können, denn für Menschen, die mit diesen technologischen Produkten nicht vertraut sind, ist die Terminologie ziemlich komplex. Es kann etwas schwierig sein, dem zu folgen.

RY: Was machen Sie?

Octopus Sprecher: (Octopus) Wir sind eine Plattform für Datenfusion und KI. Wir sind so etwas wie eine Konsolidierungsstelle, eine Art Kommando- und Kontrollzentrale, in der alle verschiedenen Systeme für Militär und polizeiliche Ermittlungen integriert sind. Wir integrieren alles für militärische und zivile Sicherheitssysteme, Drohnen und unbemannte Fahrzeuge (UAV). Aber wir kümmern uns auch um Polizei, UAV-Fahrzeuge, Polizeisysteme und bringen Web-Intelligence, Online-Profiling, Informationen und Cyber-Sicherheit mit ein. Wir vereinen alles in einem Befehls- und Kontrollsystem, in dem Sie ein vollständiges Ereignismanagement, Reaktions- und Ermittlungsfunktionen haben, und darüber hinaus verfügen wir über KI.

RY: An Grenzen gibt es also jemanden, der die Pässe scannt.

Octopus: Sie können den Pass scannen.

RY: Und können Sie dann eine Social-Media-Plattform verfolgen?

Octopus: Ja, das können wir. Normalerweise macht man das nicht, weil es laut Datenschutzverordnung nicht erlaubt ist. Aber wenn jemand auf einer Beobachtungsliste steht und nun verdächtig ist, dann darf man Informationen aus sozialen Medien, Telegram, Instagram und TikTok wiederverwenden.

RY: Aber haben Sie diese Informationen bereits oder rufen Sie sie bei Bedarf ab?

Octopus: Wir rufen sie bei Bedarf ab.

RY: Okay. Sie verfügen also erst dann darüber, wenn Sie sie benötigen?

Octopus: Aber wir können ihn auch anhand der Gesichtswiedererkennung mit der Beobachtungsliste abgleichen. Ja, wir integrieren auch Gesichtserkennung und Führerscheinerkennung, und wir können all diese Informationen zusammenführen, um – wir hatten hier die französische Zivilluftfahrtbehörde.

RY: Ja?

Octopus: Sie wollen unsere Plattform nutzen.

DL: Was hat er da gesagt? Die französische Zivilluftfahrt?

RY: Die französische Zivilluftfahrt.

DL: Okay, dann nutzen sie es vielleicht, um Passagiere an Flughäfen zu überprüfen, denke ich, oder wie auch immer, lassen Sie uns mit diesem Gespräch fortfahren.

Octopus: Ja, was machen Sie?

RY: Ich bin Berater für Cybersicherheit. Aber worauf ich mich derzeit hauptsächlich konzentriere, ist die Gesetzesänderung in Kanada in Bezug auf Drohnen. Früher durften sie nur innerhalb der Sichtweite geflogen werden, jetzt ist das nicht mehr der Fall.

Octopus: Die Gesetze werden geändert?

RY: Das liegt daran, dass wir in Kanada große Felder haben. Es macht also keinen Sinn, nur eine Art Rundkurs zu fliegen, um Ihre Farm, Ihr riesiges Feld zu schützen. Ohne ...

Octopus: In Israel benutzen alle, in allen Städten, die Polizei, alle taktischen Einheiten, die Notfalldienste, sie benutzen oft automatisierte Drohnen.

RY: Aber Sie haben andere Gesetze.

Octopus: Das meine ich ja.

DL: Ja, um es noch einmal zu wiederholen, falls Sie das nicht gehört haben: In Israel nutzt jeder Drohnen. Die Polizei, die Kommunen, die Regionen, einfach alle.

RY: Da es sich hinter der Sichtlinie befindet, ist es nicht erlaubt. Man muss sich innerhalb der Sichtlinie befinden.

Octopus: Ja, ich habe gehört, dass das ein Problem ist, mit dem sie konfrontiert sind, und dass es in Sichtweite sein muss. Jetzt ändern sie das.

RY: Ja, das ist richtig, ja.

Octopus: Es gibt also all diese großen israelischen Konzerne, Elbit, die israelische Luftfahrtindustrie, die alle Cyber-Schutzmaßnahmen gegen das Abfangen von Drohnen, Drohnen-Man-in-the-Middle-Angriffe und Drohnen-Störsignale entwickeln. Cyber-Drohnen sind also in Israel sehr stark vertreten. Wir integrieren. Wir integrieren also Störsender und Anti-Drohnen-Systeme, oder wir integrieren ...

RY: Sie haben doch das Kommando- und Kontrollzentrum, oder?

Octopus: Wir haben viele Drohnen.

RY: Ach wirklich?

Octopus: Ja, wir haben mehrere Gemeinden. Wir haben Militärprojekte für taktische Kampffzüge, wo wir auch anwendungsbezogene Tablets einsetzen. Wir sind also für die Befehls- und Kontrollfunktion zuständig.

RY: Und die israelische Armee nutzt das?

Octopus: Ja, ja, nicht nur Israel. Wir sind auch in Afrika vertreten. Auch in Asien. Wir haben Thailand; die thailändische Polizei ist unser Kunde. Wir haben die Präsidentenschutzabteilung. Sie nutzen die Kommandodrohnen, Gesichtserkennung, Personal, Schutz, Perimeter, Sicherheit, um das Königreich und den Premierminister, den Regierungspalast zu schützen.

RY: Wie viel kostet ein solches System?

Octopus: Sie sind nicht billig.

RY: Und das liegt außerhalb meiner Preisklasse, oder?

Octopus: Ab zwölf-, fünfzehntausend Dollar pro Monat, vor den anfänglichen Einrichtungskosten für die Installation und Integration.

RY: Wenn man will, dass es gut funktioniert, muss man eben dafür bezahlen.

Octopus: Wie bitte? Wir sprechen hier von großen Organisationen. Aus Frankreich hatten wir die Zivilluftfahrt, wir hatten das Ministerium für innere Sicherheit hier, die es für ihre Kontrollzentren in Betracht gezogen haben.

RY: Reaktion?

Octopus: Reaktion und Kontrolle. Wer war noch hier? Wir arbeiten auch an kritischen Infrastrukturen. Wir kümmern uns um den Schutz der Seeschifffahrt, integrieren uns in Radarsysteme, in die Marine.

RY: Ist es ein großes Unternehmen?

Octopus: Unser Unternehmen hat 50 Mitarbeiter, es ist also ziemlich klein. Alle sind Ingenieure, alle sind Softwareentwickler. Wir sind in Großbritannien, in Singapur und in Mexiko vertreten. Im Bereich Engineering sind wir 50, wir haben wahrscheinlich noch weitere – oh, aber im Moment arbeiten wir mit Partnern zusammen, großen Partnern. Wir sind Teil einer größeren Lösung. Wir arbeiten nicht alleine.

RY: Ja, natürlich, natürlich.

Octopus: Wir konkurrieren mit Thales. Wir könnten also Teil des Kommando- und Kontrollsystems von Thales sein, und obwohl wir mit Thales und Palantir konkurrieren – den Giganten.

DL: Okay, sie konkurrieren also mit Palantir. Wer ist Thales?

RY: Thales ist ein sehr großes französisches Militärunternehmen. Ich weiß nicht allzu viel über sie, aber seit ich den Namen Thales gehört habe, sind mir diese Muster aufgefallen. Aber Dimitri, er erwähnte das französische Innenministerium, die französische Zivilluftfahrtbehörde und die thailändische Polizei – für Israelis ist es wieder einmal nur Afrika. Er sagte also, dass Afrikaner dieses Tool nutzen, und natürlich auch die israelische Regierung.

DL: Er erwähnte auch Mexiko.

RY: Monaco?

DL: Mexiko. Nein, er sagte Mexiko und Großbritannien. Was zum Teufel macht Mexiko? Es hat angeblich eine linke Regierung und erlaubt diesen Widerlingen, ihre Cybersicherheits-KI-Sachen zu verkaufen. Entschuldigung, fahren Sie fort.

RY: Dimitri, Sie haben vorhin gesagt, dass sie Niederlassungen in 28 Ländern haben. Sie sind doch nur in drei Ländern registriert, oder? Sie sind natürlich in Israel registriert, aber in gewisser Weise befindet sich der Hauptsitz tatsächlich in Kanada. Laut The Breach besitzt die kanadische Niederlassung also zwei Drittel des Unternehmens. Es handelt sich also um ein israelisch-kanadisches Gemeinschaftsunternehmen, das der israelischen Regierung Software zur Begehung von Kriegsverbrechen zur Verfügung stellt und seine Produkte nach Mexiko und Großbritannien auslagert. Anscheinend arbeiten sie an einem Vertrag mit dem französischen Innenministerium – hoffentlich wird dies mit der Veröffentlichung dieses Videos nicht mehr der Fall sein –, mit der französischen Zivilluftfahrtbehörde, der thailändischen Polizei und natürlich mit afrikanischen Regierungen. Das sagt zumindest der Mann.

DL: Richtig. Okay. Hören wir uns also das Ende an, das besonders interessant ist.

RY: Halten Sie noch einmal an. Auch hier bin ich wieder völlig verwirrt. Ich bin völlig verwirrt, warum dieser Mann mir das alles erzählt.

DL: Ja, dazu kommen wir noch. Beenden wir die Aufnahme und informieren die Leute über das Geschehene. Okay, hören wir uns einfach den Rest an.

Octopus: Sie sind also Berater für Cyber?

RY: Aber kleinere Projekte, kleinere Projekte. Das ist wirklich nicht annähernd so groß.

Octopus: Ja, wir haben eine registrierte Firma in Kanada. Wir haben eine amerikanische Firma.

RY: Und warum Kanada?

Octopus: Unsere Investoren sind Kanadier.

RY: Kennen Sie Montreal?

Octopus: Natürlich. Sehr schön.

RY: Und sie möchten in ein kanadisches Büro investieren?

Octopus: Ja, als jüdischer Investor. Einige der größten Milliardäre Kanadas sind Juden und sie sind Protagonisten in der Verteidigungstechnologie, richtig?

DL: Moment mal, was? Einige der größten Milliardäre Kanadas sind Juden und sie investieren in Verteidigungstechnologie. Wow. Dieser Mann ist unglaublich. Ich glaube, das ist das zweite oder dritte Mal, dass er Sie gefragt hat, wer Sie sind. Er ist also eindeutig neugierig, aber er fährt einfach fort. Hören wir uns also die letzten Sekunden davon an.

Octopus: Ja, wir arbeiten auch mit Banken zusammen. Wir haben übrigens viele Projekte für Kanada durchgeführt. Wir haben die CIBC Bank und die Canadian NBO Bank betreut. Wir haben die Polizei von York außerhalb von Toronto unterstützt.

DL: Die Polizei von York, CIBC, eine der zwei oder drei größten Banken Kanadas.

Octopus: Die Polizei, ja.

RY: Und wie haben sie Sie gefunden?

Octopus: Wir arbeiten einfach mit Partnern auf der ganzen Welt zusammen. Und wir finden sie. Auch mit Air Canada haben wir gearbeitet.

DL: Air Canada, die größte Fluggesellschaft Kanadas.

Octopus: Mississauga.

DL: Die viert- oder fünftgrößte Stadt Kanadas.

Octopus: Mit Strom von AltaLink aus Calgary.

DL: Der größte regulierte Energieversorger in Alberta, wo Stephen Harper herkommt.

Octopus: AltaLink. Das ist ein lokaler Stromversorger in Calgary.

RY: Okay. Ja, denn in Quebec haben wir nur einen Stromversorger.

Octopus: Wir haben dort ein neues kommerzielles Projekt namens „The Well“ durchgeführt, sehr schick in Toronto.

DL: Haben Sie verstanden, was er gesagt hat? Ein großes, schickes kommerzielles Projekt? „The Well“? Wissen Sie, was er gesagt hat?

RY: Es heißt „The Well“.

DL: Also so etwas wie ein großes Einkaufszentrum? Was ist das? Wissen Sie das?

RY: „The Well Toronto“. Es sieht aus wie ein Einkaufszentrum.

DL: Okay.

Octopus: Die jüdischen Gemeinden.

DL: Er sagt, dass die jüdischen Gemeinden – er hat nicht gesagt, welche – ihre Technologie nutzen.

Octopus: Die größten Telekommunikationsunternehmen.

RY: Es war mir ein Vergnügen.

Octopus: Genießen Sie Ihre Zeit.

RY: Ja, bis bald.

DL: Ja, also Rami, erzählen Sie uns jetzt, was passiert ist? Wie ist dieses Gespräch zu Ende gegangen? Es ist nicht auf der Aufnahme, aber wie ist es zu Ende gegangen?

RY: Die Aufnahmen wurden zusammengeschnitten, sie wurden gekürzt. Ich habe den Redakteuren keine richtigen Anweisungen gegeben, sie haben die wichtigsten Stellen herausgeschnitten, Dimitri. Aber wir lieben unsere Redakteure. Aber im Grunde genommen sagt er, dass viele jüdische Organisationen, jüdische Gemeindezentren in Kanada ihre Software verwenden, und dann hält er inne und fragt mich, ob ich Jude bin. Und dann überlege ich – das alles passiert übrigens in einer Viertelsekunde, aber in meinem Kopf

vergeht die Zeit so langsam, und ich rechne und überlege und denke: Soll ich sagen, dass ich Palästinenser bin? Soll ich die Nationalität meiner Mutter angeben? Sie stammt aus dem Libanon. Oder soll ich sagen, dass ich Jude bin? Denn der Mann geht einfach davon aus, dass ich Jude bin, und die ganze Zeit denke ich: Ich habe Angst, in einem Netz aus Lügen gefangen zu sein. Wenn ich sage, dass ich Jude bin, und er mir dann von einem Feiertag erzählt, der nächste Woche stattfindet und von dem ich keine Ahnung habe, dann würde ich in einem Netz aus Lügen gefangen sein. Also sagte ich: Nein, ich bin Libanese. Denn wenn ich gesagt hätte, ich sei Palästinenser, Dimitri... Also sagte ich, ich sei Libanese, und alles, was er daraufhin sagte, war: „Viele Libanesen sind in Afrika finanziell gut gestellt.“ Dann hörte er einfach auf zu reden, und innerhalb von zwei Minuten ging ich. Ja, ich konnte also nicht herausfinden, welche jüdischen Gemeindezentren seine Software verwendeten. Und das war das letzte wertvolle Stück Information, das er uns gab.

DL: Es ist wieder einmal erstaunlich, ich komme auf das zurück, was ich zu Beginn gesagt habe: Diese Menschen sollen Sicherheitsexperten von Weltklasse sein. Man würde meinen, wenn er sich Gedanken darüber gemacht hätte, ob Sie jüdisch sind oder nicht, hätte er das zu Beginn geklärt, bevor er anfing, zu plaudern und Ihnen all diese Informationen mitzuteilen. Aber hey, was weiß ich schon? Ich bin kein Sicherheitsexperte.

RY: Eine weitere Aufnahme, zu der wir noch kommen werden, beginnt später in der Aufzeichnung. Ich habe beschlossen, diesen Teil herauszuschneiden, aber er sagt: Rami Yahia, das ist ein jüdischer Name. Rami stammt vom Wortstamm für Gesundheit oder etwas in dieser Richtung im Hebräischen. Und dann Yahia – ich weiß, dass Yahia ein Prophet im Islam ist und es ist das arabische Wort für, ich glaube, den Propheten Johannes.

DL: Richtig.

RY: Aber diese Leute gingen tatsächlich davon aus – sie meinten: „Es gibt Menschen in Israel mit dem Namen Rami Yahia, und die sind Juden.“ Ich glaube also, er ging tatsächlich davon aus, dass ich Jude und kein Palästinenser bin, denn warum sollte ein Palästinenser zu einem israelischen Stand gehen?

DL: Das wäre mir nie in den Sinn gekommen. Bevor wir zum nächsten Unternehmen übergehen, zeigen wir Folgendes. Das ist ein Foto, das Sie im israelischen Pavillon aufgenommen haben. Oh, ich muss den YouTube-Share-Bildschirm schließen.

DL: Folgendes hatten sie. Und ich finde es einfach unglaublich, dass die französische Regierung so etwas zulässt. Sie bewerben offen israelische Militärausrüstung, während Israel einen Völkermord begeht. Wow. Okay, kommen wir zum nächsten Unternehmen. Sie wollten etwas sagen, Rami. Möchten Sie noch etwas hinzufügen, bevor wir das Thema Octopus verlassen?

RY: Ich wollte nur sagen, dass The Breach einen Artikel über Octopus geschrieben hat. Wir haben kurz darüber gesprochen. Er wurde von Anas Ambri veröffentlicht.

DL: Da ist der Artikel auf dem Bildschirm.

RY: Und sie berichteten darüber, wie Octopus in Gaza getestet wird, um es dann in die griechischen Flüchtlingslager zu exportieren, um dort die Syrer und Palästinenser in diesen Flüchtlingslagern zu überwachen, und anschließend wird diese Software, wenn sie getestet und exportbereit ist, auf der Milipol für die Heimatschutzbehörde vorgestellt. Es gibt also eine Verbindung von Gaza über europäische Flüchtlingslager zu einer Stadt in Ihrer Nähe oder zur Heimatschutzbehörde, um sie dann gegen unsere eigene Bevölkerung einzusetzen. Ich finde diesen ergänzenden Bericht von The Breach, der schon lange vor uns veröffentlicht wurde, wirklich gut. Ich glaube, das war im Januar 2025. Er ist sehr aufschlussreich, und ich bin Anas Ambri sehr dankbar dafür. Ich habe mit ihm gesprochen und werde ihn morgen anrufen, damit wir dieser Sache vielleicht auf den Grund gehen können.

DL: Sie sollten Ihre Erkenntnisse auf jeden Fall mit Anas teilen. Aber auch hier haben Sie vollkommen Recht. Wie wir bei Reason2Resist so oft sagen, wird unsere Unterstützung für dieses mörderische Regime auf uns zurückfallen. Und das tut es bereits auf viele, viele verschiedene Arten. Kommen wir also zum nächsten Unternehmen, auf das Sie im israelischen Pavillon gestoßen sind. Es handelt sich um ein Unternehmen namens CoreSite. Ich zeige Ihnen kurz ein Bild von dessen Website. Da ist es: „Die versteckten Kosten von übersehenen Echtzeit-Bedrohungen. Wichtige Informationen bleiben in Standard-Videoaufnahmen oft unbemerkt und gefährden Besucher und Mitarbeiter. Unsere Gesichtserkennungstechnologie ermöglicht es Sicherheitsteams, entschlossen zu handeln.“ Check: Identifizieren Sie Personen auf Beobachtungslisten. Check: Markieren Sie unbefugten Zugang zu Sperrbereichen. Check: Muster von Ladendiebstahl, Einbruch und Betrug erkennen. Und dann sehen Sie rechts ein Werbevideo, in dem gezeigt wird, wie die Gesichtserkennungstechnologie funktioniert. Auf seiner Website wirbt CoreSite intensiv für ein Produkt namens API. Es wird wie folgt beschrieben: „API von CoreSite ist eine fortschrittliche Gesichtserkennungslösung, die selbst in den anspruchsvollsten Umgebungen branchenführende Genauigkeit bietet. Die API-Technologie von CoreSite bietet leistungsstarke Erkennungsfunktionen bei extrem schlechten Lichtverhältnissen, Bildern von geringer Qualität sowie schwierigen Blickwinkeln und teilweise verdeckten Gesichtern. Darüber hinaus ermöglicht die signaturbasierte Technologie von CoreSite die Gesichtserkennung, ohne dass sensible Daten wie Gesichtsbilder gespeichert werden müssen.“ Hören Sie sich das an: „Auf diese Weise werden Innovation und Effizienz mit dem Datenschutz in Einklang gebracht, um den regionalen politischen Vorschriften zu entsprechen.“ Das klingt für mich – als Anwalt – so, als hätten sie einen Weg gefunden, Datenschutzgesetze zu umgehen und ihre Gesichtserkennungstechnologie zu verbessern, um ihren Kunden zu helfen, Gesichter in schwierigen Umgebungen zu identifizieren, ohne sogenannte sensible Daten zu speichern. Sie umgehen also – so verstehe ich das – sie umgehen Datenschutzgesetze. Nicht unbedingt auf illegale Weise, sondern sie haben einfach eine Gesetzeslücke gefunden und nutzen diese aus.

Nun möchte ich Ihnen zeigen, dass zum Management von CoreSite eine Person namens Tony Porter gehört, die mir aufgefallen ist. Es handelt sich um ein israelisches Unternehmen, aber

Porter ist der Datenschutzbeauftragte. Er ist also derjenige, der dem Unternehmen dabei hilft, Datenschutzgesetze zu umgehen oder Schlupflöcher zu finden. Tony wurde 2014 vom britischen Innenminister zum Beauftragten für Überwachungskameras ernannt. Er war also Regierungsbeamter und übte diese Funktion sieben Jahre lang aus. Er entwickelte die nationale Strategie für Überwachungskameras, legte eine Reihe von Überwachungsstandards fest und erstellte Leitlinien für die Strafverfolgungsbehörden zum rechtmäßigen und ethischen Einsatz von Gesichtserkennungssystemen. Er verfügt über Fachkenntnisse sowohl im Bereich Wirtschaft als auch Strafverfolgung. Er ist ein Geheimdienstspezialist mit Erfahrung in den Bereichen Community- und Unternehmensmanagement, Finanzsektor, internationale Terrorismusbekämpfung sowie Schwere und Organisierte Kriminalität. Als Polizeikommandant leitete er die Terrorismusbekämpfungsermittlungen für Großbritannien während der Olympischen Spiele 2012 in London. Auch hier haben wir also jemanden, der sich in einer öffentlich finanzierten Regierungsposition etabliert hat. Die Steuerzahler haben das Gehalt dieses Mannes getragen, und jetzt nutzt er die Stellung, die er sich als Angestellter der britischen Regierung aufgebaut hat, um sich in einem Geschäft zu bereichern, das im Grunde genommen an den verschiedenen abscheulichen Menschenrechtsverletzungen Israels mitschuldig ist. Das ist die Welt, in der wir hier im Westen leben, liebe Leute. Das sind die Menschen, die sowohl auf Regierungsebene als auch im privaten Sektor das Sagen haben. Lassen Sie uns nun von dem guten alten Tony ablassen. Bevor wir uns Ihr Gespräch mit dem Vertreter von CoreSite auf der Milipol anhören, könnten Sie uns etwas mehr über das Produkt erzählen, über das Sie mit ihm gesprochen haben?

RY: Ja, Dimitri, ich habe hier ein kleines Bild. Aus Datenschutzgründen habe ich eines verwendet, auf dem man das Gesicht des Mannes nicht wirklich sehen kann, obwohl er wusste, dass ich dieses Foto gemacht habe. Man sieht, dass er mich ansieht, und ich habe ihn gefragt, ob ich ein Foto machen darf. Das Produkt ist also im Grunde eine Kamera, die mit einer Software verbunden ist, und diese Software ist in der Lage, eine unglaubliche Bildverarbeitung und Gesichtserkennung durchzuführen. Selbst wenn man völlig verpixelt ist, selbst wenn es nachts dunkel ist, selbst wenn man weit entfernt ist, kann diese Kamera, diese Software, erkennen, wer man ist. Auf ihrer Website vergleichen sie ihre Software mit der der Konkurrenz und behaupten, dass sie 20 Mal effizienter ist. Selbst der Mann, mit dem ich gesprochen habe und der sagt, dass er seit fünf Jahren im Bereich der Gesichtserkennung arbeitet, meint, dass dies das irrsinnigste Produkt ist, das er je gesehen hat. Und es funktioniert so, dass man eine Eingabequelle hat, in diesem Fall eine Kamera, genauer gesagt eine Webcam, aber er sagt, dass diese durch CCTV, Bodycams, Drohnen oder jede andere Art von Videoquelle ersetzt werden könnte, und dass es in der Lage ist, jemanden sehr schnell zu erkennen und dann eine Überprüfung anhand einer Whitelist oder einer Blacklist durchzuführen, ich glaube, auf der Website steht, dass das in 0,01 Millisekunden geschieht. Es kann anhand dieser Whitelist oder Blacklist nach Übereinstimmungen suchen. Auch dies scheint sehr nützlich für Polizeibeamte zu sein, die Bodycams tragen, wenn sie jemanden identifizieren wollen, oder für die Grenzsicherheit, wenn sie Personen identifizieren wollen, die auf einer Beobachtungsliste stehen. Im Grunde genommen handelt es sich also um Überwachung.

DL: Ist es also Ihr Verständnis, Rami, auch wenn Sie vielleicht keine Antwort darauf wissen, dass diese Gesichtserkennungstechnologie jeder kaufen kann, solange er bereit ist, den Preis zu zahlen? Oder wird sie nur an zugelassene Kunden verkauft? Wenn beispielsweise ein Milliardär sagt: „Ich möchte ein Expertenteam, das jederzeit in Nanosekunden Gesichter identifizieren kann“, könnte diese Person dann diese Technologie kaufen, weil sie die finanziellen Mittel dazu hat? Oder ist sie nur für staatliche Stellen verfügbar?

RY: Ich habe ihm diese Frage gestellt. Ich sagte: „Wer nutzt dies?“ Zunächst einmal lautete seine Antwort: Jeder. Ich denke, das beantwortet Ihre Frage, Dimitri. „Jeder“. Er sagte nicht jedes Unternehmen, jeder Staat. Er sagte nur: Jeder. Aber ich habe ihn auch gefragt: „Würde ein Einkaufszentrum, würde Walmart ein Kunde von Ihnen sein?“ Er sagte: „Auf jeden Fall.“ Es handelt sich also um ein Tool, mit dem man Menschen scannen, mit einer Liste abgleichen und dann auf der Grundlage des Abgleichs entscheidende Maßnahmen ergreifen kann.

DL: Okay, hören wir uns also Ihr Gespräch mit dem Mitarbeiter von CoreSite an.

CoreSite: Im Grunde, jeden Videostream, Live-Stream, Videos, was auch immer. Sie laden also offensichtlich etwas hoch.

RY: Sie werden wahrscheinlich Ihr Gesicht hier hochgeladen haben. Und dann erklären Sie im Grunde, dass Sie eine Bedrohung darstellen.

CoreSite: Ein Teil der Vorschriften impliziert also eine ethische und moralische Nutzung. Man kann nicht einfach alle beobachten. Sie können nur einige Personen beobachten, eine begrenzte Liste von Personen, und das wäre dann eine Beobachtungsliste. Aber sobald sie auf der Liste stehen, gibt es eine Übereinstimmung und sie werden erkannt. Selbst hier sind wir ziemlich nah an der Kamera, wo Sie den Mann über meiner Schulter sehen können auf dem...

RY: Ja, dieser Typ. Was zum Teufel?

CoreSite: Ja, ja. Das ist also nur von der Webcam.

RY: Aber das ist nicht für militärische Zwecke, denn man würde sich ja keine normale Webcam ansehen.

CoreSite: Nein, nein, nein. Das ist nur für die Ausstellung.

RY: Okay, aber man könnte eine bessere Kamera einsetzen.

CoreSite: Man kann echte Kameras verwenden, Drohnen oder was auch immer. Im Grunde jede Videoquelle. Auch wenn das Bild unscharf ist, verwenden wir dennoch eine Menge Daten. Es ist für militärische Zwecke konzipiert.

RY: Wo wird das derzeit eingesetzt?

CoreSite: Überall. Wir sind ein globales Unternehmen, also im Grunde genommen in vielen kommerziellen und militärischen Bereichen...

DL: Entschuldigung, was hat er gesagt, Rami? In vielen Bereichen?

RY: Ich glaube, er sagte lokal oder kommerziell und militärisch.

DL: Lokale und militärische Behörden, okay. Entschuldigung, bevor wir fortfahren, könnten Sie uns bitte erklären, was gerade passiert ist? Er hat Ihnen etwas darüber gesagt, dass man auf einer Beobachtungsliste steht. Was haben Sie in diesem Moment aus dem Gespräch verstanden?

RY: Denken Sie daran, dass ich vor einer Kamera stehe. Hinter mir laufen Leute vorbei. Etwa 50, 60, 70 Meter hinter mir steht eine Frau, die gerade diesen Test mit uns gemacht hat. Ich glaube, sie wurde für die Simulation auf eine Beobachtungsliste gesetzt. Und er sagt: Ich bin mir nicht sicher, ob Sie diese Frau auf dem Bildschirm sehen können. Man konnte sehen, dass sie markiert war. Und sie war etwa 70 Meter hinter mir. Man konnte sie auf dem Bildschirm kaum erkennen. Sie war wie ein winziger kleiner Pixel. Und er meinte: Wir können sie erkennen.

DL: Unmöglich.

RY: Da habe ich angefangen zu fluchen. Ich dachte mir: Heilige Scheiße, das ist ja ziemlich cool. Aber ich finde es auch wichtig zu erwähnen, dass sie auf ihrer Website für Smart Cities werben. Die Städte haben also Kameras, die Bilder werden an CoreSite übertragen, und CoreSite verfolgt dich im Grunde genommen. Alle reden über Verschwörungstheorien zu Smart Cities. Nach dieser Veranstaltung bin ich total umgehauen von diesen Smart Cities, Dimitri, und ich finde, das sollten wir alle sein.

DL: Auf jeden Fall. Okay, hören wir uns die letzten paar Minuten davon an.

CoreSite: Das macht ihnen das Leben ein bisschen leichter, denn man versucht zum Beispiel, einen Polizisten dazu zu bringen, sich 2.000 Gesichter zu merken...

RY: Das wird niemals passieren.

CoreSite: Ja, genau. Es gibt sogenannte Super-Erkenner für große Datenmengen. Okay, die sind sehr gut darin, aber wenn man 2.000, 3.000, 5.000 oder eine halbe Million Menschen hat, ist das unmöglich.

RY: Das ist sehr cool. Und wie viel kostet solch eine Software?

CoreSite: Das hängt vom Anwendungsfall ab. Es gibt verschiedene Stufen, je nachdem, wie viele Kanäle Sie nutzen möchten. Es geht um den Wert für das System. Wir versuchen also sicherzustellen, dass es für Sie tatsächlich einen Mehrwert darstellt.

RY: Könnte man das also für die private Sicherheit nutzen?

CoreSite: Ja, das könnte man. Wenn Sie Bodycams haben, die live streamen können, dann können Sie die Bodycams einfach direkt nehmen, natürlich auch Hundekameras oder ...

RY: Buchstäblich jede Videoquelle.

CoreSite: Ja. Das ist ziemlich einfach.

RY: Es ist also nicht nur für die Grenzkontrolle gedacht, sondern könnte auch für die Sicherheit in einem Einzelhandelsgeschäft eingesetzt werden.

CoreSite: Ja, eine große Kette.

RY: Walmart oder so etwas?

CoreSite: Ja, genau.

DL: Ich möchte hier kurz unterbrechen, Rami, denn ich bin mir nicht ganz sicher, wie ich seine Aussage interpretieren soll, aber für mich klingt es so, als hätte das Unternehmen eine große Datenbank mit Verdächtigen, Personen auf einer Beobachtungsliste, Taugenichtsen, und man zahlt für den Zugriff auf diese Datenbank. Als Sie ihn gefragt haben, wie viel das kostet, hat er gesagt: „Das hängt davon ab, wie viele Kanäle Sie nutzen“, richtig? Für mich klingt das so, als hätten sie eine riesige Datensammlung und man zahlt dafür, wie viel von diesen Daten man einsehen möchte. Haben Sie das auch so verstanden?

RY: So wie ich es verstanden habe, könnte es sich bei den Kanälen um die Zugangspunkte handeln. Nehmen wir also an, Sie haben eine Bodycam, zehn Bodycams oder 100 Bodycams, dann variiert der Preis. Aber ich glaube, als ich mit ihm gesprochen habe, erwähnte er, dass sie Zugang zu Beobachtungslisten der Regierung haben, auf die sie dann direkt zugreifen können, richtig? Nehmen wir einfach mal Interpol oder eine lokale Polizeibehörde. Sie können diese also nutzen. Ich denke also, man könnte Zugang zu diesen Whitelists erhalten, seine eigenen Whitelists verwenden und auch nach der Anzahl der Überwachungskameras bezahlen, die man in die Software integrieren möchte.

DL: Okay. Es ist noch etwa eine Minute übrig. Hören wir uns den Rest an.

CoreSite: Das nennen wir in unserer Software „Interesse“. Blacklist, Whitelist. Wenn jemand auf der Liste steht, erhält man einen Alarm. Wir haben auch eine andere Whitelist. Wenn man ein Rechenzentrum oder etwas Ähnliches hat, trägt man seine Mitarbeiter ein. Wenn jemand, der nicht zum Personal gehört, vor der Kamera erscheint, dann ...

RY: Ich habe früher bei CGI gearbeitet, und alle, die im Bereich Cybersicherheit tätig waren, mussten immer einen Augenscan machen, um einen Büroraum zu betreten. Wenn wir die Berechtigung hatten, ließen sie uns rein. Und das ist in gewisser Weise weniger aufdringlich.

CoreSite: Ja, es ist buchstäblich so, dass, sobald Sie in meiner Kamera auftauchen, sobald Sie hereinkommen, sobald Sie auf die Kamera zugehen, insbesondere für die Zugangskontrolle, wir ein super schönes, klares, großes Gesicht haben, und fertig.

RY: Wie ist die Resonanz bisher?

CoreSite: Wie bitte?

RY: Wie haben die Leute reagiert?

CoreSite: Ganz gut. Das Wichtigste ist wirklich, dass es viele Vorteile gibt, wie zum Beispiel die Datenschutzgrundverordnung ...

RY: Aber die DSGVO und in Kanada ... Haben wir außerhalb andere Gesetze?

CoreSite: Ja, es gibt Ähnliche, aber es ist eben doch anders. Wir haben Standorte in den USA, und hier sind sie eigentlich etwas begünstigt.

RY: Gibt es in den USA strengere Gesetze?

CoreSite: Ja, in einigen Bundesstaaten, ja. Wir hatten das Vergnügen, eines der schlimmsten zu erleben, was aber gut ist, weil wir es durchgestanden haben und mit euch zusammenarbeiten. In Amerika verwenden sie übrigens Gesichtsaufzeichnungen.

RY: Und das hier stammt aus Israel, richtig?

CoreSite: Ja.

RY: Und Sie sind ein Kämpfer, oder?

CoreSite: Ich nicht, nein. Sergio hat das gesagt. Ja, ja. Es ist so, als wäre ich nicht einmal im Vertrieb, sie haben mich alle verlassen. Also ja. Sie sind alle verschwunden.

RY: Jetzt ist es also zu spät.

CoreSite: Ja, ja. Ja, sie sind verschwunden. Sie haben mich verlassen.

RY: Und sie fahren in den Urlaub?

CoreSite: Ja, ja, genau. Ich arbeite seit etwa fünf Jahren mit Gesichtserkennung bei mehreren Unternehmen.

RY: Und dieses scheint besser zu sein?

CoreSite: Ja, die Entwicklung hat sich dramatisch verbessert. Wir nehmen so etwas wie –

RY: Das ist verrückt. Das ist verrückt.

CoreSite: Nur mit einer kleinen HD-Webcam. Wenn es eine echte Kamera mit einem echten Objektiv ist, ist es natürlich noch besser, aber...

DL: Bevor wir zum vierten und letzten Unternehmen übergehen, möchte ich Ihnen allen noch etwas mitteilen, Rami, Sie kennen diese Geschichte nicht, ich habe sie Ihnen noch nie erzählt, aber ich habe persönliche und schmerzhaft Erfahrungen mit Gesichtserkennungstechnologie

gemacht. Denn Ende der 90er Jahre habe ich eine Auszeit von meiner Anwaltstätigkeit genommen. Ich hatte mehrere Jahre an der Wall Street gearbeitet und war von der Anwaltschaft ziemlich angewidert. Eine Freundin von mir, eine Wall-Street-Anwältin, die in Yale und Stanford studiert hatte und sehr talentiert war, gründete ein professionelles Blackjack-Team. Es handelte sich um Menschen, die Kartenzählen praktizierten, um sich einen Vorteil beim Blackjack zu verschaffen, und sie lud mich ein, Mitglied des Teams zu werden. Das ist übrigens völlig legal. Es ist nichts Illegales daran. Und wir haben schnell gelernt, dass die Casino-Branche, das war in den 90er Jahren, – fast niemand hatte Gesichtserkennungstechnologie. Und die Pioniere dieser Technologie waren, soweit ich weiß, tatsächlich in der Casino-Branche, die sie zur Identifizierung von Personen einsetzte, die sie nicht in den Casinos wünschten. Wir erfuhren, dass wir 1999 von einer Sicherheitsfirma der Casino-Branche namens Gryphon Investigations in eine Datenbank aufgenommen worden waren, die eine der ersten Versionen dieser Technologie von einem Unternehmen in Boston namens Biometrica erworben hatte. Dies war also noch bevor Gesichtserkennungstechnologie in Flughäfen oder auf Straßen eingesetzt wurde – sie begann in Casinos. Und so habe ich sie schließlich verklagt. Ich verklagte diese Leute gemäß den Datenschutzgesetzen der Vereinigten Staaten, weil sie Gesichtserkennungstechnologie bei mir eingesetzt hatten. Am Ende einigte ich mich außergerichtlich, aber irgendwann erhielt ich eine höchst ungewöhnliche Einladung vom CEO von Biometrica, der mich davon überzeugen wollte, dass sein Unternehmen lediglich eine Technologie zur Verfügung stellte und dass diejenigen, die wirklich meine Rechte, meine Datenschutzrechte, verletzt hatten, die Detektei der Casino-Branche waren, die seine Technologie lizenziert hatte. Sie waren es, die mein Bild ohne meine Zustimmung in ihre Datenbank aufgenommen hatten. Also lud er mich nach Boston ein und führte mich durch die Produktionsstätte, die Software-Einrichtung, und ich traf die besten Ingenieure und so weiter, und am Ende des Tages entschied ich mich, sie fallen zu lassen, weil ich überzeugt war, dass meine eigentliche Klage gegen die Detektei in Las Vegas gerichtet war. Aber ich sage Ihnen, ich hätte mir damals nie vorstellen können, dass diese Technologie einmal allgegenwärtig sein würde. Heute ist sie überall. Sie ist allgegenwärtig, wird immer ausgefeilter und ist zu einem wichtigen Mittel geworden, mit dem unser Recht auf Privatsphäre ausgehöhlt wird. Das ist natürlich keineswegs eine Besonderheit Israels, denn sie haben diese Technologie in Israel im Zuge der Unterdrückung und Tötung von Palästinensern so intensiv genutzt, dass sie viele Möglichkeiten zur Verbesserung der Technologie kennengelernt haben. Und wieder einmal profitiert die israelische Wirtschaft von den Gräueltaten ihrer Militär- und Sicherheitskräfte gegen die Palästinenser. Wie auch immer, fahren Sie fort...

RY: Dimitri, bevor wir weitermachen – wir haben uns intensiv mit diesem Thema beschäftigt, um uns darauf vorzubereiten, und ich bin mir nicht sicher, ob Sie es mitbekommen haben, aber bestimmt nicht, denn sonst wären Sie sicher empört. Aber wussten Sie, dass Awz Ventures drei Sitze im Vorstand von CoreSite hat? Und sie sind ein großer Investor hinter CoreSite. Es ist eine ihrer Leidenschaften, sozusagen ihre Vorzeiginvestitionen. Und diese Information steht auf ihrer Website. Sie können ihren Vorstand sehen, und es handelt sich um den Gründungspartner, Manager, was auch immer, den CEO von Awz.

DL: Das ist also die Firma, zu der Woolsey von der CIA, der Mann vom Mossad und der ehemalige Chef des CSIS, der kanadischen CIA, gehören. Sie sagen also, es geht nicht nur um Octopus Systems, sondern auch um CoreSite?

RY: Wir haben keine Informationen über Octopus, um zu wissen, wie viele Sitze sie im Vorstand haben. Aber bei CoreSite, wenn man ihre Website aufruft und auf Vorstand klickt, sieht man, dass der CEO von Awz Partner, ich habe seinen Namen vergessen, und seine beiden anderen Handlanger im Vorstand von CoreSite sitzen. Und das ist dieselbe kanadische Firma, Dimitri, von der Sie sagten, dass sie nur einen Block von Ihnen entfernt ist. Sie sind die Hauptgeldgeber von CoreSite. Sie haben Zugriff auf all diese Daten. Und alles liegt in den Händen dieser Leute, die wir gerade offengelegt haben, und wie korrupt ihr Vorstand ist.

DL: Wow. Wie weit diese Tentakel reichen...

ENDE

Vielen Dank, dass Sie diese Abschrift gelesen haben. Bitte vergessen Sie nicht zu spenden, um unseren unabhängigen und gemeinnützigen Journalismus zu unterstützen:

BANKKONTO:

Kontoinhaber: acTVism München e.V.
Bank: GLS Bank
IBAN: DE89430609678224073600
BIC: GENODEM1GLS

PAYPAL:

E-Mail:
PayPal@acTVism.org

PATREON:

<https://www.patreon.com/acTVism>

BETTERPLACE:

Link: [Klicken Sie hier](#)

Der Verein acTVism Munich e.V. ist ein gemeinnütziger, rechtsfähiger Verein. Der Verein verfolgt ausschließlich und unmittelbar gemeinnützige und mildtätige Zwecke. Spenden aus Deutschland sind steuerlich absetzbar.

Falls Sie eine Spendenbescheinigung benötigen, senden Sie uns bitte eine E-Mail an: info@acTVism.org

BANKKONTO:

Kontoinhaber: acTVism München e.V.
Bank: GLS Bank

PAYPAL:

E-Mail:
PayPal@acTVism.org

PATREON:

<https://www.patreon.com/acTVism>

BETTERPLACE:

Link: [Click here](#)

IBAN: DE89430609678224073600
BIC: GENODEM1GLS