
CORNELIUS GRANIG
DARKNET
Die Welt im Schatten
der Computerkriminalität
Sicher
im Netz:
DARKNET.HELP
K&S

CORNELIUS GRANIG

DARKNET

Die Welt im Schatten der Computerkriminalität

K&S

Bildnachweis
S. 40/189: N.N.; S. 50: Gert-René Polli; S. 61: Ivo Ivanovski; S. 135: Johanna Kliment; S. 193: KRN (Kultur.Region.Niederösterreich); S. 199: DIHK/Paul Aidan Perry; S. 210: Manfred Andexinger; S. 222: Daniel Brun; S. 252: Thomas Topf

www.kremayr-scheriau.at

ISBN 978-3-218-01157-0

Schutzumschlaggestaltung: Sophie Gudenus
Unter Verwendung eines Bildes von ARTSILENSE/shutterstock
Lektorat: Gudrun Likar
Satz und typografische Gestaltung: Sophie Gudenus
Druck und Bindung: Christian Theiss GmbH, St. Stefan im Lavanttal

INHALTSVERZEICHNIS

1_ VORWORT

Kiew, am 4. Jänner 2013: Nach den langen Feierlichkeiten zum Jahreswechsel befindet sich die Ukraine in ihrem traditionellen geschäftlichen Tiefschlaf. Ein hochrangiger deutscher Wirtschaftsvertreter nimmt pflichtbewusst trotzdem schon jetzt seine Arbeit auf. Er öffnet sein digitales Postfach und klickt auf einen Link in einem ihm von einem Kollegen zugesandten E-Mail, als ihm fast das Herz stehen bleibt: Jemand hat offenbar die Festplatte seines Computers kopiert und im Internet frei zugänglich seine Nachrichten publiziert.[1] Die Veröffentlichung wird begleitet von Vorwürfen, seine Organisation würde Wirtschaftsspionage betreiben und in seinem engsten Umfeld befinde sich ein Geheimagent. Vorwürfe, die bis heute im Internet zu finden sind. Dieser Fall ist kein Einzelfall, aber einer von vielen, in denen die Betroffenen eine große Scheu davor haben, namentlich in Erscheinung zu treten. Zu groß ist die Angst davor, dass Presseberichte eher negative Folgen für sie oder ihre Organisation haben könnten. Es heißt schließlich nicht umsonst: „Wo Rauch ist, da ist auch Feuer.“ Dies suggeriert, dass jemand wohl nicht ganz ohne triftigen Grund im Kontext einer bösen Tat erwähnt wird, was zu einer sofortigen Vorverurteilung führt.

Damit haben wohl auch jene Täter spekuliert, die sich per E-Mail an Kunden einer verschwiegenen liechtensteinischen Privatbank wandten, bei denen sie große Schwarzgeldbestände vermuteten, und von ihnen 10 % ihres Guthabens erpressen wollten. Für den Fall der Nichtzahlung drohten sie mit der Meldung der

Kontostände an die Steuerbehörden. Dass sogar Medienberichte über derartige Vorfälle mit Vorsicht zu genießen sind, zeigt der Fall eines prominenten Hamburger Geschäftsmannes, der im Zuge der Berichterstattung über diese Erpressung von wichtigen Zeitungen als betroffener Kontoinhaber „interviewt" wurde und heute in Zusammenhang mit diesen Presseartikeln von reinen medialen Erfindungen spricht. Zuerst ein Bank-Datenleck und dann noch Fake News um dieses herum?

Noch schlimmer kommt es, wenn sensible Gesundheitsinformationen oder Fotos von medizinischen Eingriffen veröffentlicht werden. Patienten einer osteuropäischen Schönheitsklinik wurden Opfer eines Datenlecks, bei dem Tausende Fotos von Operationen im Darknet auftauchten, die erst gegen die Zahlung von hohen Geldbeträgen wieder entfernt wurden. Hatte der Klinikbetreiber zuerst russische Hacker hinter dem Datendiebstahl vermutet, so laufen mittlerweile Gerichtsverfahren gegen ehemalige Mitarbeiter der Klinik. Dieser Fall illustriert, wie wenig Skrupel manche Täter haben, die aus Geldgier offenbar nicht einmal vor der Veröffentlichung entstellender Fotos von Patienten zurückschreckten.

Die Computerkriminalität hat auch schon längst den Bereich der Politik erreicht, wo versucht wird, demokratische Wahlen zu beeinflussen und Politiker anzugreifen, um anderen Kandidaten Vorteile zu verschaffen. In Österreich wurden zwei sehr bekannte Spitzenpolitiker Opfer von nachhaltig rufschädigenden Veröffentlichungen im Internet:

> *„In einigen Fällen waren diese Posts so schändlich, dass wir bei den Betreibern gerichtlich erwirken konnten, dass die Absender genannt werden mussten, sodass wir eine Klage einbringen konnten. Es wurden Computer ausfindig gemacht, von denen solche Mails verschickt wurden, allerdings behauptete zum Beispiel der Inhaber einer Agentur, er wisse nicht, wer auf diesem Computer gearbeitet habe, das könne jeder gewesen sein. Damit ging er frei. Das ähnelt dem Fall einer Politikerin aus der jüngsten Zeit",*

sagt der ehemalige Salzburger Landeshauptmann Franz Schausberger.[2] Sein niederösterreichischer Amtskollege Erwin Pröll sah sich über Jahre mit einer umfangreichen, anonymen Kampagne konfrontiert, die eine schwere Belastung für ihn und seine Familie darstellte:

> *„Es wurden im Internet gezielt und auf breiter Ebene Gerüchte gestreut, die meine Familiensituation betrafen. Es war von Polizeieinsätzen, unehelichen Kindern und ähnlichen Unwahrheiten die Rede. All das wurde durch die sozialen Medien verbreitet – in einem ungeheuren Tempo und ohne die Möglichkeit, es stoppen oder einfangen zu können (...). Diese Zeit war hart. Vor allem deshalb, weil man machtlos ist und nichts oder nur sehr wenig dagegen unternehmen kann. Dort, wo wir Personen und Namen hatten, die diese Gerüchte weitergetragen haben, wurde der Anwalt eingeschaltet. Aber der Großteil der Anschuldigungen wurde ja unter Decknamen und anonym verbreitet."*

Die Strafverfolgung solcher Delikte ist oft sehr schwierig, vor allem wenn sich die Täter zum Tatzeitpunkt im Ausland befinden und ihre Taten in- und ausländische Geschädigte betreffen. Das illustriert etwa der Fall eines weltweit agierenden marokkanischen Hackers, der in der Schweiz vor Gericht gestellt wurde, weil er durch Phishing-Attacken mehr als Hunderttausend Kreditkartendaten unrechtmäßig beschafft und illegal verwendet hatte und so ein Millionenschaden entstand. Im Herbst 2016 wurde ihm gemeinsam mit zwei Komplizen in der Schweiz der Prozess für alle Straftaten gemacht. Der Täter war geständig und erhielt eine dreijährige Freiheitsstrafe. Obwohl die Ankläger das Einverständis aller betroffenen Länder hatten und die Angeklagten umfang-

reiche Geständnisse ablegten, hob das Schweizer Bundesstrafgericht die Anklage auf und entschied, dass nur der Teil der Taten angeklagt werden dürfe, der Schweizer Geschädigte betrifft. Da die dafür vorgesehene Höchststrafe durch den Gefängnisaufenthalt schon abgesessen war, mussten die Täter sofort freigelassen und für die zu lange in der Haft verbrachte Zeit mit über 100.000 Franken entschädigt werden, wie der *Tages-Anzeiger* berichtete.[3]

Datendiebstahl und Verletzung der Privatsphäre, digitaler Rufmord: Macht das Internet es Kriminellen leichter, ihre Straftaten unbemerkt zu begehen und ungestraft davonzukommen? Nicht immer. Denn manchmal werden digitale Spuren, die sehr lange Zeit auffindbar sind, zu ihrem größten Problem. So geschehen im Fall des Hackers, der im November 2016 das Netzwerk für fast eine Million Kunden der Deutschen Telekom lahmlegte. Die Betroffenen konnten über zwei Tage lang keine Verbindung zum Internet herstellen.[4] Aufgrund der Schwere der Straftat rief das deutsche Bundeskriminalamt die „Operation Harbour" ins Leben und suchte mit einem großen Team und internationaler Unterstützung nach dem Verbrecher. Der Täter Daniel Kaye hatte während der Tatbegehung einmal sein Facebook-Profil aufgerufen. Das und einige andere digitale Spuren führten die Ermittler zu ihm. Er behauptete anfangs, dass alles ein Irrtum und er selbst Opfer eines Hackers geworden sei, der seine digitale Identität missbraucht habe. Auch diese Lüge konnte ihm nachgewiesen werden, und er wurde schließlich von deutschen und britischen Gerichten zu langjährigen Haftstrafen verurteilt.

Aus den angeführten Beispielen lässt sich erahnen, wie vielfältig Computerkriminalität ist und welches Potenzial die digitalen Werkzeuge für Verbrecher haben. Dabei hat die Kriminalität, die von Rechentechnologie unterstützt wird, eine lange Historie, die ihren Anfang in den 1930er-Jahren nach der Machtübernahme Adolf Hitlers in Deutschland nahm. Die Nationalsozialisten benutzten von IBM hergestellte Lochkarten und von einer IBM-Tochterfirma angemietete Zählmaschinen, um eine umfangreiche und detaillierte Analyse ihrer Bevölkerung durchzuführen, aus der sie nach und nach erkennen konnten, wo sich welche Bevölkerungsgruppen in Deutschland oder später in den besetzten Gebieten aufhielten. Die Verwendung dieser modernen Technologie wurde zu einer Schlüsselfrage für die Logistik der Transporte in Konzentrationslager und für die Vernichtung der Juden.[5] IBM verurteilte in einer Pressemitteilung die Verbrechen der Nationalsozialisten und verwies darauf, dass diese politischen Kräfte vor und während des Zweiten Weltkrieges die Kontrolle über ihr Unternehmen in Deutschland erlangt hatten. Die Stellungnahme von IBM – auf die im Kapitel „Historische Entwicklung" noch näher eingegangen wird – illustriert auch das Risiko, das mit den großartigen Erfindungen der Informationsgesellschaft verbunden ist: Gelangen sie in die falschen Hände, können sie für üble Zwecke eingesetzt werden. Nur gibt es einen wesentlichen Unterschied zu früher: Waren die Nutzer von neuen Technologien einst Staaten oder große Firmen und Organisationen, die einen beträchtlichen Aufwand für den Einsatz treiben mussten, so stehen diese durch die Durchdringung unserer Gesellschaft mit den neuen Informations- und Kommunikationstechnologien häufig auch für einzelne Individuen unentgeltlich zur Verfügung. Das Internet ist 50 Jahre nach seiner Erfindung in der Mitte unserer Gesellschaft angekommen, und an deren Rändern tummeln sich immer mehr Kriminelle, die diese Technologien anwenden. Das technische Darknet ist dabei nur eine Ecke des Netzes, in dem besondere Vorkehrungen für Verschlüsselung und Anonymität gelten und dessen Inhalte nicht durch normale Suchmaschinen gefunden oder von normalen Webbrowsern aufgerufen werden können.[6] Während in den letzten Jahren viel darüber geschrieben wurde, welche Gefahr aus diesem Bereich kommt, wird häufig darauf vergessen, dass es generell zu einer schrittweisen Digitalisierung der Krimina-

lität gekommen ist, mit der die Strafverfolgungsbehörden nur schwer mithalten können. Der Schweizer Generalbundesanwalt Michael Lauber sagte dazu in einem Zeitungsinterview:

> *„Wir bekämpfen die Kriminalität des 21. Jahrhunderts mit einer Organisation des 19. Jahrhunderts."*[7]

In diesem Buch wird das „große Darknet" beschrieben, das dunkle Netz, in dem die Digitalisierung der Kriminalität voranschreitet und in der Computerkriminalität in all ihren vielfältigen Formen Verbreitung findet. Das Buch nimmt sowohl auf die vergangene als auch die gegenwärtige Technologienutzung Bezug, mit der altbekannte Verbrechen unterstützt werden, die aber auch neue Kriminalitätsformen hervorgebracht hat, die ausschließlich in der virtuellen Welt existieren. Der Schwerpunkt der Recherchen liegt im deutschsprachigen Raum, aus dem die meisten Fallbeispiele und Interviewpartner kommen. Überdies wird ein Eindruck von den Strukturen, Technologien und der Dimension dieser Nebenwelt vermittelt, die deshalb so groß geworden ist, weil Täter von den in der realen Welt nicht vorhandenen Möglichkeiten – etwa dem vollständigen Verwischen von Spuren, der mangelnden Nachvollziehbarkeit von Aktionen und auch dem einfachen Legen falscher Fährten – angezogen werden wie Motten vom Licht. Das macht es für die Polizei so schwer, Kriminelle zu finden und zweifelsfrei zu überführen. Die gute Arbeit der Strafverfolgungsbehörden und vor allem deren Zusammenarbeit mit Whistleblowern und Bürgerrechtsaktivisten illustriert aber auch die positiven Seiten der neuen Technologien, wenn diese sorgfältig und gesetzestreu eingesetzt werden. In den letzten Jahren häufen sich die Erfolge bei der Aufklärung von Delikten im Bereich der grassierenden Korruption, die ohne Unterstützung von anonymen Hinweisgebern, die im Schutze des Darknets agieren, nicht möglich wären.

_Was ist Computerkriminalität und welche Behörden erfassen sie?

Oft wird die Frage aufgeworfen, ob Computerkriminalität nur eine erweiterte Form von bestehenden kriminellen Handlungen ist, die damit einfacher internationalisiert und anonymisiert werden können. Das ist in manchen Belangen durchaus zutreffend, wenn man beispielsweise an das Agieren nigerianischer Betrüger denkt, die bereits in den 1980er-Jahren Bittbriefe versandt haben, um an Geld aus dem Ausland zu kommen, und nun mit Spam-Mails eine viel einfachere Verbreitungsmöglichkeit vorfinden, als sie der traditionelle Postweg bot. Allerdings gibt es auch völlig neue Delikte, die ohne Computersysteme und Netzwerke nicht denkbar wären. Darunter fallen alle Kategorien von elektronischer Datenmanipulation und Hacking. Grundsätzlich kann man für Straftaten mit Computerunterstützung eine Einteilung nach den folgenden Kategorien vornehmen:

- Das widerrechtliche Einbrechen in Computersysteme oder Netzwerke durch Hacker
- Verschiedene Formen von Betrug und Diebstahl von Daten
- Das Verbreiten von obszönen oder pornografischen Materialien bis hin zu kinderpornografischen Inhalten
- Das Ausüben von psychischer oder physischer Gewalt und die Bedrohung wehrloser Opfer, beispielsweise durch Cyber-Mobbing, Hate Speech oder Cyber-Stalking[8]

Interessant ist auch der Blick in die Kriminalstatistiken der verschiedenen Länder, die ein jährliches Wachstum dieser Straftaten um bis zu 30 % ausweisen. Dabei werden aber unterschiedliche Definitionen verwendet, sodass die Statistiken nicht direkt vergleichbar sind. Das österreichische Bundeskriminalamt hat in seinem jüngsten Lagebericht die folgende Begriffsdefinition verwendet:

„Das gesamte Ausmaß des Begriffs Cybercrime lässt sich nur schwer fassen. In der Alltagssprache werden dazu alle Straftaten gezählt, die unter Verwendung von Informations- und Kommunikationstechnik (IKT) oder gegen diese verübt werden. Die Polizei unterscheidet dabei zwischen Cybercrime im engeren und Cybercrime im weiteren Sinne.

Als Cybercrime im engeren Sinne werden alle Straftaten bezeichnet, bei denen es sich um direkte Angriffe auf Daten oder Computersysteme handelt. Darunter fallen beispielsweise Datenbeschädigung, Hacking oder Distributed-Denial-of-Service(DDoS)-Attacken, die eine Dienstblockade darstellen.

Cybercrime im weiteren Sinne erfasst jene Delikte, bei denen die Informations- und Kommunikationstechnik in der Planungsphase, Vorbereitung und zur Ausführung herkömmlicher Straftaten eingesetzt wird – wie etwa Betrugsdelikte, Kindesmissbrauchsmaterial, Cyber-Grooming, Cyber-Mobbing oder Cyber-Bullying. Dabei kann es sich um jede Form von Kriminalität handeln."[9]

Um die „Computerkriminalität im weiteren Sinne" besser zu erfassen, werden diese Delikte in der deutschen Polizeilichen Kriminalstatistik (PKS) nicht unter dem Begriff „Cybercrime" registriert, sondern unter dem Tatbestand, der im Vordergrund steht, mit der speziellen Sonderkennung „Tatmittel Internet". Das gilt z.B. für Ransomware-Attacken, die unter dem Tatbestand der Erpressung erfasst werden, bei denen Kriminelle Computer verschlüsseln und nur gegen Zahlung von (meist digitalem) Lösegeld wieder entschlüsseln. Mit der Sonderkennung „Tatmittel Internet" lässt sich ein Bezug zur Computerkriminalität herstellen, auch wenn die Hauptstraftat eine andere ist.

Liechtenstein führt selbst keine Statistik über Delikte im Bereich der Computerkriminalität. Dort arbeitet man eng mit den Schweizer Behörden zusammen, die in den letzten Jahren enorme Anstrengungen unternommen haben, um eine neue nationale Koordinationsstelle im Eidgenössischen Finanzdepartement einzurichten. Das „Kompetenzzentrum Cyber-Sicherheit" soll die optimale Zusammenarbeit aller beteiligten Stellen aus dem zivilen und militärischen Bereich sicherstellen. Darüber hinaus wurde in der Schweizer Regierung ein neuer Cyberausschuss unter Teilnahme der Minister für Justiz/Inneres, Finanz und Verteidigung eingerichtet, der auf höchster Ebene über diese Fragestellungen berät.

Der Aufbau gesamthaft agierender Behörden nach dem Vorbild der Schweiz oder zumindest Konzepte für die effiziente Koordination in diesem sensiblen Bereich sind unerlässlich, da die Computerkriminalität laufend an inhaltlicher Breite gewinnt und sich länder- und sektorenübergreifend immer mehr ausbreitet.

_Was ist das Darknet?

Die Inhalte des Internets gliedern sich in zwei wesentliche Bereiche: das Clear Web und das Deep Web, das auch das Dark Web beinhaltet (dieses benutzt Technologien des Darknets).

Das Clear Web (auch World Wide Web, Surface Web oder Visible Web genannt) ist der Teil des Internets, der von herkömmlichen Suchmaschinen (wie Google, Yahoo oder Bing) gefunden werden kann. Man schätzt, dass es fünf Billionen Webseiten beinhaltet.

Das Deep Web (auch Invisible Web oder Hidden Web genannt) basiert auf den gleichen Technologien wie das Clearnet, ist aber nicht durch Suchmaschinen auffindbar, weil es von dieser Suche nicht erfasst oder davon ausgenommen wurde. Dazu zählen beispielsweise die internen Webseiten großer Konzerne, Webseiten, die nur nach Eingabe eines Passworts erreichbar sind oder sich hinter einer Paywall befinden. Man nimmt an, dass das Deep Web mindestens 500-mal größer als das Clear Web ist.

Das Dark Web ist der kleinste Teil des Internets und stellt eine innere Schicht des Deep Web dar, die auf einer besonderen

Technologie, dem Darknet, basiert. Es kann nur über einen speziellen Browser erreicht werden.

Nach Schätzungen von Experten macht das Deep Web 99 % des Internets aus (davon sind 0,1 % im Dark Web enthalten), das Clear Web weniger als 1 %. In diesem Buch wird das Dark Web in der Folge mit dem Begriff „Darknet" bezeichnet, da dieser weitverbreitet ist und sich für diesen Bereich des Internets im deutschen Sprachraum wohl durchgesetzt hat.

_Wie kann man auf das Darknet zugreifen?

Ganz einfach, indem man sich die Browser-Software Tor auf einem Desktop-Computer oder Smartphone installiert. Häufig wird auch gefragt, ob diese Installation strafbar ist, ob Behörden damit auf einen aufmerksam werden oder ob man damit sofort auch Teil eines kriminellen Netzwerks wird. Die Antwort zu all diesen Fragen ist ein klares Nein. Was man – mit dem Tor-Browser ausgestattet – im Darknet macht, ist jedem Benutzer so wie auch in den anderen Teilen des Internets selbst überlassen. Es liegt in der Verantwortung des jeweiligen Users, ob er sich dort im Rahmen der Gesetze bewegt oder ob er sich zu Straftaten hinreißen lässt. Der Tor-Browser selbst ist nur ein Werkzeug, um einen besonderen Teil des Internets zu erschließen. Finanziert wird der Browser überwiegend durch amerikanische Behörden oder ihnen nahestehende Organisationen – ursprünglich war ja das Darknet als sichere Kommunikationsplattform für amerikanische Behördenmitarbeiter konzipiert worden. Die Freigabe für die Benutzung durch jedermann hat vor allem den Hintergrund, dass Bürgerrechtler und Whistleblower in die Lage versetzt werden sollen, ihre Aktivitäten gegen diktatorische Regime oder das Aufzeigen von Missständen in Organisationen oder Unternehmen im Schutz der Anonymität durchführen zu können.

Einer der Mitgründer des Tor Project, Roger Dingledine, brachte es in einem Interview auf den Punkt:

> *„Es gibt eigentlich kein ‚Dark Web', das existiert nicht. Das sind nur einige wenige Webseiten."*[10]

Damit verwies Dingledine auf die Benutzung des technischen Darknets durch Kriminelle. Seine Recherchen hatten ergeben, dass nur 3 % des Verkehrs auf dem Tor-Netzwerk illegal seien, die restlichen 97 % würden nur die Anonymität dieser Umgebung nutzen. Dass diese Werkzeuge durch Kriminelle missbraucht werden, ist ein zumindest von den USA als Hauptfinanzierer durchaus in Kauf genommener Nebeneffekt. Die in diesem Buch beschriebenen Anwendungsfälle lassen in vielen Bereichen aber darauf schließen, dass die Werkzeuge und Funktionalitäten des Darknets nur für einen kleinen Teil der Computerkriminalität verantwortlich sind. In vielen Fällen erscheint dieser Aufwand den Kriminellen auch gar nicht notwendig, da sie beispielsweise in dem Land, aus dem heraus sie operieren, ohnehin vor Strafverfolgung sicher sind. Häufig ist es auch so, dass große Berichte über Datenlecks falsch oder schlecht recherchiert sind und zumindest die Annahme eines Angriffs aus dem anonymen Darknet bei näherer Betrachtung falsch ist, weil sich ein Innentäter in der Organisation ganz einfacher Mittel bedient hatte und später Kopien der von ihm einfach und ganz ohne aufwendigen Technologieeinsatz erlangten Daten in Umlauf bringt.

_Struktur dieses Buches

Der erste Teil des Buches beinhaltet einen kurzen Abriss über die Entwicklung der Kriminalität im Zusammenhang mit der Nutzung von Computertechnologien und Rechenmaschinen. Er beginnt mit den Nationalsozialisten, die basierend auf Lochkartentechnologie eine erste äußerst abscheuliche „Big Data"-Anwendung benutzten, um ihre Bevölkerung zu zählen, zu kategorisieren und danach bestimmte Bevölkerungsgruppen systematisch zu vernichten. In der Zeit des Kalten Krieges war der

technologische Wettlauf ein ständiger Wegbegleiter. Die Russen versuchten bis in die 1960er-Jahre, eigene Computer zu entwickeln, beschlossen dann aber, westliche Systeme zu kopieren. Die anderen Staaten des Ostblocks machten dabei in großem Stil mit. Das Ziel all dieser spektakulären, in der Nähe des Geheimdienstmilieus ablaufenden Vorgänge war stets die Erlangung der technologischen Vorherrschaft, die zur Ausschaltung der Feinde führen sollte. Mit Lieutenant General Dan Leaf kommentiert ein hochrangiger US-Militär die historische Entwicklung, während der ehemalige österreichische Geheimdienstchef und frühere Sicherheitschef von Siemens, Gert-René Polli, das letzte Jahrzehnt und die aktuelle Situation beleuchtet.

Im zweiten Teil des Buches werden die vielen Formen der Computerkriminalität beschrieben. Das reicht von der Computersabotage über Phishing-Angriffe bis hin zu Seitenkanalattacken, über die kryptografische Prozesse in Computerchips gestört werden, um danach in Systeme eindringen zu können oder ihren Ablauf zu verändern. Am vielfältigsten sind die verschiedenen Formen des Betrugs, der mit digitaler Hilfe neue Dimensionen angenommen hat. Niemand ist mehr vor Angriffen gefeit, da die allgegenwärtige Digitalisierungswelle auch die Kriminalität erfasst hat. Der langjährige mazedonische IT-Minister und Topmanager Ivo Ivanovski nimmt in einem Interview zu den neuen Entwicklungen Stellung und kommentiert interessante Fälle mit internationaler Dimension aus seinem Heimatland.

Im dritten Teil wird die Technik beschrieben, auf der das Darknet basiert und überdies erläutert, wie man – rechtlich einwandfrei – selbst in diese Welt eintauchen kann. Das vorgestellte Spezialbetriebssystem Tails ist eine unentgeltliche Plattform, die für Whistleblower und Bürgerrechtsaktivisten eine sichere Arbeitsumgebung darstellt. Die in diesem Kapitel besuchten dunklen Teile des Darknets illustrieren, dass das Gerede von der organisierten Kriminalität im Internet schon einen validen

Hintergrund hat. Handelsplätze, auf denen Waffen, illegale Substanzen und falsche Reisepässe gekauft oder Auftragsmorde bestellt werden können, werden von skrupellosen Gangstern betrieben, die es mit den neuen Technologien leicht haben, über Ländergrenzen hinweg zu operieren. Häufig nutzen sie auch Kryptowährungen, die keiner Zahlungsverkehrskontrolle unterliegen. Der österreichische Kryptowährungsexperte und Unternehmer Max Tertinegg beleuchtet die Situation rund um Bitcoin und andere digitale Währungen und deren Bedeutung für das Darknet.

Im Hauptteil des Buches werden spektakuläre Fälle behandelt und dabei sowohl die Ausbreitung der Computerkriminalität als auch die Möglichkeiten ihrer Verhinderung diskutiert. Das reicht von angeblichen und wirklichen Datenlecks im Gesundheitsbereich, der anonymen Verleumdung von Politikern im Internet und der Beeinflussung von Wahlen über den Datendiebstahl bei Banken und die Bedrohung von deren Kunden bis hin zu Angriffen auf die Infrastruktur großer Telekommunikationskonzerne und Energieversorger. Dabei vermitteln Opfer und Experten aus der Schweiz, Österreich, Deutschland, Liechtenstein und anderen Ländern der Welt eine Einschätzung über den Hintergrund und die Tragweite dieser Taten. In Exklusiv-Interviews für dieses Buch sprechen die ehemaligen österreichischen Landeshauptleute Franz Schausberger und Erwin Pröll darüber, wie nachhaltig mittels Cyberrufmord in ihr Leben eingegriffen wurde. Zu Wort kommt auch Kriminaldirektor Fred-Mario Silberbach vom deutschen Bundeskriminalamt, der mit seinem Team einen besonders gefährlichen Hacker enttarnen und festnehmen konnte.

Im vorletzten Kapitel wird mithilfe von Behördenmitarbeitern und Sicherheitsexperten eine Übersicht über die deutschsprachigen Länder und das Aufkommen der Computerkriminalität erarbeitet. Über die Situation in Österreich spricht Manfred Andexinger, ein promovierter Politikwissenschaftler aus dem Kabi-

nett des Innenministeriums, der auch wesentliche Fragestellungen der Sicherheitsforschung aufgreift. Neben einem Überblick über das deutsche Bundeskriminalamt wirft Ilja Nothnagel – Mitglied der Geschäftsführung des Deutschen Industrie- und Handelskammertags (DIHK) – einen Blick auf die Wirtschaft, die sich vielfach im Spannungsfeld zwischen Digitalisierungsnotwendigkeiten und Cybergefahren befindet. Aus der Schweiz vermittelt der renommierte Sicherheitsexperte und ehemalige Generalstabsoberst Christoph Brun ein Lagebild, das weit über die Landesgrenzen hinausgeht. Schließlich wird der Länderüberblick durch Patrik Thoma von der Liechtensteinischen Landesverwaltung abgerundet, der die bisherige Entwicklung und Sicherheitslage sorgenvoll betrachtet.

Im letzten Kapitel dieses Buches erhalten die Leser umfangreiche Ratschläge für das sichere Arbeiten mit Computern und die Kommunikation über Netzwerke. Dabei wird sowohl auf die Bedürfnisse von privaten Benutzern als auch von größeren Organisationen oder Firmen eingegangen und ein Katalog von Maßnahmen vorgestellt, mit denen man die Sicherheit verbessern kann. Eine wesentliche Möglichkeit dafür stellt auch ein neuer, verbesserter Umgang mit anonymen Hinweisgebern (sogenannten „Whistleblowern“) dar. Der Präsident des Kuratoriums Sicheres Österreich (KSÖ), Erwin Hameseder, informiert in einem exklusiven Interview über die Aktivitäten seines Cybersicherheits-Thinktanks und gibt einen Ausblick auf die Zukunft.

Abschließend wird die Plattform DARKNET.help vorgestellt, die weit über das Buch hinausgehende, vertiefende und laufend aktualisierte Materialien aus der Praxis der Cyber-Security bereitstellt und Privatanwendern, Firmen und Organisationen mit Ratschlägen bei und gegen Cyberattacken zur Seite steht und ihnen hilft, weniger angreifbar zu werden.

2_ HISTORISCHE ENTWICKLUNG

Als Apple-Chef Tim Cook im Oktober 2018 in einer Rede vor dem Europäischen Parlament vor dem Entstehen eines „datenindustriellen Komplexes“ warnte, tat er das in Anspielung auf die Warnung des früheren US-Präsidenten Dwight D. Eisenhower, der in seiner Abschiedsrede im Jahr 1961 vor dem zunehmenden Einfluss des „militärisch-industriellen“ Komplexes gewarnt hatte:

> *„Wir in den Institutionen der Regierung müssen uns vor unbefugtem Einfluss – beabsichtigt oder unbeabsichtigt – durch den militärisch-industriellen Komplex schützen. Das Potenzial für die katastrophale Zunahme fehlgeleiteter Kräfte ist vorhanden und wird weiterhin bestehen. Wir dürfen es nie zulassen, dass die Macht dieser Kombination unsere Freiheiten oder unsere demokratischen Prozesse gefährdet. Wir sollten nichts als gegeben hinnehmen. Nur wachsame und informierte Bürger können das angemessene Vernetzen der gigantischen industriellen und militärischen Verteidigungsmaschinerie mit unseren friedlichen Methoden und Zielen erzwingen, so dass Sicherheit und Freiheit zusammen wachsen und gedeihen können.“*[11]

Cook wählte diese Analogie, da offenbar in den Augen von Apple die Daten ihrer Kunden in falsche Hände geraten und wie im Fall von Cambridge Analytica missbräuchlich verwendet werden könnten. Er sprach über private Daten, mit denen gewinnbringend gehandelt werde und die im schlimmsten Fall „als Waffe mit militärischer Effizienz“ eingesetzt würden.[12] In der Geschichte der Informationstechnologie ist die Entstehung von machtpolitischen Komplexen unter Ausnützung von Technologievorteilen

nicht neu. Der nachfolgende kurze und fragmentarische Abriss über die Historie der Computerkriminalität beginnt in einer besonders problematischen Zeit, als die Vorläufer der Computer verwendet wurden, um die Bevölkerung zu vermessen und basierend auf den so erhobenen Daten Strategien für deren partielle Vernichtung zu entwickeln.

_„Big Data“ im Dritten Reich

Wenn es um die Frühzeit der Computer geht, sind den meisten von uns Bilder von riesigen Metallschränken erinnerlich, in denen sich Röhren befanden, welche die ersten Computersysteme antrieben, während große herumfliegende Käfer in diesen Röhren immer wieder Fehler verursachten (ihre Entfernung wurde übrigens als „De-Bugging“ bezeichnet, ein Ausdruck, der sich bis heute im Sprachgebrauch von Programmierern für Verfahren zur Fehlersuche gehalten hat). Vor diesen Systemen gab es aber schon eine Generation von Rechenmaschinen, die mit Lochkarten betrieben wurden. Eine davon, die in Deutschland entwickelte Hollerith-Maschine DEHOMAG D11, erlangte besonders negative Berühmtheit, da sie von den Nationalsozialisten zur Volkszählung und genauen Erfassung (inklusive der ethnischen Merkmale) der Bevölkerung in Deutschland und später in besetzten Gebieten eingesetzt wurde. Die Rechenmaschinen entstammten der Deutschen Hollerith-Maschinen Gesellschaft mbH (DEHOMAG), einem Tochterunternehmen von IBM, das nach Herman Hollerith benannt war, der im Jahr 1884 die Lochkarte patentieren hatte lassen, auf der Daten gespeichert wurden. Im Jahr 1890 wurde die Hollerith-Maschine, wie das aus einer Tabelliermaschine, Lochkartensortierer, Lochkartenlocher und dem Lochkartenleser bestehende System genannt wurde, von der amerikanischen Volkszählungsbehörde zur Auszählung der Volkszählungsdaten des Jahres 1890 eingesetzt. Dadurch konnte die benötigte Zeit von sieben Jahren auf zwei Jahre (unter

Einsatz von 500 Angestellten) verringert werden. 1896 gründete Hollerith die Tabulating Machine Company, die er 1911 an einen Investor verkaufen musste, der sie mit zwei anderen Firmen zur CTR (Computer Tabulating Recording Corporation) fusionierte und im Jahr 1924 in IBM (International Business Machines Corporation) umbenannte. Seit 1910 gab es mit der DEHOMAG einen deutschen Lizenznehmer, der Hollerith-Maschinen vermietete. An dieser Firma erwarb IBM in den 1930er-Jahren 90 % der Anteile und steigerte den Personalstand von 155 Mitarbeitern im Jahr 1925 auf 2561 im Jahr 1940. Die Gewinne wurden größtenteils als Lizenzabgaben an den Mehrheitseigentümer in den USA abgeführt.

Der große amerikanische IT-Konzern IBM geriet Jahrzehnte nach dem Einsatz der Hollerith-Maschinen durch die Nazis unter massiven öffentlichen Druck, nachdem der amerikanische Autor Edwin Black ein Buch mit dem Titel „IBM und der Holocaust“ veröffentlicht hatte, in dem die Technologienutzung durch die Nationalsozialisten untersucht wurde. Black warf IBM die Beitragstäterschaft zu den Massenmorden des Holocausts im Zweiten Weltkrieg vor, oder zumindest eine aktive Hilfestellung für das damalige Regime. Den ehemaligen Präsidenten von IBM, Thomas J. Watson sen., beschuldigte er überdies, für seine Verdienste um die Datenverarbeitung des Dritten Reiches von Adolf Hitler am 28. Juni 1937 den „Deutschen Adlerorden mit Stern“ erhalten zu haben.

IBM räumte in einer Presseerklärung vom 14. Februar 2001 ein, dass von ihrer deutschen Tochterfirma DEHOMAG Systeme an Nazi-Deutschland geliefert worden waren:

> *„Es ist seit Jahrzehnten bekannt, dass die Nazis Hollerith-Maschinen eingesetzt haben und dass diese in den 1930er-Jahren von IBMs deutscher Tochterfirma – der Deutschen Hollerith-Maschinen Gesellschaft mbH (DEHOMAG) – geliefert wurden.“*[13]

Allerdings verwies man schon damals darauf, dass IBM viele Unterlagen über die Aktivitäten der DEHOMAG, die in Deutschland bis zu 2500 Mitarbeiter beschäftigte, verloren hatte und man daher keine detaillierten Informationen mehr dazu habe. Die wenigen verfügbaren Dokumente würden aber von Historikern untersucht:

„IBM verfügt nicht über viele Informationen über diese Zeit oder die Aktivitäten der DEHOMAG. Die meisten Dokumente wurden im Krieg verloren oder zerstört. Die verbliebenen Dokumente wurden vor einiger Zeit öffentlich verfügbar gemacht, um die geschichtliche Forschung zu unterstützen. Die Dokumente wurden von den Standorten der Firma in New York und in Deutschland an die New York University und die Universität Hohenheim in Stuttgart transferiert – beide sind renommierte Institutionen, die als Verwalter für diese Aufzeichnungen geeignet sind. Unabhängige Experten dieser Einrichtungen überwachen nun den Zugriff auf diese Dokumente durch Forscher und Historiker."[14]

Am 29. März 2002 erschien eine weitere Stellungnahme des Konzerns, nachdem inzwischen auch der Einsatz der IBM-Technologie im von den Nazis besetzten Polen medial diskutiert wurde. Man verwies nochmals darauf, dass sich internationale Experten im Rahmen von zeitgeschichtlichen Analysen mit den neuen Fragestellungen befassten und IBM auch jederzeit bereit sei, neue Dokumente zur Verfügung zu stellen, die sich mit dieser Zeit befassten:

„IBM hat auch klargestellt, dass wir im Falle des Auffindens neuer Dokumente über diese Zeit diese zusätzlich verfügbar machen werden."[15]

IBM-Chefin Virginia Rometty stand leider nicht für ein Interview für dieses Buch zur Verfügung, allerdings meldete sich der weltweite Kommunikationschef des Unternehmens, Edward Barbini, und übersandte eine umfangreiche Stellungnahme. Er führte aus, dass die Nazis im Zweiten Weltkrieg die Kontrolle über die deutsche Tochterfirma von IBM erlangt hatten:

„Uns ist es wichtig zu betonen, dass unsere Firma nie zu diesen Vorwürfen geschwiegen hat. Die Nazis erlangten vor und im Zweiten Weltkrieg die Kontrolle über die deutschen Firmen von IBM, wie sie auch die Kontrolle über andere Unternehmen erlangten, die in ausländischem Eigentum standen."[16]

Die Rolle des legendären IBM-Präsidenten Thomas J. Watson, nach dem IBM inzwischen die neue, sehr strategische Produktreihe „Watson" im Bereich künstlicher Intelligenz benannt hat, wird in Hinblick auf das Deutschland-Geschäft von IBM zu dieser Zeit stark relativiert:

„Thomas Watson hat eine Medaille erhalten – darüber wird oft geschrieben –, aber er hat sie als Präsident der Internationalen Handelskammer erhalten, nicht als Vorstandsvorsitzender von IBM … und sie wurde ihm 1937 überreicht, bevor der Krieg begann. Er sandte die Medaille im Jahr 1940 zurück, um gegen die Aggression der Nazis zu protestieren. (…)

Es ist wissenschaftlich nicht erwiesen, dass die IBM-Zentrale in New York die Aktivitäten der DEHOMAG managen konnte."[17]

Bei IBM distanziert man sich auch in aller Form von den Taten der Nazis, hat bisher aber keine neuen Dokumente zu diesen Fragen gefunden. Ein interner Ausschuss befasst sich derzeit mit der Technologiefolgenabschätzung in sensiblen Geschäftsfällen:

„IBM und seine Mitarbeiter auf der ganzen Welt verurteilen die verabscheuungswürdigen Verbrechen der Nazis und alle Unterstützer ihrer unbeschreiblichen Taten. (…) Basierend auf den Informationen unseres Unternehmens gibt es keine neuen Informationen und Fakten von Forschern über diese wichtige Fragestellung und Zeit. (…)

Im Hinblick auf den Technologieeinsatz und dessen Compliance sollten Sie wissen, dass IBM einen internen Ausschuss eingerichtet hat, der sich mit potenziellen Geschäften beschäftigt, um sicherzustellen, dass es zu keinem Technologiemissbrauch kommt. Wir führen eine sorgfältige Prüfung von möglichen Projekten durch. Es gibt viele Berichte über das Projekt ‚Maven', das sich mit dem Einsatz von Drohnen für das amerikanische Militär befasst. Wir glauben, dass das Ziel dieses Projekts das Durchkämmen von großen Datenmengen ist, um möglicherweise die eine Nadel im Heuhaufen zu finden, die helfen kann, Leben zu retten. Sei es das Leben von Amerikanern, das ihrer Verbündeten oder das der Zivilbevölkerung. Das ist eine Mission, die IBM unterstützt und der Grund, warum wir weitermachen. Wir möchten auf keinen Fall den Einsatz von Technologien unterstützen, die das Verletzen oder Töten von Menschen automatisieren."[18]

IBM verweist abschließend auch darauf, dass der Einsatz von künstlicher Intelligenz dazu führen soll, menschliche Entscheidungen zu verbessern, dass sie diese aber nicht ganz ersetzen kann, und schließt mit der nachdenklichen Bemerkung:

„Es gibt Entscheidungen, die nicht durch Technologie ersetzt werden können."[19]

Die Diskussion über den historischen Einsatz von IBM-Technologie illustriert die Gefahr, die mit den neuen Technologien einhergeht: Wenn sie in die falschen Hände geraten, können sie große, irreparable Schäden anrichten und sogar dazu führen, dass staatliche Gewalt sich in einem ungeheuren Ausmaß gegen Menschen richtet.

_Das Computer-Wettrüsten im Kalten Krieg

Nach dem Zweiten Weltkrieg wurde auf Basis von Transistoren eine neue Technologie entwickelt, mit der die bisher mit Elektronenröhren betriebenen Computer schrittweise abgelöst wurden. Der viel geringere Stromverbrauch, Größe und Hitzeentwicklung der Transistoren machten ihren Einsatz viel einfacher. Damit wurde der Grundstein für den Siegeszug der Computer gelegt. Bis dahin war es aber noch ein weiter Weg, da IBM erst im Jahr 1955 den ersten durch Transistoren betriebenen Rechner (IBM 608) vorstellte. Heute stecken in den von uns verwendeten Computern und Smartphones Milliarden Transistoren (beispielsweise enthält der A11-Prozessor von Apple, der im iPhone A8 steckt, 4,3 Milliarden Transistoren).

Nach dem Zweiten Weltkrieg begann der Rüstungswettlauf der Supermächte, in dem die Computertechnologie eine immer größere Rolle spielte. Die Sowjetunion entwickelte bis in die 1960er-Jahre eigene Computersysteme, stieg dann aber darauf um, westliche Systeme illegal zu kaufen und zu kopieren. Die Sowjets waren dem Westen allerdings trotz dieser Strategie in vielen Belangen unterlegen:

- Durch die zentrale Wirtschaftsplanung gab es nicht die notwendige Flexibilität, um auf Design- oder Produktionsänderungen zu reagieren. Daher kam es immer wieder zu Engpässen bei wichtigen Komponenten.
- Durch die schiere Größe der Sowjetunion und die schlechte Information zwischen den verschiedenen IT-Zentren wusste die eine Hand häufig nicht, was die andere tat.
- Die wichtigste Zielsetzung für viele sowjetische Manager war die Erreichung vordefinierter Produktionsquoten. Das ging häufig zulasten der Qualität.

- Im Rahmen der Vergütung für sowjetische Manager gab es keine Leistungsanreize für Innovation und Erfindungen.
- In vielen Fällen gab es eine sehr klare Trennung zwischen Entwicklung und Produktion, sodass die Bereiche nicht gut aufeinander abgestimmt wurden.
- Die Sowjets arbeiteten in vielen Fällen ohne elektronische Design-Unterstützung (CAD/CAM), um Computer zu designen – weil sie auch dafür zu wenige Computersysteme hatten.
- Aus Angst, dass Computer antirevolutionäre Aktivitäten unterstützen könnten, wurde nur einer kleinen Gruppe von Menschen Zugang zu diesen Technologien gewährt.
- Die Unterstützung für Anwender von Computern war denkbar schlecht, und noch schlechter war die Computerwartung, sodass viele Systeme nur äußerst mangelhaft oder gar nicht funktionierten.

Die Sowjets verloren durch die aufwendigen Beschaffungsvorgänge und die nachfolgenden Reverse-Engineering-Bemühungen, um die Systeme nachzubauen, viel Zeit und waren beispielsweise im Großrechnerbereich dem Westen sieben bis 15 Jahre hinterher. Ein CIA-Report aus dem Jahr 1989 illustriert, dass der damals beste PC, ein Modell der Serie IBM PS/2, 23 Kilogramm wog, auf einem Schreibtisch Platz fand und mit einer Rechengeschwindigkeit von 3 MIPS[20] arbeitete. Der damals beste Großrechner aus der Sowjetunion wog im Vergleich dazu neun Tonnen, musste in einer Halle untergebracht werden, die mindestens 20 Meter lang war, und war gerade fünf Mal so schnell.

Zur Kontrolle von Technologieexporten war 1949 von den USA das Coordinating Committee for Multilateral Export Controls (COCOM) gegründet worden, dem alle NATO-Staaten sowie Japan und Australien angehörten. Dieses Komitee führte eine Liste von sowohl zivil als auch militärisch verwendbaren „Dual-

Use"-Gütern und Technologien, deren Export in den kommunistischen Osten verboten war. In einem Lagebericht des CIA wird 1982 erwähnt, in welcher Weise die Sowjets trotzdem illegal beschaffte amerikanische Technologie nutzten:

> *„Mitte der 1960er-Jahre kopierten die Sowjets integrierte Schaltkreise (ICs) der Serie 7400 von Texas Instruments, um Logika-2-Schaltkreise zu produzieren. Diese ICs wurden dann benutzt, um ihren eigenen ES-1030-Computer zu entwickeln, dessen Design und Architektur vom IBM-Großrechnermodell 360/40 kopiert war. Dieser Großrechner fand seinen Einsatz vor allem im militärischen Bereich."*[21]

In einem anderen Bericht aus dem Jahr 1989 wird davon gesprochen, dass einzelne Staaten des Ostblocks wie Ungarn und Polen erfolgreich die COCOM-Regelungen umgingen und erfolgreich Nachbauten von IBM-PCs produzierten, indem sie Technologie in Österreich und in der Schweiz einkauften. Diese beiden Länder galten bis Ende der 1980er-Jahre als wichtige Drehscheiben für illegale Technologieexporte in den Osten, da sie als neutrale Länder nicht von den COCOM-Regelungen betroffen waren. Der amerikanische Geheimdienst CIA berichtete 1989, dass der Markt mit Neugeräten, aber vor allem mit gebrauchten Großrechnern der Marke DEC VAX florierte:

> *„Es existieren große Anreize für die Sowjets, westliche Technologie und hier vor allem Computer zu kaufen. Obwohl diese Rechner nach westlichen Maßstäben als ‚veraltet' betrachtet werden, sind sie in der Regel erst drei bis fünf Jahre alt. Damit sind sie um einiges fortschrittlicher als die neuesten Rechner, welche die Sowjetunion selbst produzieren kann. Preise für gebrauchte Rechner betragen üblicherweise einen Bruchteil des Neupreises – der Listenpreis für eine gebrauchte VAX 11/750s wäre beispielsweise um die 90.000 Dol-*

lar, während gebrauchte Geräte um 15.000 Dollar gekauft werden können. Überdies ist es einfacher, gebrauchte Geräte zu vertreiben, die ursprünglich an europäische Endbenutzer verkauft wurden. Die amerikanischen Exportbestimmungen werden von den europäischen Händlern für Gebrauchtgeräte größtenteils ignoriert. (...) Überdies ist die Fälschung von Endbenutzerzertifikaten für den Export weitverbreitet, sodass bei der Auflistung von Österreich und der Schweiz als Zielland für gebrauchte Computer schon bei der Ausstellung mit einer Umleitung in den Osten gerechnet werden kann."[22]

_Fragwürdige Computerexporte durch eine Gruppe um Udo Proksch

Österreich war aufgrund seiner geografischen Lage und seiner Neutralität ein Knotenpunkt für Embargogeschäfte. Besonders gut war man damals mit der Deutschen Demokratischen Republik im Geschäft, die auch blendende politische Kontakte zu Österreich unterhielt.[23] In dem im Jahr 1984 von britischen und amerikanischen Journalisten herausgegebenen Buch *Techno-Bandits* wurden die Wege beschrieben, die Computer von West nach Ost nahmen. Österreich wurde dabei ein eigenes Kapitel gewidmet, da man diesem Land eine zentrale Rolle als „Kanal" für illegale Exporte zuschrieb, der beispielsweise durch den berüchtigten Geschäftsmann Udo Proksch und seine Freunde genützt wurde.[24] Ein enger Freund von Proksch, der KZ-Überlebende Rudi Wein, war in den 1960er-Jahren für den Büromaschinenkonzern Olivetti tätig geworden und hatte im April 1966 gemeinsam mit Udo Proksch die Firma KIBOLAC Handelsgesellschaft gegründet. Diese Firma begann in großem Stil Westtechnologie in die Sowjetunion und nach Osteuropa zu exportieren.[25] In ihrem Umfeld wurde die Firma Sacher Technik Wien von Rudolf Sacher und Karl Heinz Pfneundl gegründet, die in Zusammenarbeit mit der amerikanischen SSII (Semiconductor Systems International, Inc.) und ihrem Gründer Peter Gopal in allerhand

illegale Machenschaften, unter anderem das Reverse Engineering von Texas-Instruments-Chipsätzen und deren Verkauf an die DDR und Polen, involviert war. Gopal kaufte die Chips am freien Markt und analysierte sie mit Kamera und Mikroskop. So konnte er die Baupläne ausspähen und sie an Fabriken im Osten für die Produktion von Kopien dieser Bauteile mithilfe der Österreicher weiterverkaufen. 1978 wurde er wegen des Diebstahls und Handels mit Firmengeheimnissen von Intel und National Semiconductor verhaftet. Im Laufe der Untersuchungen, die von mehreren Behörden in den USA gegen ihn geführt wurden, tauchten auch die Namen von Udo Proksch, dessen Bruder Roderich und Rudolf Sacher in den Unterlagen von Gopal auf.

Nach dem Überlaufen des hochrangigen Stasi-Offiziers Werner Stiller 1979 in den Westen wurden Wein und seine Komplizen von den österreichischen Behörden verhört. Stiller gab viele Namen weiter, darunter offenbar auch den von Rudi Wein, dem damaligen Eigentümer des Café Gutruf in Wien, einem Treffpunkt der österreichischen „High Society". Wein wurde die Leitung der „Residentur" der ostdeutschen Staatssicherheit in Wien als IM „Prokurist" zugeschrieben. Die Stasi habe über ihn eine Karteikarte angelegt, auf der folgende Beschreibung enthalten war:

„Wein, Rudolf – österr. Staatsbürger, (...). Stabile Zusammenarbeit. Schaffte Voraussetzungen zur Materialbeschaffung auf dem Gebiet der Elektronik. Abdeckung durch Aktivitäten mit Außenhandelsbetrieben der DDR. Der IM konnte die inoffizielle Arbeit durch seine offizielle Geschäftstätigkeit mit DDR-Organen abdecken."[26]

Stiller beschuldigte Rudolf Sacher, für die DDR-Organisation IAI (Industrieanlagen Import) eine 74-seitige Studie über den Stand der westlichen Technik in der Halbleiterproduktion ausgearbeitet zu haben, die ihren Weg in den DDR-Staatssicherheitsdienst fand. Und auch von Gopal kamen schwere Beschuldigungen,