Der Fall der Berliner Mauer, der Untergang des Sowjetreiches sowie die wachsende Bedeutung neuer Kommunikationsformen und des Internets veranlassten die Planer im Pentagon und die Agenten der diversen Geheimdienste, sich neue Tätigkeitsfelder zu erschließen: die virtuelle Cyberwelt. „Es ist eine Doktrin, das Pentagon hat Cyberspace formell als neues Kriegsgebiet anerkannt“, schrieb der stellvertretende US-Verteidigungsminister William J. Lynn III. im Herbst in einem Essay der Zeitschrift *Foreign Affairs*. Von **Armin Wertz**[*].

Dieser Artikel ist ein exklusiver Auszug aus dem gerade erschienen Buch „Die Weltbeherrscher. Militärische und geheimdienstliche Operationen der USA“

Als 2008 „ein ausländischer Nachrichtendienst“, wie Lynn behauptete, versuchte, in die Systeme einiger NSA-Generale einzudringen, war dies „ein Weckruf“ und ein „Wendepunkt in der US-Cyber-Strategie“, vergleichbar mit 1939, als Präsident Franklin D. Roosevelt jenen Brief erhielt, in dem ihn Albert Einstein vor der Möglichkeit eines Atomkrieges warnte. Und 2011 schließlich drohte Präsident Barack Obama unverhohlen mit Krieg. Die USA sahen sich im Internet im Krieg und behielten sich das Recht vor, in Zukunft auf Hacker-Attacken in ihre Systeme mit konventionellen Waffen zu reagieren. Sollte irgendein Land mit Viren, Würmern oder Trojanern in die USA eindringen, riskiere es einen Gegenangriff mit allen militärischen Mitteln, mit Kampfflugzeugen, Panzern und Truppen. Dabei sind die USA die emsigsten Lauscher und Hacker von allen.

2009 richtete das Pentagon das U.S. Cyber Command (CYBERCOM) mit einer Cyberoperationszentrale auf dem Luftwaffenstützpunkt Lackland bei San Antonio, Texas, mit zunächst 7000 Luftwaffenangehörigen ein. CYBERCOM dient vorrangig dem Schutz der Spionagesatelliten im Orbit. Dazu entwickelt das Pentagon einen fliegenden Schild unbemannter Drohnen. In der Exosphäre testet die Luftwaffe seit 2010 den X-37B-Raumgleiter, der mit Raketen bestückt werden soll, um Schläge gegen rivalisierende Netze wie das chinesische, das zur Zeit erst im Entwicklungsstadium ist, durchführen zu können. Für die audiovisuelle Überwachung plant das Pentagon, eine Armada von 99 Global-Hawk-Drohnen in der Stratosphäre zu installieren. Und für eine erweiterte und präzisere Überwachung aus dem Weltraum ersetzt das Pentagon „seine teuren Spionagesatelliten durch eine neue Generation von leichten Billigmodellen wie dem ATK-A200. Seit seinem erfolgreichen Start im Mai 2011 kreist dieses Modul in 250 Meilen Höhe über der Erde mit ferngesteuerten Kameras von U-2-Qualität, die dem US-Zentralkommando heute eine ‚gesicherte Nachrichten-, Überwachungs- und Aufklärungsfähigkeit‘ garantieren.“

Vierzig Kilometer nordöstlich von Washington befindet sich Fort George G. Meade, kurz Fort Meade, mit zahlreichen Regierungsbehörden, wie der Defense Information School, dem

Defense Courier Service, dem United States Cyber Command und dem Hauptquartier der größten und mächtigsten Geheimdienstorganisation der Welt, der National Security Agency (NSA). Schon 2006 sprach ein Fachmann in der Zeitung *USA Today* von der „größten Datenbank, die je auf der Welt aufgebaut wurde“, wobei das Ziel „eine Datenbank über jedes jemals geführte Telefonat“ sei.

In ihrem Open Source Center in McLean, Virginia, werten die „vengeful librarians“ (rachsüchtige Bibliothekare), wie sie liebevoll genannt werden, sämtliche Informationsquellen aus, die der Öffentlichkeit zugänglich sind, also lokale Radio- und TV-Stationen, Zeitungen, Internet-Chatrooms, Facebook, Twitter. Ob in Arabisch oder Mandarin, ob ein ärgerliches Tweet oder ein nachdenklicher Blog, die Analytiker sammeln jeden Fetzen Information. Gleichzeitig nötigte die NSA neun Internetgiganten – darunter Microsoft, Yahoo, Google, Facebook, AOL und Skype –, Milliarden von E-Mails auf ihre Datenfarmen zu transferieren. Echelon, wie das streng geheime Sammelsystem heißt, fängt alles auf: Millionen Liebeserklärungen, verärgerte Forderungen oder bedauernde Entschuldigungen, Kundenkonten bei Banken oder Patientenprotokolle in Krankenhäusern. Die privaten E-Mails, die sich Prinzessin Diana und Dodi al-Fayed schickten, wurden ebenso aufgefangen wie die Details der Vertragsverhandlungen zwischen der europäischen Airbus und Saudi-Arabien oder die Telefongespräche zwischen einer Mutterfirma und ihren Zweigniederlassungen.

Die 1945 gegründete NSA verfügte 2007 über 54 Satelliten und weltweit über zahllose Lauschanlagen (von Waihoapai in Neuseeland über Kojarena in Westaustralien und Bad Aibling in Bayern bis zum Polarkreis), die jedes Wort, das über eine Telefonverbindung gesprochen wurde, oder jedes Fax, jede E-Mail, die über Satellit verschickt wurde, auffingen. Ende der 90er Jahre schätzte die NSA, dass weltweit circa 2,5 Milliarden Telefone und 1,5 Milliarden Internetadressen existierten, dass jede Minute annähernd zwanzig Terabytes (20 x 10^12 Bytes) Informationen um die Erde kreisten. Diese Datenmenge wurde dann an die riesigen Computer in Fort Meade weitergeleitet, von denen jeder einzelne mit einem System verbunden war, das ein Petabyte (10^15 Bytes) Daten speichern kann, acht Mal mehr als die gesamte Bücher- und Dokumentensammlung der Library of Congress. Fünf Billionen Textseiten kann das elektronische Archiv der NSA speichern. Die Computer lesen, analysieren und selektieren das Material in „petaflop speed“, d. h. der Computer kann in einer Sekunde eine Quadrillion (1024) Operationen durchführen. Verglichen mit der Geschwindigkeit der NSA-Computer „erscheint ein Blitz langsam“, sagte der ehemalige CIA-Direktor William Colby einmal. „Da war ein Programm, das in einer Minute 500 Worte in sieben Sprachen übersetzen konnte. Als ich das nächste Mal, einen Monat später, dort war, hatte es seine Kapazität verdoppelt und die

Übersetzungszeit halbiert.“

Mit anderen Systemen wie Silkworth oder Moonpenny können sich die NSA-Spione in die angeblich sichere Satellitenkommunikation von Militäreinrichtungen oder von Regierungen und Diplomaten einklinken, die geheimsten Informationen herunterladen und anschließend dechiffrieren. „Kein Code, der von den Kryptologen nicht entschlüsselt wurde.“ Schon 1989 fing alleine die Lauschstation in Menwith Hill in Nordenglands Yorkshire 17,5 Milliarden Nachrichten ab. Menwith Hill konnte damals pro Stunde zwei Millionen Nachrichten verarbeiten, von denen 13 000 genauer angeschaut wurden. Von diesen wurden 2000 nach Fort Meade geschickt. Am Ende wurden nur zwanzig tatsächlich analysiert und gespeichert. Derzeit soll die NSA in der Lage sein, alle sechs Stunden elektronische Daten im Umfang des gesamten Inhalts der Library of Congress abzufangen und herunterzuladen.

Alleine im März 2013 sammelten und verarbeiteten die NSA-Computer weltweit 97 Milliarden Mitteilungen, die von Predator- oder Reaper-Drohnen, von U-2-Spionageflugzeugen, Global Hawks, X-37B-Raumgleitern, Google Earth, Weltraumüberwachungsteleskopen und Satelliten aufgefangen worden waren. Weil das NSA-Hauptquartier Fort Meade von der Größe einer Stadt inzwischen nicht mehr ausreicht, richtete die NSA 2005 in San Antonio in einer ehemaligen Chip-Fabrik von Sony einen neuen Komplex zur Datenspeicherung ein. Und seit 2013 ist das Intelligence Community Comprehensive National Cyber-Security Initiative Data Center bei Camp Williams in Bluffdale, Utah, in Betrieb. In diesem Datenzentrum in der Wüste von Utah soll eine unendliche Menge von Informationen, das gesamte Wissen der ganzen Welt, gesammelt werden. Die 1,5 Millionen Quadratfuß große, zwanzig Gebäudekomplexe umfassende und zwei Milliarden Dollar teure Einrichtung verfügt über eigene, von der öffentlichen Versorgung unabhängige Wasseraufbereitungsanlagen, ein eigenes Elektrizitätswerk sowie sechzig Dieselgetriebene Reservegeneratoren mit den dazugehörigen Tanks, um einen drei Tage währenden totalen Stromausfall überbrücken zu können. Alleine die Computer produzieren eine jährliche Stromrechnung von siebzig Millionen Dollar.

„Mit der fortlaufenden Verbesserung der mit den diversen Überwachungsmissionen verbundenen Sensoren wächst der Datenumfang auf eine projektierte Große von Yottabytes (1024) bis 2015“, heißt es in einem Report, den die Mitre Corporation, ein Thinktank des Pentagon, erstellt hat. Ein Yottabyte entspricht einer Milliarde Terabyte. (Zum Vergleich: Für die digitale Speicherung sämtlicher Titel der amerikanischen Kongressbibliothek waren nicht mehr als 15 Terabyte nötig.) Das entspricht ungefähr einer Septillion (1 000 000 000 000 000 000 000 000) Textseiten. Zahlen größer als Yottabytes haben nicht einmal mehr Namen. Ein „Send“- oder „Answer“-Befehl auf einem PC in jedem gegebenen Haushalt – und die Details der Kommunikation landen in Big Brothers Datenbank.

Einmal aufgefangen und abgespeichert in diesen nahezu unbegrenzten Bibliotheken werden die Daten von Infowaffen und Supercomputern mit Hilfe komplizierter algorithmischer Programme analysiert, um zu bestimmen, wer von uns ein Terrorist sein kann oder werden könnte. Zu einem großen Teil müssen die abgefangenen und gespeicherten Daten nicht einmal mehr an die Zentrale in Fort Meade oder nach San Antonio geschickt werden. Das System Thin Thread korreliert die von einer Lauschstation abgefangenen Daten einer Person sofort mit bereits vorhandenen Daten von Finanztransfers, Reiseinformationen, Webrecherchen und anderen Angaben, die zur Entlarvung von Terroristen und anderen Übeltätern für notwendig erachtet werden, und vernichtet überflüssige Informationen sofort, womit das Problem eines Datenstaus im Zentralsystem (etwa in Fort Meade) weitgehend reduziert wird. Über 1,1 Millionen Terroristen oder des Terrorismus Verdächtige haben die Cyberkrieger der US-Geheimdienste inzwischen in ihre Überwachungsliste aufgenommen.

Natürlich hat die NSA ihre eigenen Hacker. Sie sind in einem geheimen Anbau, dem Friendship Annex oder FANX, auf dem Thurgood Marshall International Airport (der früher einmal Freundschaftsflughafen hieß) bei Baltimore untergebracht. Dort versuchen ganze Teams von Angreifern, in die Kommunikationssysteme befreundeter wie feindlicher Regierungen einzudringen. Andere Mannschaften wehren Versuche ab, in die US-Systeme einzudringen. Die NSA habe schon bei dem Angriff auf den Irak 1991 unbezahlbare Erfahrungen in Cyberspionage gesammelt, deren Techniken während des Kosovokrieges und später im Kampf gegen al-Qaida noch perfektioniert worden seien, erklärte ein ehemaliger NSA-Mitarbeiter Seymour Hersh gegenüber. „Was immer die Chinesen uns antun, wir können es besser. Unsere offensiven Cyber-Fähigkeiten sind weit fortgeschrittener."

Doch noch ist die Orwell'sche Welt nicht perfekt. Nicht nur, dass die NSA vor Beginn der Kriege im Nahen Osten oder am Hindukusch kaum über Daten aus Irak oder Afghanistan verfügte – der für die Region zuständige Lauschposten der NSA hatte nicht einmal einen Dolmetscher, der Paschto oder Dari beherrschte, die beiden am meisten verbreiteten Sprachen in Afghanistan –, auch im Vorfeld der Angriffe am 11. September 2001 versagten die Hightech-Experten. Über eineinhalb Jahre lang hörte die NSA zwei der führenden Hijacker während ihrer Vorbereitungen für die Anschlage ab und wusste, dass sie auf Weisung von Osama bin Laden handelten. Die Flugzeugentführer hatten ihr Hauptquartier in Laurel, Maryland, beinahe in Sichtweite des Büros des NSA-Direktors eingerichtet. Doch die NSA-Schnüffler beantragten nie einen Haftbefehl oder informierten wenigstens die CIA oder das FBI über die Anwesenheit der Verdächtigen.

Erfolgreicher hingegen belauschten sie ihre Verbündeten. Dazu hat der weltweit

operierende Special Collection Service (SCS) der NSA auf sämtlichen US-Botschaften „einen Antennenrotor namens ‚Einstein', eine Datenbank zur Analyse von Mikrowellen (Interquake) sowie ein Programm namens ‚Sciatica' eingerichtet, mit dem Agenten Signale im Gigaherzbereich erfassen können". Das aus der NSA-Zentrale in Fort Meade gesteuerte Programm Birdwatcher erfasst und analysiert verschlüsselte Signale und kann geschützte virtuelle Privatnetze, wie sie etwa von Botschaften und Privatunternehmen für die hausinterne Kommunikation genutzt werden, identifizieren.

2013 sorgten die Enthüllungen des Computerspezialisten Edward Snowden, der für Booz Allen Hamilton, eine private Vertragsfirma der NSA auf Hawaii, gearbeitet hatte, in Mexiko und Indonesien sowie vor allem in Europa für Aufregung. Snowden hatte umfangreiche Unterlagen der NSA kopiert und anschließend der Londoner Tageszeitung *The Guardian* zur Verfügung gestellt, die bewiesen, dass der US-Geheimdienst mit seinem geheimen Überwachungsprogramm Prism direkten Zugriff auf die Kommunikationsinhalte der Kunden größer IT- und Internetunternehmen hat.

Gemeinsam mit ihrem britischen Partner, dem Government Communications Headquarters (GCHQ), zapfte die NSA unter dem Codenamen Tempora die internationalen Glasfasernetze an. Nachdem sich auch noch Australien, Neuseeland und Kanada den Lauschern angeschlossen hatten, erhielt diese Abhörkoalition den Namen Five Eyes. Zwar nimmt die NSA seit 2007 seine „second-party-Five Eyes-Verbündeten", also andere NATO- oder SEATO-Partner, offiziell von der Überwachung durch ihr Computersystem Boundless Informant aus. Doch „können wir – und tun das oft auch – die Signale der meisten ausländischen third-party-Partner ins Auge fassen", wie aus einem 2013 öffentlich gemachten NSA-Dokument hervorgeht. Mit den third-party-Partnern sind eindeutig so enge Verbündete wie Deutschland, Frankreich oder Italien gemeint.

In Zusammenarbeit mit den Kollegen der CIA überwachte die NSA Videokonferenzen von UN-Diplomaten, spähte die diplomatischen Vertretungen der Europäischen Union in Washington und New York aus, überwachte unter dem Codenamen Dropmire das Kryptofax der EU-Botschaft in Washington, zapfte die Telefone im Europapalast des Europarats in Straßburg an, belauschte weltweit mindestens 38 Botschaften von Verbündeten, drang in das Computernetz des französischen Außenministeriums ein, verschaffte sich Zugange zum Netz des Zahlungsverkehr-Dienstleisters Swift, hackte das E-Mail-Konto des damaligen mexikanischen Präsidenten Felipe Calderón und zapfte die Mobiltelefone von insgesamt 122 Staats- und Regierungschefs an, darunter jene von Calderóns Amtsnachfolger Peña Nieto, des ehemaligen indonesischen Präsidenten Susilo Bambang Yudhoyono und der deutschen Bundeskanzlerin Angela Merkel.

Zwar betonen Washingtoner Cyber-Experten oft die Gefahren, die den USA aus dem Internet drohen, und reden oder schreiben gerne von befürchteten Angriffen, die das gesamte Energiesystem Nordamerikas lahmen könnten (was nach Expertenmeinung allerdings nahezu unmöglich ist, da es keine zentrale Schaltstation gibt, sondern Hunderte staatlicher wie privater Betreiber, die unabhängig voneinander operieren). Besonders China „führt eine wirtschaftliche Offensive" gegen die USA, behauptet James Lewis, ein Mitarbeiter am Zentrum für Strategische Studien, der zuvor für das Außen- sowie das Handelsministerium der Clinton-Regierung gearbeitet hatte. „Ein Teil davon ist Wirtschaftsspionage, wie wir sie kennen und verstehen. Ein Teil ist Wilder Westen. Jeder klaut von jedem. Unser Problem ist: Was können wir tun? Ich glaube, wir müssen sie (die chinesische Cyberbedrohung) langsam als ein Handelsproblem behandeln."

Dabei tun die Chinesen nur, was Amerikaner schon längst machen. Schon früh kümmerte sich die NSA um die Auftragsbücher der amerikanischen Wirtschaft. Alleine im Jahr 1993 „verhalf (das Spionagenetz) Echelon US-Firmen in Übersee zu Verträgen im Wert von 26,5 Milliarden Dollar, indem es Regierungen in der Dritten Welt alarmierte. Minister akzeptierten Bestechungsgelder." So horchte Echelon die Gespräche des ehemaligen französischen Ministerpräsidenten Edouard Balladur ab und verdarb dem Rüstungskonzern Dassault ein Sechs-Milliarden-Dollar-Geschäft. Silkworth fing Nachrichten ab, die bewiesen, dass Verkäufer der europäischen Airbus Industries saudischen Beamten Schmiergelder angeboten hatten. Das Geschäft machte daraufhin Boeing. 1994 belauschte Echelon die Telefonkommunikation zwischen Frankreichs Thomson-CSF und der brasilianischen Regierung über einen 1,4-Milliarden-Dollar-Vertrag für ein Kontrollsystem im Regenwald des Amazonas. Und „Moonpenny stellte sicher, dass auf den Philippinen, in Malawi, Tunesien, Peru und im Libanon Verträge, die sonst an europäische Firmen gegangen wären, letztendlich an amerikanische Unternehmen gingen".

In einer Rede im Mai 2009 veranschlagte Präsident Obama die Verluste amerikanischer Unternehmen in den Jahren 2007 und 2008 infolge von Cyberspionage auf acht Milliarden Dollar: „Es wird geschätzt, dass Kriminelle alleine im letzten Jahr weltweit geistiges Eigentum von Firmen im Wert von einer Billion Dollar gestohlen haben." Nicht nur Kriminelle, auch die USA sind prächtig im Geschäft des Cyberspace-Diebstahls. Die US-Botschaftsmitarbeiter scheinen gelegentlich weniger der Aufrechterhaltung der diplomatischen Beziehungen denn der Wirtschaftsspionage zu dienen, wie aus Wikileaks-Dokumenten hervorgeht, die in den Zeitungen des McClatchy-Pressekonsortiums, zu denen u. a. der *Miami Herald*, der *Philadelphia Inquirer* oder die *Sacramento Bee* gehören, veröffentlicht wurden.

Nachdem Russland Michail Chodorkowski verhaftet und seine Ölfirma Jukos aufgelöst hatte,

begannen die USA eine Art Ölkrieg gegen das Land. Um die alleinige Dominanz im Ölgeschaft zu erhalten, leiteten die USA diverse gegen Russland gerichtete Operationen ein. Zunächst heuerte die US-Botschaft in der Slowakei eine texanische Consultingfirma an, die auf das Ölgeschaft spezialisiert war, und begann, heimlich die slowakische Regierung zu beraten, wie sie die 49 Prozent Anteile an der slowakischen Ölpipeline-Gesellschaft Transpetrol kaufen konnte, die Jukos hielt. Die Texaner, die den Kaufverhandlungen beiwohnten, versicherten dem unerfahrenen slowakischen Wirtschaftsminister Lubomir Jahnatek, dass die verlangten 120 Millionen Dollar für die 49 Prozent von Jukos ein Schnäppchen seien. Die russische Gazprom sei bereit, einen weit höheren Preis zu bezahlen.

„Wir haben allen beteiligten Parteien klargemacht, dass wir unsere Beraterrolle nicht an die große Glocke gehängt sehen wollen“, hieß es in einem Kabel der US-Botschaft vom 10. August 2006, das den Deal beschrieb. „Jahnatek schätzt die Informationen des (texanischen) Beraters sehr und wird auch weiterhin von ihm und der US-Botschaft Informationen erwarten.“ Und der Journalist Kevin G. Hall ergänzte in seinem Artikel: „Die US-Botschaften konzentrieren sich weltweit“ auf die Sicherung möglichst vieler Ölressourcen. Von den 251 287 WikiLeaks-Dokumenten, die McClatchy (das Pressekonsortium, für das Hall arbeitet) erhielt, bezogen sich 23 927 – beinahe eines von zehn – auf Öl. Gazprom alleine ist in 1789 erwähnt.“

Ein anderer Ölkonzern, der den Unmut der USA auf sich gezogen hatte, war der italienische Öl-Gigant Eni. Der Konzern hatte versucht, sein Engagement ausgerechnet in zwei Staaten auszudehnen, die die USA als Feinde ansehen: Iran und Russland. „Der Eni-Vorstand Paolo Scaroni erzählte dem Botschafter, dass der iranische Energieminister Eni Investitionsmöglichkeiten im südlichen Pars und auf den Azadegan Öfeldern angeboten hat“, ist einem als geheim eingestuften Kabel der US-Botschaft in Rom vom 12. Januar 2007 zu entnehmen. „Scaroni sagte, Eni sei interessiert an zusätzlichen Investitionen, solange der Iran nicht multilateralen Sanktionen unterliege.“ Besonders aufgebracht waren die USA über Enis Absicht, das neue Geschäft als Rückzahlungen von Schulden des Irans zu deklarieren, die teilweise noch aus den 50er Jahren stammten. Als Eni 2009 erneut einen Versuch unternahm, die Geschäftsbeziehungen mit dem Iran auszudehnen, meldete die US-Botschaft nach Washington: „Posten denkt, dass es gute Grunde für USG (US-Regierung) gibt, skeptisch zu sein.“

Die Lauschoperationen der NSA-Satelliten brachten den USA noch mehr Beweise über unerwünschte Geschäftsverbindungen der Italiener. Wie einem Kabel der US-Botschaft in Rom vom 24. April 2008 – kurz vor Silvio Berlusconis letzter Amtsübernahme als Ministerpräsident – zu entnehmen ist, drängte der Botschafter das State Department und

Finanzministerium, Druck auf Scaroni auszuüben. Diesmal ging es um Italiens Geschäfte mit Russland. Ein Deal mit Eni hatte einerseits Gazprom Zugang zu Libyens Öl verschafft, wofür Eni andererseits an der Pipeline, die Gazprom durch das Schwarze Meer bauen wollte, beteiligt werden sollte. Dieses Projekt hatte mit einem ähnlichen US-Projekt konkurriert, das die kaspische Region unter Umgehung Russlands direkt mit Europa verbunden hatte. Washington wollte Russland unbedingt von Libyens Ölquellen fernhalten.

„Posten wünscht, die neue Berlusconi-Regierung unter Druck zu setzen, so dass Eni weniger als Steigbügelhalter für Gazprom handelt“, teilte die US-Botschaft in Rom ihren Vorgesetzten in einem vertraulichen Kabel mit. Ein paar Jahre später, am 20. April 2011, gab Scaroni schließlich dem Druck nach und machte in einer Presseerklärung einen Rückzieher: Eni werde das Geschäft, das Gazprom einen Anteil am libyschen Öl gegeben hatte, zeitweilig stornieren.

Schon 2007 hatte Brian Gladwell, ein ehemaliger Computer-Experte bei der NATO, die Einsicht verkündet: „Im Cyberspace haben wir heute eine Situation, in der staatlich gesponserter Diebstahl von Wirtschaftsinformationen eine Wachstumsindustrie ist.“

Inzwischen arbeiten wissenschaftliche Einrichtungen im Auftrag der U.S. Defense Advanced Research Projects Agency (DARPA) bereits an der nächsten Generation von Spionagewerkzeugen. Jahrelang bastelten Wissenschaftler an sogenannten Micro-Air-Verhicles (MAVs), fliegenden Robotern von der Größe kleiner Insekten, die ideal für Spionagetätigkeiten waren. Weil die Energieversorgung dabei eine kaum überwindbare Schwierigkeit darstellte, verfielen die Forscher auf eine neue Idee. Zahlreiche Forschungseinrichtungen in den USA sind längst dabei, völlig unverdächtige Spione zu kreieren: lebende Insekten, an denen ein paar winzige Veränderungen vorgenommen werden wie etwa Stimulatoren oder Elektroden, die in ihr Nervensystem eingepflanzt werden. Wissenschaftler haben herausgefunden, dass es viel einfacher ist, ein Insektenhirn und damit das Flugverhalten zu kontrollieren, als MAVs zu bauen.

Darum implantierten Biologen etwa der Texas A&M University Kakerlaken schon im Entwicklungsstadium Mikrochips ein, die mit dem Nerven- und Muskelsystem verknüpft wurden. Auch an der Universität von Michigan und an der Universität von Kalifornien in Berkeley pflanzten Wissenschaftler Hirschhornkäfern und am MIT Motten erfolgreich derartige mikroelektromechanische Systeme (MEMs) ein. Im bewegungslosen Zustand ihrer Entwicklung – z. B. im verpuppten Zustand – lassen sich die Insekten einfacher operieren und manipulieren. Die ausgewachsenen Insekten verhielten sich auch mit der eingebauten Hardware völlig normal. So konnten die Forscher den Flug der Motten steuern.

Die Energieversorgung der eingebauten Chips, so erhoffen es sich die Wissenschaftler, könnte durch die Umwandlung der Hitze und der mechanischen Energie, die das Insekt im Flug erzeugt, erreicht werden. Für den Fall, dass die natürlich erzeugte Energie nicht ausreicht, haben Wissenschaftler der Cornell Universität einen Radioisotopen-Transmitter entwickelt, der kybernetische Organismen mit radioaktiver Energie versorgt.

Sobald die Wissenschaftler diese Cyborgs oder Cybugs, wie sie genannt werden, kontrollieren können, sollen sie zum Einsatz kommen. Ausgerüstet mit Kameras, Mikrophonen und anderen Sensoren könnten sie dann von einem Kontrolleur gesteuert werden, ähnlich den unbemannten Drohnen, die Ziele in Afghanistan, Jemen, Pakistan, Somalia, Mali, Mexiko und anderen Ländern ausspionieren.

[«*] Armin Wertz ist seit 1997 freier Journalist, zunächst in Ost- und Südafrika, dann in Südostasien. Von 1976 bis 1979 war er Nachrichtenredakteur beim Stern, dann freier Journalist in Zentralamerika, von 1982 bis 1985 Auslandsredakteur beim Spiegel. Anschließend war er viele Jahre Korrespondent in Mexiko, Mittelamerika und die Karibik für den Spiegel, später für die Frankfurter Rundschau und den Tages-Anzeiger (Zürich), von 1991 bis 1995 Korrespondent der Frankfurter Rundschau und des Tages-Anzeigers in Israel.