NOH SOON-TAEK/REUTERS

Der Cyberwar ist kein auf das Netz begrenzter bloß virtueller Krieg. Solche Attacken können der Vorwand für einen militärischen Angriff sein. Andererseits kommt he Internets aus (südkoreanische Soldaten bei einer Übung in Seoul, im Hintergrund eine Plakatwerbung für den Film »Matrix Revolutions«)

Werkzeug und Waffe

Vom Kommandoinstrument des US-Militärs im Kalten Krieg zum universellen Kommunikationskanal im globalen Kapitalismus und neuen Gefechtsschauplatz der USA und ihrer Konkurrenten. Die Karriere des Internets. **Von Theo Wentzke**

Das Internet ist als militärische Erfindung der USA in der Planung des mit Kernwaffen zu führenden dritten Weltkriegs gegen den Hauptfeind Sowjetunion in die Welt gekommen. Den Atomkrieg berechenbar zu machen, hieß auch, davon auszugehen, dass russische Nuklearraketen auf US-amerikanischem Territorium einschlagen und massive Zerstörung anrichten. Vor dieser Gefahr mussten die politischen und militärischen Kommandostrukturen geschützt, der Zugriff auf Land und Leute, sichergestellt werden. In enger Symbiose entwarfen US-Rüstungsfirmen und Forschungseinrichtungen des Verteidigungsministeriums das Konzept, die militärische Kommunikation von Leitungen auf Datenpakete umzustellen, welche von Routern dezentral durch nicht zerstörte Teile des Netzwerks geschleust werden. Dies war Voraussetzung für die dezentrale Architektur des Internets, an deren Ausgestaltung Forschungsinstitute, Telefonunternehmen und Computerfirmen beteiligt wurden.

Der Dual Use des Internet

Doch kaum war die Architektur technisch fertig, dankte der Feind ab. Seitdem wird die Technik verteilter Kommandozentralen für militärische Netze selbstverständlich unter Geheimhaltung weiterentwickelt, die Internettechnologie dagegen ist für den Dual Use freigegeben: Die Technologiefirmen der USA sollten zusehen, was sich daraus geschäftlich machen lässt. Und das war einiges.

Der Siegeszug des Internets verdankt sich wie jeder technologische Fortschritt im Kapitalismus dem Umstand, dass es sich als Mittel des Geschäfts bewährt. Produzierende Unternehmen verkürzen durch die Nutzung von Onlineabsatz- und Beschaffungsmärkten die Zirkulationszeit ihres Kapitals, das sich somit öfter profitbringend umschlagen lässt. Sie errichten verteilte Produktionsstätten weltweit, die sie vom Heimatstandort rund um die Uhr steuern, binden Zulieferer just in time ein, lassen Buchhaltung und Rechnungswesen im Ausland mit deutlich niedrigerem Lohnniveau erledigen. Handelsunternehmen mindern den Aufwand für den Weg zum Kunden, indem sie ihre bisherigen Vertriebswege durch virtuelle Kaufhäuser ergänzen oder ersetzen, und erschließen sich damit gleich die ganze Welt als Markt. Finanzunternehmen schieben Aktien, Devisen, Derivate auf Finanzplätzen aller Kontinente in Sekundenbruchteilen hin und her und machen die elektronisch ermöglichte Geschwindigkeit der Reaktion zu einer neuen Gewinnquelle. Das Internet verallgemeinert sich darüber zum Standard der ökonomischen Konkurrenz: Keine Geschäftssphäre kann sich dem entziehen. Letztlich muss selbst das Handwerk im Netz »drin« sein.

Der Zugang zum Netz und die Übertragung der Daten in ihm ist die Geschäftssphäre der Internetprovider. Sie betreiben seinen Ausbau im industriellen Maßstab mit immer schnelleren, leistungsfähigeren, für immer größere Datenmengen geeigneten Übertragungsmethoden. Das alle Nationen überspannende Internet ist das Werk der großen US-amerikanischen Telekomunternehmen und einiger anderer aus anderen Zentren des Kapitalismus: Sie bilden das Rückgrat, das sie im Zusammenschluss ihrer Netze herstellen und um dessen Ausnutzung sie konkurrieren. Nationale, regionale und lokale Provider vervollständigen die materielle Infrastruktur des World Wide Web im globalen Kapitalismus, das noch den letzten Erdwinkel erschließt und einbezieht, sofern es sich lohnt.

Darauf bauen die eigentlichen Internetdienstleister Google, Apple, Facebook und Co. auf. Google verlinkt mit seiner Suchmaschine die ganze Welt, verschafft jedem User Zugriff auf Informationen aller Art und der interessierten Geschäftswelt Zugang zu einem virtuellen Weltmarkt. Die Firma baut ihr Geschäftsmodell durch weitere Internetdienste, vom E-Mail-Konto über Cloudspeicher und Videostreaming bis zur digitalen Kartographie des Globus immer weiter aus. Der Teil der Menschheit, der sich im Netz tummelt, soll in Google-Diensten gefangen bleiben. Darüber werden fleißig Daten gesammelt, zu Kundenprofilen aufbereitet, als Marktchancen ausgewertet. So oder so ähnlich kämpfen alle Internetkonzerne um die Monopolisierung ihrer Zugriffsmacht auf die globale Gemeinde der User und Konsumenten, die sie mit dem Netz stiften.

Bedürfnis nach Abschottung

Für die Staaten wird das Internet zum unentbehrlichen Mittel der Verwaltung, Steuerung und nicht zuletzt der Kontrolle der Gesellschaft. Sie organisieren und überwachen die Infrastruktur ihrer Länder – Stromerzeugung und Verteilung, Wasserversorgung, Krankenhäuser, Bahnen, die Verkehrslenkung – elektronisch über das Internet. Polizei und Justiz werden vernetzt, betreiben für ihre Zwecke eigene Datenbanken und effektivieren damit die Kontrolle der Gesetzestreue der Bürger. Im Netz kann der Staatsschutz anhand der Mails, Foren und Chatrooms überprüfen, was die Regierten so denken und wollen. Dagegen waren frühere Eingriffe ins Briefgeheimnis ein Witz. Die militärische Nutzung des Internets wurde ohnehin fortgesetzt. Elektronisch gesteuerte Tötungsautomaten nutzen neben dem Satellitenfunk das Mobiltelefon deklarierter Feinde als Mittel zur Zielerfassung. Summa summarum hängen heute das ganze Innenleben kapitalistischer Nationen, die Erfolge ihrer Kapitalisten auf dem Weltmarkt und der Einsatz ihrer Macht nach außen technologisch am weltweiten Netz.

Diese Bilanz ist ganz im Sinne des Erfinders. Die Geschäftssphäre ist fest in der Hand von US-Konzernen: Intel und AMD liefern Chips für die Rechner, Microsoft bietet Betriebssysteme für PC und Rechnernetzwerke, Google Software für mobile Endgeräte sowie Suchmaschinen, Cisco Router und Switches für die Verknüpfung zur Netzwerkinfrastruktur, IBM Hochleistungsrechner und Oracle Datenbanken – alles, was es technisch für das Netz und die Verarbeitung massenhafter Daten braucht, ist Verkaufsschlager von US-Firmen, die nicht nur den Heimatmarkt damit vollstopfen, sondern an Aufbau und Nutzung des Netzes in aller Herren Länder verdienen.

Wo Raum und Zeit als Schranke kapitalistischer Ausnutzung von Land und Leuten zwar nicht gänzlich beseitigt, aber deutlich relativiert werden, da sind US-Konzerne die entscheidenden Anbieter und Organisatoren der nötigen Technik, die ihren Vorsprung gegenüber der Konkurrenz immer weiter zum Monopol ausbauen. Und das verschafft den USA eine neue strategische Position: Weltweit alle Staaten, die das Netz so ausgiebig nutzen, sind in der Pflege ihres Kapitalstandorts von den Leistungen amerikanischer IT-Firmen abhängig, die ihrerseits unter dem Recht und der Kontrolle der Vereinigten Staaten stehen.

Doch so sehr die wunderbare Transparenz des Internets für die Unternehmen das Medium zur Austragung ihrer Konkurrenz ist, so sehr ist sie, gerade deshalb, auch ein Problem. Die Kommunikation, intern wie mit den Geschäftspartnern, soll vor den Konkurrenten gerade geschützt sein, nur dann ist sie unter kapitalistischen Gesichtspunkten tauglich. Aber auch Nichtkapitalisten haben im Kapitalismus gute Gründe fürs Geheimhalten von Wohnadresse, Freizeitinteressen oder Gesundheitsdaten. Alles hinterlässt Spuren im Netz, soll aber nicht von jedermann gefunden werden. Das Bedürfnis nach Exklusivität des Zugriffs, nach Abschottung der eigenen Daten schafft bei anderen wieder das Bedürfnis, letztere auszuhebeln. Nicht nur, um an die Pläne der Konkurrenz heranzukommen, sondern auch zwecks Störung, z. B. durch gezielte Lahmlegung von fremden Servern oder zwecks betrügerischer Nutzung fremder Kreditkartendaten.

Den Abschottungsbedarf bedient die IT-Branche mit hierarchisch differenzierten Zugangsbe-

utige Kriegführung nicht mehr ohne die Nutzung des

rechtigungen, Firewalls und Verschlüsselungsprogrammen – und für deren Überwindung bietet sie geschäftsmäßig im »Darknet« massenhaft Viren, Würmer, Trojaner etc. oder gleich ganze gekaperte Netzwerke an. Darauf baut wiederum das Geschäft mit dem Auffinden von Sicherheitslücken und Maßnahmen dagegen auf. Gerne lassen sich dafür auch Hacker einspannen, denen nichts über die Hoheit des Bürgers über dessen Daten geht. Der Kampf um die Infiltration des Netzes bzw. deren Verhinderung geht so weit, dass er dessen technische Intaktheit immer wieder in Frage stellt.

Angesichts dieses Treibens sieht sich ein Staat wie die BRD als Aufsichts- und Regelungsmacht gefordert, die Interessengegensätze zu regeln und auch dieser Sphäre eine kapitalistische Rechtsordnung zu verpassen. Er erklärt Daten zum Privateigentum, spendiert den Bürgern ein »Recht auf informationelle Selbstbestimmung« und scheidet damit die laufende Erzeugung und Beschaffung von Daten und Programmen in erlaubte und verbotene Formen.

Mittel zur Kontrolle der Welt

Weil das Netz so angreifbar, gleichzeitig aber die Basis der gesamten Infrastruktur des Staates und die Existenzbedingung seiner Gesellschaft ist, also seine Souveränität daranhängt, belässt der Staat es nicht dabei, Übergriffe zu ahnden, sondern stellt das Netz unter seine Kontrolle. Er verpflichtet die Privatwirtschaft, Cyberattacken zu melden, schafft ein »Bundesamt für Informationssicherheit«, das über die gerade virulenten Viren informiert und kümmert sich speziell um die IT-Sicherheit der national wichtigen »kritischen Infrastrukturen«. Sich selbst genehmigt er natürlich praktisch unbeschränkten Zugriff auf den Datenverkehr, samt Bundestrojaner und Vorratsdatenspeicherung.

Wie ein Staat seine Gesellschaft im Netz und mittels des Netzes kontrolliert, so verfahren die USA mit der ganzen Welt. Sie machen sich den Umstand zunutze, dass sich der nationale Innenraum der Staaten nicht mehr von seiner Außenwelt abschotten lässt, wenn Geschäftsverkehr und Alltagsleben flächendeckend über das Internet organisiert und abgewickelt werden. Die Supermacht ergreift die Chance, die eine Internationalität des Netzes bietet, um die souveräne Verfügung anderer Staaten über Land und Volk, diese elementare Bestimmung politischer Herrschaft, aufzuweichen und sich umfassend in fremde Souveränität einzunisten.

Das kann sie, weil die Technologie für das Netz und seinen Betrieb weitgehend von US-Konzernen stammt. Ihr Staat verpflichtet sie, mit seinen Geheimdiensten zu kooperieren, nicht nur auf dem eigenen Hoheitsgebiet, sondern überall, wo sie ihre Technik installieren oder selbst Internetkabel, Knotenpunkte, Server und Datenbanken betreiben. Mit der NSA und anderen Diensten hat er sich einen Riesenapparat geschaffen, den weltweiten Datenverkehr mitzuschneiden und auszuwerten. Zudem sorgt er dafür, dass ihm dieser Zugriff erhalten bleibt bzw. er weiter perfektioniert wird. Die NSA testet Hochleistungsrechner, Netzwerkkomponenten und Software von US-Herstellern, bevor sie auf den Markt kommen. So bleibt bei jedem Stück neuer Internettechnik der Vorsprung der US-Dienste vor der Konkurrenz gewahrt: Sie wissen über Sicherheitslücken und Einfallstore Bescheid, bevor der Rest der Staatenwelt die technischen Neuheiten daraufhin inspizieren kann. Mindestens 2000 solcher »Backdoors« sollen der NSA zu Gebote stehen.

Washington lässt sich sogar seine Kontrollmacht – technisch von kriminellen Machenschaften nicht zu unterscheiden, aber rechtlich voll abgesegnet – von seinen Konzernen gleich in Hard- und Software made in USA einbauen, bis hin zu gegen Antivirenprogramme resistenter Malware, die auch das Neuformatieren von Festplatten oder Neuinstallieren von Betriebssystemen übersteht. Mit Viren, Würmern und Trojanern produzieren die NSA und ihre Helfer digitale Waffen, mit denen die Vereinigten Staaten Rechnernetzwerke, Internetknoten oder elektronisch gesteuerte Industrieanlagen in den Griff bekommen und gegebenenfalls lahmlegen.

Damit geraten die USA in den Rang einer übergeordneten Souveränität, die über die ökonomischen, politischen und militärischen Anstrengungen fremder Staaten Bescheid weiß, gegebenenfalls vorsorglich eingreifen kann und das auch tut. Mit dem 2010 entdeckten Computerwurm Stuxnet, der die Leittechnik der Urananreicherungsanlage in Natanz störte, haben sie das am Iran vorexerziert. Seit den Enthüllungen des ehemaligen CIA-Mitarbeiters Edward Snowden weiß die Welt über die strategische Vorgabe des Pentagon Bescheid, »kritische Systeme« anderer Länder »nach Belieben kontrollieren/zerstören« zu können. Die USA können also vermöge des Internets fremde Staaten lahmlegen, wenn ihre Interessen das gebieten, ohne das Militär loszuschicken. Sie können jenseits aller politisch-diplomatischen Wege, den Willen des anderen Souveräns per Angebot und Erpressung zu beeinflussen, in dessen Herrschaftsbereich hineinwirken (was sich dann natürlich wiederum für Drohung und Erpressung nutzen lässt). Die anderen Staaten sehen sich damit einer Bedrohung gegenüber, gegen die sie nichts tun können, oder sind einem Angriff ausgesetzt, den sie vielleicht, wie im Fall des Irans, nicht einmal bemerken oder zuordnen können.

Allerdings ist das Netz keine Einbahnstraße. Es gestattet Kommunikation in beide Richtungen, erlaubt auch anderen Zugriff auf Informationen und Eingriff in Datenbanken. Die USA sehen damit ihren Monopolanspruch in Frage gestellt. Die geschätzten technischen Eigenarten des Netzes – es gewährt Zugang von jedem Punkt der Erde aus, verrät die Identität des Absenders nur unzureichend durch eine IP-Adresse, gesendete Daten finden über autonome Wege zum Ziel – sehen sie als Ensemble von Sicherheitsrisiken. Letztlich ist jeder User ein mögliches Einfallstor, ein trojanisches Pferd, einer, der auf Land und Leute von außerhalb der Reichweite US-amerikanischer Macht zugreifen könnte. Jede stattgefundene Attacke auf US-Daten gilt als nationale Katastrophe, gegen welche die Heimatfront aufzurüsten ist.

Für die Organisation der Abwehr von Einblicken und Eingriffen, wie die USA sie sich gegen den Rest der Welt herausnehmen, werden nicht nur alle einschlägigen Sicherheitsorgane mobilisiert und zur Zusammenarbeit verpflichtet. Auch der private Sektor der Wirtschaft muss sich erklären lassen, dass er »die vordere Front der Verteidigung« ist – schließlich betreibt er über 90 Prozent des Netzes – und wird entsprechend in die Pflicht genommen: Firmen müssen Cyberattacken nicht nur melden, sondern aktiv mithelfen beim Sammeln und Sortieren von Adressen und Verbindungen. Dafür werden sie von (unter Umständen sehr teurer) privatrechtlicher Haftung für die patriotische Weitergabe von Daten befreit. All das dient einem rein militärischen Zweck: der Ausschaltung des Gegners. Alle Ziele, die die USA über das Netz in Sachen Ausforschung, Kontrolle und Unterwerfung der Staatenwelt verfolgen, und alle Mittel, die sie dafür einsetzen, kehren unter dem gar nicht bloß ideologischen Titel »Verteidigung gegen Cyberattacken« wieder. Tatsächlich ist ohne die Sicherstellung der Unangreifbarkeit der Heimatfront das Monopol auf Kontrolle im Netz und die freie Handhabbarkeit der dafür nötigen Waffen nicht zu haben.

Den Rivalen lahmlegen

Dieser Sicherheitsanspruch der USA verträgt keine Rivalität, keine Versuche anderer, sich deren Herrschaft über das Netz zu widersetzen. So gesehen verteidigen die Vereinigten Staaten immerzu nur ihren Netzfrieden bzw. reagieren immer bloß auf Angriffe anderer, auch nichtstaatlicher oder gar einzelner Akteure, die sich auf dem Schwarzmarkt die Malware für ihre asymmetrischen Attacken besorgen. Auf Angriffe reagieren sie mit Strafaktionen – Nordkorea, dem sie Ende 2014 eine unanständige Cyberattacke auf Sony vorwarfen, stellten sie mal eben für ein paar Tage das Netz ab; gegen chinesische Offiziere, die sie für einen zum Risiko für die »strategische Stabilität« erklärten »Diebstahl geistigen Eigentums« verantwortlich machen, erheben sie Anklage.

Die Kriegsgründe für den Cyberwar scheinen – wie auch beim konventionellen Krieg – immer nur in den Waffen zu liegen, die der Feind hat. Und der scheint Feind nur zu sein, weil er sie hat. Einerseits korrigiert die Liste der »key cyber threats«, die von den USA ins Visier genommen werden, der Eindruck von Defensive und Beschränkung auf den Cyberspace, der da erweckt wird: Sie ist nämlich identisch mit der Liste der Machtrivalen und Feinde, die US-Amerika auch in der analogen Welt hat; an denen also nicht nur stört, dass sie Cyberwaffen besitzen. Andererseits – und das ist die Wahrheit der defensiven Ideologie: In letzter Instanz wird ein anderer Staat mit seinem eigenen Willen und seinen Interessen nur dadurch zum unerträglichen Feind, dass er sich Mittel zulegt, um sich dem Diktat der Vormacht zu widersetzen.

Weil die Netzkontrolle nie fertig und lückenlos ist und der Rest der Welt sie sich nicht zuverlässig gefallen lässt, untermauert das US-Verteidigungsministerium sie in seiner Erklärung zur Cyberstrategie von 2015 mit einer förmlichen Kriegsdrohung: »Die Vereinigten Staaten werden fortfahren, auf Cyberattacken gegen US-Interessen zu einer Zeit, in einer Art und Weise und an einem Ort unserer Wahl mit angemessenen Instrumenten der US-Macht und in Übereinstimmung mit den einschlägigen Gesetzen zu antworten.« Sie erklären den Cyberspace zum nationalen Sanktuarium, also zum US-amerikansichen Zuständigkeitsgebiet. Und sie stellen klar, dass Cyberwar kein auf das Netz begrenzter, bloß virtueller Krieg ist, Attacken auf den virtuellen Raum ihnen vielmehr einen richtigen Krieg mit allen Waffengattungen und in allen Räumen wert sind, in denen sie militärische Gewalt entfalten. Auch umgekehrt stellen die Erklärungen zur Militärdoktrin klar, dass jede Trennung von Cyberwar und klassischem Krieg abseitig ist: Das Ministerium »hat Fähigkeiten zu Cyberoperationen entwickelt und ist dabei, diese Fähigkeiten in das gesamte Arsenal von Mitteln einzubauen, die die US-Regierung benutzt, um nationale Interessen zu verteidigen; dazu gehören diplomatische, informelle, militärische, ökonomische, finanzielle und polizeiliche Mittel«. Im Krieg der Zukunft wird es darauf ankommen, über das Internet die Infrastruktur der Heimatfront des Gegners lahmzulegen, seine militärische Kommunikation zu stören, die Steuerung seiner Schiffe, Raketen, Satelliten zu übernehmen und gegen ihn zu wenden. Krieg findet nicht mehr nur zu Lande, zu Wasser, in der Luft und im Weltraum statt, sondern auch im Cyberspace, dem »fünften Kriegsschauplatz« – und dort für die vier anderen.

Konkurrenz im Cyberspace

Der Anspruch und die Praxis der USA, die übrige Staatenwelt auszuforschen, ihrer Kontrolle zu unterwerfen und gleichgelagerte Versuche anderer mit einer Kriegsdrohung zu beantworten, führen in einer imperialistisch geordneten Welt zur logischen Konsequenz: Während die meisten der fast 200 Staaten aus Mangel an Geld und technischen Fähigkeiten der US-amerikanischen Oberaufsicht einfach ausgeliefert sind, strengen sich die interessantesten Objekte des Zugriffs, die potenten Partner und die weltpolitischen Rivalen, an, es den USA gleichzutun.

Berlin versucht, teils mit Brüssel, den USA den Zugriff auf deutsche/europäische Daten zu erschweren. Die Bundesrepublik hat ein »Cyberabwehrzentrum«, in dem alle relevanten Behörden und Staatsschutzorgane zusammenarbeiten. Daneben hat sich die Bundeswehr noch eigene Cyberstreitkräfte zugelegt. Alles natürlich unter dem Titel »Verteidigung« und »Abwehr«. Dabei ist es kein Geheimnis, dass die Fähigkeit, Attacken im Netz zu detektieren und die Funktionsweise von Schadprogrammen zu analysieren, gleichbedeutend ist mit der Möglichkeit, dergleichen auch zu konstruieren und einzusetzen. Über den Unterschied von Möglichkeit und Wirklichkeit braucht dabei niemand zu spekulieren: Es ist offiziell, dass der Auslandsgeheimdienst der Kanzlerin noch viel enger »befreundete« Partner als die USA, nämlich die wichtigsten Mitglieder ihrer Europäischen Union nicht weniger schamlos ausforscht als die NSA die BRD.

In China sind in staatlichen Behörden nur noch national gefertigte Computer gestattet. Zugleich wird Huawei zum schlagkräftigen Konzern für Netzwerktechnologie aufgerüstet, als Angebot an andere Länder, sich aus der Abhängigkeit von den USA zu befreien – und um so selbst möglichst in deren Position zu kommen. Russland, das es bis zur Manipulation der US-Präsidentschaftswahlen gebracht haben soll, sieht seine Souveränität vom US-Zugriff auf seine Netze so bedroht, dass Wladimir Putin sich vom Parlament einen »Kill Switch« genehmigen lässt, nämlich die Befugnis, die Internetverbindungen in der Russischen Föderation abzuschalten, um einem befürchteten ernsten Angriff die Wirkung zu nehmen. Zugleich wälzt man Pläne, ein russisches Internet mit möglichst viel eigener Technik ganz neu aufzubauen.

Für alle Konkurrenten der USA gilt: Wer das Netz selbst als nationales Machtmittel nutzen will, darf nicht angreifbar sein. Darüber bekommt dieser ganze Sektor neuer Technologie einen strategischen Charakter. Datenbanken, Netzwerkknoten, Serversoftware, alles ist nicht nur Gebrauchs- und Geschäftsmittel im zivilen Leben, sondern zugleich Waffe. Insbesondere an den technologischen Fortschritten in dem Sektor hängt die militärische Schlagkraft der Nation. Unter dem Aspekt dieses »Dual Use« bekommt auch das deutsche Großprojekt »Industrie 4.0« einen über die ökonomische Konkurrenz hinausweisenden Stellenwert: Es geht darum, die Welt mit deutschen Standards sowie deutscher Soft- und Hardware für das »Internet der Dinge« auszustatten, sich damit für die industrielle Konkurrenz möglichst vieler Nationen möglichst unverzichtbar zu machen und deren Technologieabhängigkeit für das Implantieren deutscher Kontrollmöglichkeiten zu nutzen. Das ist der deutsche Einstieg ins digitale Wettrüsten.

■ Theo Wentzke ist Redakteur der Zeitschrift *Gegenstandpunkt*. Zuletzt erschien von ihm an dieser Stelle am 31. März ein Beitrag über das »Elend des deutschen Trade-Unionismus«

■ Eine umfangreichere Fassung dieses Artikels findet sich im Heft 1/2017 der Zeitschrift *Gegenstandpunkt*. Bestellung unter www.gegenstandpunkt.com/gspbest.html

■ **Lesen Sie morgen auf den *jW*-Themaseiten:**

Streit um Nachlass. Wem gehören die Fotografien des KZ-Häftlings Francisco Boix?

Von Ruth Perez-Chaves und Carmela Negrete