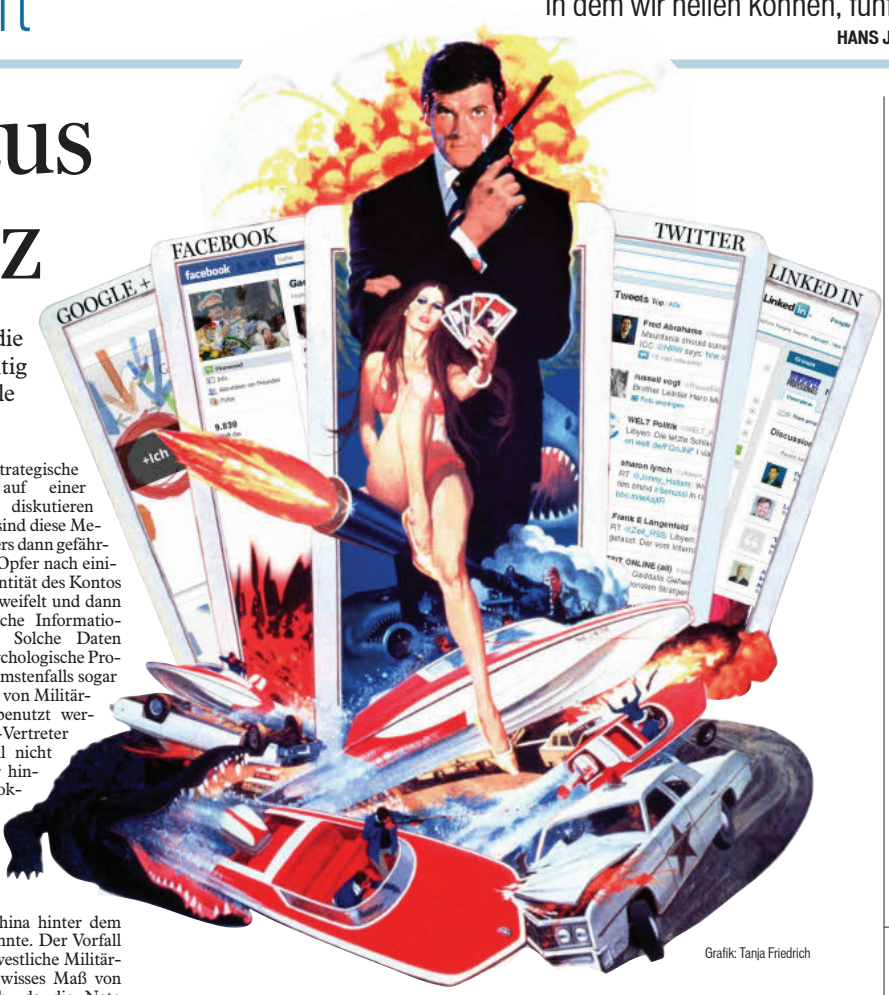
Wissenschaft

„Ich glaube, dass ein realistischer Zeitraum, in dem wir heilen können, fünf Jahre sind."
HANS JÄGER, AIDS-EXPERTE

Spione aus dem Netz

INTERNET Das digitale Zeitalter hat die Welt der Nachrichtendienste nachhaltig verändert. Spione nutzen heute soziale Netzwerke für viele Operationen.



Grafik: Tanja Friedrich

VON UNSEREM MITARBEITER **ROMAN GOERGEN**

Toronto – Das romantische Klischee des Spions kämpft um sein Überleben. Die Ära des Agentenaustauschs auf nebligen Berliner Brücken, der konspirativen Übergabe von Aktenordnern an dunklen Straßenecken und Erpressungsversuchen mit kompromittierenden Fotos verschwindet zusehends in das Reich von John le Carré-Romanen. Die Agenten des Cyber-Zeitalters tummeln sich stattdessen auf sozialen Netzwerken.

Der Fall des Nato-Admirals James Stavridis hat nun auch die Öffentlichkeit auf diesen Umstand aufmerksam gemacht. Stavridis ist einer der höchstrangigen Militärvertreter der westlichen Welt. Die britische Zeitung „Sunday Telegraph" hatte in der vergangenen Woche enthüllt, dass die Spionageabwehr der Nato auf ein gefälschtes Facebook-Konto gestoßen war, das den Namen des Admirals trug. Von diesem Konto aus seien gezielt Freundschaftsanfragen an Führungspersönlichkeiten in den Rängen des europäischen Militärs verschickt worden.

Der Vorgang, bei dem Informationsdiebe gefälschte Online-Profile anlegen, um Anderen vorzugaukeln, es handele sich um eine ihnen bekannte Person, wird „spear phishing" genannt. Bei der Nato wurde sofort versichert, dass keiner der attackierten Militärs strategische Geheimnisse auf einer Facebook-Seite diskutieren würde. Jedoch sind diese Methoden besonders dann gefährlich, wenn das Opfer nach einiger Zeit die Identität des Kontos nicht mehr anzweifelt und dann mehr vertrauliche Informationen preisgibt. Solche Daten könnten für psychologische Profile oder schlimmstenfalls sogar zur Erpressung von Militärgeheimnissen benutzt werden. Nato-Vertreter wollten offiziell nicht bestätigen, wer hinter der Facebook-Operation stehen könnte. Allerdings spekulierte der Telegraph darüber, dass China hinter dem Fall stecken könnte. Der Vorfall bringt für das westliche Militärbündnis ein gewisses Maß von Ironie mit sich, da die Nato selbst versucht, sich soziale Netzwerke zunutze zu machen. Auf Facebook und Co. angesprochen, betont ein Nato-Sprecher: „Sie haben eine wichtig Rolle in unseren Operationen in Libyen gespielt. In ihnen hat sich die Zunahme von öffentlicher Opposition widergespiegelt. Gleichermaßen konnten wir darüber die Truppenbewegungen der Streitkräfte des Regimes verfolgen."

> *„Die sozialen Netzwerke haben eine wichtig Rolle in unseren Operationen in Libyen gespielt.*
>
> Ein Sprecher der Nato

Israel und der Iran

Im Sommer vergangenen Jahres nutzte das Bündnis Echtzeit-Einträge libyscher Blogger auf dem Netzwerk Twitter, sogenannte „Tweets", um Gaddafi-Truppen aufzuspüren und zu bombardieren. Die Twitter-Informationen waren dabei besonders wertvoll, weil das Uno-Mandat für Libyen keine Bodentruppen gestattete und die Nato daher auf alternative Beobachtungen aus nächster Nähe angewiesen war.

Solche Berichte bestätigen nach Einschätzung von Joseph Fitsanakis und Micah-Sage Bolden einen signifikanten Trend: Für Nachrichtendienste, egal ob militärisch oder zivil, ist die Arbeit ohne Rückgriff auf soziale Netzwerke nicht mehr möglich. Die beiden amerikanischen Politologen veröffentlichten erst im Februar eine Studie, die den Umgang der internationalen Agenten mit sozialen Netzwerken untersucht. Sie stützen ihre Einschätzung dabei auf drei Fallstudien: die Revolutionen des „arabischen Frühlings", den libyschen Bürgerkrieg und Israels Operationen gegen Gaza-Aktivisten. Laut Fitsanakis habe besonders der arabische Frühling die US-Regierung dazu veranlasst, „Richtlinien zu entwickeln, wie taktisch relevante Informationen aus sozialen Netzwerken gewonnen werden können". Allerdings zeigten Ereignisse in Israel auch, wie Aktivisten in solchen Medien nicht nur ermutigt, sondern auch bekämpft werden können. Während der von europäischen Gruppen organisierten „Willkommen in Palästina"-Solidaraktion war der israelische Geheimdienst seinen Gegnern stets einen Schritt voraus. Jegliche Online-Aktivität und geplante Proteste waren den Staatsbehörden dank deren eigener Präsenz auf Facebook und Twitter genau bekannt.

Experten wie Fitsanakis betonen auch, dass die Öffentlichkeit sich die Arbeit von Nachrichtendiensten oft falsch vorstelle und annehme, dass es vornehmlich um das „Ausschnüffeln von Geheimnissen" gehe. Stattdessen sei ein großer Teil der Arbeit schlichtweg das Auswerten von frei zugänglichen Informationen, was im Fachjargon als „open sourcing" bezeichnet wird. Und dazu seien soziale Netzwerke eine geradezu „endlose Fundgrube".

CIA liest Millionen Tweets am Tag

Das hat auch die CIA erkannt und deswegen ihr „Open Source Center" (OSC) ins Leben gerufen. Der US-Geheimdienst beschäftigt nach eigenen Angaben mehrere hundert mehrsprachige Datenanalysten, die täglich unzählige öffentlich zugängliche Informationsquellen durchkämmen. Die Relevanz von sozialen Netzwerken wurde den OSC-Experten besonders 2009 bewusst. Denn auch während der „grünen Revolution" im Iran nutzen Regimegegner vor allem Facebook und Twitter, um ihre Proteste zu organisieren. Als Reaktion zu den Ereignissen im Iran hat die CIA technische Kapazitäten erhöht. Die Datenverwerter des Geheimdienstes im OSC sollen derzeit schon in der Lage sein, täglich fünf Millionen Tweets zu überwachen. Die Schreibtisch-Agenten verfassen regelmäßige Berichte über die öffentliche Meinung rund um den Globus, die sich auf Facebook, Twitter und Blogs stützen – eine Zusammenfassung, auf die Präsident Barack Obama gerne und oft zurückgreift. Zur Veranschaulichung der Relevanz berichtet OSC-Direktor Doug Naquin, dass seine Analysten vorhergesagt hatten, dass „soziale Netzwerke in Ägypten zu einem entscheidenden Faktor werden und eine Bedrohung für das Regime darstellen".

TIERSEUCHE

Erreger ist identifiziert

Antwerpen – Belgischen Wissenschaftlern ist es gelungen, die Überträger des für Rinder, Ziegen und Schafe gefährlichen Schmallenberg-Virus zu identifizieren. Es handle sich um Mückenarten, die auch die vor fünf Jahren grassierende Blauzungenkrankheit übertrugen, teilte das Institut für Tropenmedizin in Antwerpen am Freitag mit. Der Erreger sei in den Gnitzen-Arten Culicoides obsoletus, C. dewulfi und C. pulicaris nachgewiesen worden - drei der fünf Arten, die auch die Blauzungenkrankheit übertrugen. Die Erkrankung war im November 2011 erstmals bei Tieren aus dem kleinen Ort Schmallenberg von Forschern des Friedrich-Loeffler-Instituts beschrieben worden. Das Virus gehört zur Gattung der Orthobunyaviren. Andere Erreger aus dieser Gruppe wie der Blauzungenerrege werden auch von Stechmücken übertragen. In Deutschland wurde der Schmallenberg-Erreger inzwischen in 980 Betrieben nachgewiesen. Er führt während der Trächtigkeitsphase zu Missbildungen bei den Föten sowie Totgeburten. *dpa*

ASTRONOMIE

Ein Teleskop für extreme Zeitreisen

Kapstadt – Das Radioteleskop SKA soll alle vorangegangenen Geräte weit übertreffen. Nach aktueller Planung wird es aus mehreren Tausend Einzelteleskopen bestehen, die über Glasfaserkabel verbunden sind. SKA steht für „Square Kilometre Array" . Die Teleskope sollen über mehrere Länder verteilt werden. Wissenschaftler hoffen, bis zu 13 Milliarden Jahre zurück in die Vergangenheit des Universums lauschen zu können – also fast bis zum Urknall. Australien und Südafrika bieten sich als Standorte an, weil große Flächen mit wenig störenden Radiointerferenzen benötigt werden. Mehr als 70 Institute in 20 Ländern und Partner aus der Industrie sind beteiligt. SKA soll im Jahr 2016 starten. *dpa*