Denkwürdigkeiten

Journal der Politisch-Militärischen Gesellschaft

Nr. 70
Februar 2011

Herausgegeben vom Vorstand der Politisch-Militärischen Gesellschaft e.V. (pmg) in Berlin

ISSN 1436-3070

LEADOFF

Liebe Mitglieder,

nicht nur im Iran und im Irak, im Cyberspace und bei der Neuausrichtung der Bundeswehr ist es spannend. Der Beitrag vom 27. Januar aus Kairo vermittelt eindrucksvoll die brisante Entwicklung vor Ort.

In einem Gespräch mit einem militärischen Kameraden in Kairo erfuhr ich gestern früh, wie er die vorangegangene Nacht verbracht hatte: er stand mit anderen Freiwilligen und einem Knüppel in der Hand und beschützte das "Compound", in dem er mit seiner Familie wohnt, vor Übergriffen von freigelassenen Schwerverbrechern aus einem Gefängnis ganz in der Nähe. Trotz mehrerer Gewaltdelikte in unmittelbarer Nachbarschaft ging es für ihn und seine Familie gut. Sie befinden sich inzwischen sicher in Deutschland.

Unsere besten Wünsche begleiten in diesen herausfordernden Tagen unsere Freunde, Kameraden und deren Familien in Kairo, ebenso das ägyptische Volk, dem wir die Kraft und Einsicht für einen friedlichen Weg zu mehr Demokratie wünschen.

Ralph Thiele, *Vorstandsvorsitzender*

In dieser Ausgabe

THEMEN

Der Freitag des Zorns und seine Nachwirkungen

Trotz Demonstrationsverbot wurden am Mittwochnachmittag (26.01.) und am Abend die Proteste in Ägypten fortgesetzt. Vor allem in Kairo und Suez kam es zu gewalttätigen Zusammenstößen. In Kairo kamen dabei ein Polizist und ein Demonstrant ums Leben. Damit stieg die Zahl der Toten auf sechs, vier Demonstranten und zwei Polizisten.

Gestern kam es in Suez (vor dort wird wenig bis gar nichts berichtet) zu schweren Zusammenstößen. Die mehrheitlich jugendlichen Demonstranten fordern den Rücktritt von Präsident Mubarak und werden dabei von den Vorgängen in Tunesien inspiriert.

Unbestätigten Berichten zufolge soll Gamal Mubarak mit Familie und seine Mutter, Suzanne Mubarak, das Land verlassen haben und sich in London aufhalten. Der Generalstabschef befindet sich in Washington zu Gesprächen.

Mohamed ElBaradei, Reformpolitiker und früherer Chef der IAEA, will heute aus Wien nach Ägypten zurückkehren. Er könnte ein möglicher Gegenkandidat bei der Präsidentenwahl im Herbst zu Mubarak sein.

Die Demonstrationen am Mittwoch (26.01.) erreichten zwar nicht die Stärke vom Vortag, aber sie sind eine klare Warnung an Präsident Mubarak. Landesweit wurden nach Behördenangaben 860 Demonstranten festgenommen. Die meisten von ihnen sollen Angehörige der Moslembruderschaft sein. Ihnen wirft das Regime vor, Ausgangspunkt der Gewalt zu sein.

Trotz der Androhung von Verhaftungen durch das Innenministerium gingen am Mittwoch (26.01.) wieder zahlreiche Menschen (bei weitem aber nicht so viele wie am Dienstag) landesweit auf die Straßen. In Kairo forderten ca. 1.500 Demonstranten ein Ende der Herrschaft von Hosni Mubarak. Obwohl die Behörden zuvor die Internetdienste Facebook und

Twitter lahmgelegt hatten, gelang es den mehrheitlich jugendlichen Demonstranten ihre Aktionen untereinander abzustimmen – sie verständigten sich über SMS. Die Polizeigewalt (Wasserwerfer und Tränengas) von Dienstagabend wiederholte sich und wurde verschärft. Es gibt Berichte wonach die Polizei Rubber-Bullets einsetzte. Die zahlreich eingesetzten „zivilen" Muchabarat (Geheimdienstleute) führten laufend einzelne Demonstranten ab und verfrachteten sie in bereitgestellten Polizeitransporter.

Die Polizeigewalt machte auch vor Journalisten nicht halt. Es gibt Meldungen der Organisation „Schutz für Journalisten", dass mindesten 12 Medienvertreter angegriffen, ihre Ausrüstung (Kameras, Mobiltelefone, etc.) konfisziert und sie selbst zum Teil verprügelt wurden. Bis zum Abend wurden zwei neue Tote gemeldet. Für den 28. Januar, nach dem Gebet, wurde im Internet zum „Freitag des Zorns" aufgerufen.

Das Regime versucht, die Protestbewegung zu diskreditieren, indem sie die Moslembruderschaft (MB) beschuldigt, für die Gewalt verantwortlich zu sein. MB-Mitglieder sollen demnach Steine auf Polizisten geworfen und öffentliches Eigentum beschädigt haben. Die MB hat jedoch nicht zur Teilnahme an den Demonstrationen aufgerufen. Es waren prominente säkulare Oppositionelle wie die frühere IAEA-Chef Mohammad ElBaradei und der Schriftsteller Alaa Aswany, die die Kundgebungen unterstützten, selbst daran aber nicht teilnehmen.

Aswany – in seinem Bestseller „Das Yacoubian Haus" klagt er die Korruption und die Brutalität der Polizei in Ägypten an – lobte die Jugendlichen, weil sie die „Barriere der Furcht" durchbrochen hätten.

Die Mit-Organisatoren der Kundgebungen sind unter anderem auch die säkulare Jugendgruppe „Bewegung des 6. April".

In der Nacht von Dienstag auf Mittwoch kam es in Kairo zu blutigen Zusammenstößen zwischen Polizei und Demonstranten, als die Sicherheitskräfte begonnen hatten den Tahir-Platz um ca. 01:30 Uhr Ortszeit zu räumen. Viele Demonstranten hatten sich bereits für eine Übernachtung eingerichtet, wurden aber „vertrieben". In der Nähe des Nationalmuseums wurde ein Polizeiwagen angezündet und Demonstranten verbarrikadierten sich auf einigen Brücken über den Nil.

In Suez wurden am Dienstagabend drei Menschen getötet, in Kairo kam ein Polizist um. Darauf untersagte das Innenministerium mit sofortiger Wirkung jegliche Straßenproteste und öffentlichen Zusammenkünfte. Offiziell wurden landesweit 860 Demonstranten festgenommen, 250 Demonstranten und 103 Polizisten verletzt.

Ägyptische Internetseiten berichteten am Mittwoch, Gamal Mubarak habe mit seiner Familie am Dienstag das Land verlassen. Nach anderen Berichten soll auch Mubaraks Frau Suzanne nach London ausgereist sein. Für beide Meldungen liegen keine Bestätigungen vor. Ferner soll sich Generalstabschef Sami Hafiz Enan in Washington zu Konsultationen aufhalten.

Internationale Reaktionen

In Deutschland und Frankreich stößt das Demonstrationsverbot der ägyptischen Regierung auf Kritik. Außenminister Guido Westerwelle mahnte alle Seiten zu Zurückhaltung und Gewaltverzicht. Die französische Außenministerin Michele Alliot-Marie sagte, die Menschen hätten ein Recht auf Demonstrationen ohne Gewalt.

Die USA, Verbündeter und Geldgeber Ägyptens, riefen ebenfalls zur Zurückhaltung auf. Außenministerin Hillary Clinton erklärte, Mubaraks Regierung sei stabil und suche nach Wegen, die Bedürfnisse der Bevölkerung zu erfüllen.

Nach Ansicht der EU-Kommission spiegeln die regierungskritischen Proteste in Ägypten den Wunsch der Bevölkerung nach einem "politischen Wechsel" wider. Die Ereignisse in Ägypten seien ein "Zeichen" für die Hoffnungen vieler Menschen in dem Land, sagte die Sprecherin der EU-Außenbeauftragten Catherine Ashton.

Bewertung

Die Demonstranten in Ägypten orientieren sich an denen von Tunesien. Sie fordern Freiheit und echte Demokratie. Noch ist nicht absehbar, ob der Umsturz in Tunesien tatsächlich einen Dominoeffekt in der arabischen Welt haben wird. Was sich im Moment in Nord-Afrika abspielt, wirft auch die Frage nach der Haltung des Westens, auf.

Im Falle Tunesiens hat der französische Präsident Sarkozy zugegeben, dass Frankreich zu lange auf der falschen Seite gestanden und die Lage falsch eingeschätzt habe.

Im Falle Ägyptens sind es in erster Linie die USA, die in einem Zwiespalt stecken: Ägypten gilt im Nahostkonflikt und beim Verhältnis zu Israel als moderat und ist militärischer Verbündeter der USA im Antiterrorkampf. Gleichzeitig weiß Washington über die wahre innere Verfassung Ägyptens und den Charakter des Regimes Mubarak nur zu gut Bescheid.

Die Obama-Administration rief die ägyptische Regierung dazu auf, die Proteste nicht mit Gewalt niederzuschlagen. Außenministerin Clinton bezeichnete die ägyptische Regierung als gefestigt, die eine Antwort auf die legitimen Interessen und Bedürfnisse des ägyptischen Volkes finden muss.

Die Frage die die Menschen in Ägypten derzeit am meisten interessiert ist: Werden wir das tunesische oder das iranische Szenario erleben? Wird Mubarak einen Abgang à la Tunesien erhalten, oder wird die Jugendbewegung ähnlich wie im Iran unterdrückt?

Ziemlich sicher basteln die Machthaber in Kairo, vor allem aber auch das ägyptische Militär, an einer Lösung. Sie müssen sich auf die Zeit nach Mubarak vorbereiten – so oder so – und suchen wahrscheinlich nach einem geeigneten Nachfolger in den eigenen Reihen.

Um Mubarak – und seine Familie – ist es in den letzten Tagen ziemlich still geworden ist. Die Gerüchte um die „Flucht“ von Sohn Gamal mit Familie und Frau Suzanne nach London, wollen nicht abreißen. Das würde allerdings bedeuten, dass es keine Vater-Sohn-Nachfolge geben wird. Ob dann Vater Mubarak noch die Kraft aufbringen kann und bis zur Präsidentenwahl im Herbst durchhält, ist derzeit mehr als fraglich.

Es dürfen daher auch keine öffentlichen Reden und Auftritte vom Alt-Präsidenten erwartet werden. Was soll er auch noch sagen? Ankündigungen zu umfassenden Reformen glaubt ihm nach dreißig Jahren „Stillstand“ sowieso keiner mehr.

MilAttStab, Kairo

Der Beitrag gibt die persönliche Auffassung der Verfasser wieder.

THEMEN

Cybersecurity

Zur (R)Evolution unserer Sicherheit und Prosperität

Leider noch zu oft wird Cybersecurity bloß als eine technische Herausforderung verstanden, bei der es darum geht, Computer-, Informations- und Kommunikationstechnik vor zufälligen Ausfällen, Viren oder bewussten Angriffen zu schützen. Diese Betrachtung wird der Herausforderung, um die es geht, nur teilweise gerecht. Vielmehr entwickelt sich der Cyberspace [1] als Raum, der aus der Vernetzung von Computer-, Informations- und Kommunikationstechnik entsteht, zu einem der strategisch bedeutendsten Räume des 21. Jahrhunderts. Handels-, Finanz- und Informationsströme werden darüber genauso abgewickelt wie soziale Austauschbeziehungen unterschiedlichster Ausprägung. Konzepte, Technik, organisatorische Abläufe und das Handeln von Menschen müssen so aufeinander abgestimmt werden, dass es gelingt, die Vorteile des Cyberspace zu nutzen und die damit verbundenen Verwundbarkeiten[2] weitgehend einzudämmen.

Gerade für eine wirtschaftsstarke Nation wie Deutschland, die auf wissensintensive Hoch-Technologie setzt, ist Cybersecurity eine besondere Herausforderung. Deutschland profitiert von den Möglichkeiten des Cyberspace, wenn es z.B. darum geht, arbeitsteilige Prozesse weltweit zu koordinieren und wird gleichzeitig Opfer dieser Vorzüge, wenn sich Dritte auf illegale Weise über die gleiche Infrastruktur Zugang zu relevantem Know-How verschaffen wollen. Es ist diese ambivalente Natur des Cyberspace, die dazu führt, dass künftig verstärkt gemeinsame staatliche und private Sicherheitsansätze gefragt sind, um einen Interaktionsraum zu sichern, von dem Behörden, Unternehmen und Bürger gleichermaßen abhängen – zumal sich die relevante Infrastruktur mehrheitlich im Besitz privater Akteure befindet bzw. von diesen betrieben wird, was die Möglichkeit des direkten staatlichen Einwirkens tendenziell beschränkt. Den Cyberspace sicher zu machen, ist daher eine der vordringlichsten sicherheits- und wirtschaftspolitischen Aufgaben.

Wie die öffentlich-private Zusammenarbeit zum Ausbau der Cybersecurity aussehen könnte, wird in der vorliegenden Ausarbeitung anhand von vier konkreten Vorschlägen beleuchtet. Zuvor beginnen wir mit einigen Grundsatzüberlegungen zur Bedeutung des Cyberspace und unterbreiten im Anschluss einen Vorschlag, um den Begriff der Cybersecurity zu präzisieren.

[1] Der Science Fiction-Autor William Gibson nutzte den Begriff Cyberspace erstmals in seinem Roman Neuromancer. Er thematisiert darin die Möglichkeiten computergenerierter grafischer Räume. Siehe: William Gibson, Neuromancer (New York: Berkley Publisher Group, 1984). Umgangssprachlich wird der Begriff meist mit dem Internet gleichgesetzt. Dabei handelt es sich jedoch nur um eine konkrete Anwendungsform der unterschiedlichen Möglichkeiten, die mit der Nutzung des Cyberspace verbunden sind.

[2] Diese Verwundbarkeiten resultieren weitgehend aus den Eigenschaften des Internets, das in der ursprünglichen Konzeption Sicherheit per se nahezu unberücksichtigt lies.

Bringt ein Computerangriff die Klimapolitik der Europäischen Union zu Fall?

Die Frage mag reißerisch klingen, beschreibt jedoch einen realen Vorgang. Erst vor wenigen Tagen haben sich nach Presseberichten bislang unbekannte Täter in das für den Handel mit Emissionsrechten in der Europäischen Union genutzte Computersystem eingehackt und CO_2-Lizenzen im Wert von gut 50 Millionen € gestohlen. Die Europäische Kommission sah sich daraufhin veranlasst, den Handel mit Emissionszertifikaten vorerst auszusetzen. Die möglichen Wirkungen und Nebenwirkungen dieses kriminellen Akts gehen weit über die technische Sicherheit eines Computerhandelssystems hinaus, denn beim Handel mit Emissionszertifikaten geht es um das Kernstück der ehrgeizigen europäischen Klimapolitik.

Der jüngste Vorfall reiht sich ein in eine lange Kette von Zwischenfällen, bei denen moderne Computer-, Informations- und Kommunikationsinfrastrukturen und die darüber angebotenen Dienstleistungen entweder für missbräuchliche Taten verwendet wurden oder diese selbst Ziel illegaler Aktionen waren. Jenseits der technischen Raffinesse und der möglichen Absicht der Täter verweist dieses aktuelle Beispiel auf zwei Aspekte, die gerne übersehen werden: Vertrauen und Psychologie.

Moderne Computer-, Informations- und Kommunikationssysteme sind technisch komplex und anspruchsvoll. Gerade deshalb ist es für deren Akzeptanz unerlässlich, dass die Nutzer Vertrauen in die entsprechende Infrastruktur aufbauen. Vertrauen, dass ihre Daten nicht verloren gehen, nicht manipuliert oder von Unberechtigten gelesen werden. Genau dieses Vertrauen wird durch Vorfälle wie das Leck im Handelssystem mit CO_2-Zertifikaten aber untergraben. Damit greift das psychologische Moment: Wenn schon ein solches System nicht sicher ist, was ist dann als nächstes möglich? Wer ist mit welchen Mitteln in der Lage, welche anderen Straftaten zu begehen bzw. welchen Schaden zu verursachen? Ver-

trauen und Psychologie verstärken einander – im positiven wie im negativen Sinne. Und genau in dieser Wechselwirkung liegt der Grund, weshalb sich moderne Gesellschaften mit der Sicherheit ihrer Computer-, Informations- und Kommunikationsinfrastrukturen beschäftigen müssen.

Nehmen wir die Wirtschaftsnation Deutschland. Nach Angaben des Statistischen Jahrbuchs stieg der Anteil von Personen in Deutschland, die das Internet nutzen, von unter 50% im Jahr 2002 auf deutlich über 70% im Jahr 2009. Im gleichen Zeitraum stieg der Anteil deutscher Haushalte mit Breitbandanschluss von 38% auf 82%, bei den Unternehmen von 54% auf 84%. Gleichzeitig nutzen bereits 48% der befragten Unternehmen die Dienstleistungen im Bereich E-Government für die komplette elektronische Verfahrensabwicklung.[3] Mit einem Umsatz von gut 130 Milliarden € ist Deutschland Europas größter Markt für Produkte und Dienstleistungen im Bereich der Informations- und Kommunikationstechnik; im weltweiten Vergleich belegt Deutschland Platz vier. Mit etwa 850.000 Beschäftigen ist die Branche Deutschlands zweitgrößter Arbeitgeber nach dem Maschinen- und Anlagenbau.[4]

Diese Beispiele verdeutlichen, wie wichtig die Sicherheit des Cyberspace für die Prosperität Deutschlands ist. Und sie machen deutlich, dass der Cyberspace mehrere Nutzungsformen zulässt: Er ist Handelsraum, über den kommerzielle und nicht-kommerzielle Dienstleistungen vertrieben werden. Der Cyberspace ist auch Informationsraum, der dem Nutzer die Möglichkeit des Zugriffs auf vielfältige Daten- und Informationsbestände gibt, gleichzeitig aber auch beispielsweise für die Verbreitung von Propaganda unterschiedlicher Art genutzt werden kann. Gleichzeitig ist der Cyberspace auch Steuerungsraum, der genutzt werden kann, um durch die Übertragung von Daten hochkomplexe Anlagen und industrielle Fertigungsverfahren zu betreiben, zu kontrollieren und zu warten. Aufgrund von illegalen Aktivitäten wird der Cyberspace auch zum Tatraum, in dem Straftaten begangen werden, deren Aufklärung sehr schwierig ist.[5] Zusätzlich machen verschieden Anwendungen im Bereich der sozialen Medien den Cyberspace zu einem allgemeinen Interaktionsraum, den Menschen für die Pflege von Beziehungen unterschiedlichster Art nutzen.

Aus strategischer Sicht entwickelt sich der Cyberspace zu einem eigenständigen Operationsraum, den verschiedene Akteure für ihre Zwecke nutzen. Damit ergänzt der Cyberspace die klassischen Operationsräume Land, See, Luft und Weltraum. Der Cyberspace durchdringt diese anderen Operationsräume und wird damit gleichzeitig zu einem Enabler und Multiplikator der Handlungen in den klassischen Operationsräumen. Das gilt für staatliches Handeln genauso wie für privates Handeln. So nutzen beispielsweise Sicherheits- und Streitkräfte intensiv moderne Computer-, Informations- bzw. Kommunikationstechnik und greifen dabei teilweise auf die gleiche satellitengestützte Infrastruktur zurück, die auch Unternehmen für ihren Kommunikations- und Datenverkehr in Anspruch nehmen. Geht es also um den Cyberspace, treten Staat und Wirtschaft gleichermaßen als Nachfrager und Anbieter elektronisch gestützter Dienste auf, so dass sie ein gemeinsames Interesse an der Sicherheit der dafür benötigten Infrastruktur haben.

Was ist Cybersecurity?

Kein Zweifel, Cyber ist „hype". Kaum ein anderes Thema ist in jüngster Zeit aufgrund aktueller Vorfälle dermaßen intensiv in der öffentlichen Presse behandelt worden. Politische Grundsatzdokumente wie die neue NATO-Strategie und die Strategie zur inneren Sicherheit der EU-Innenminister räumen dem Thema breiten Raum ein. Und auch bei der Münchner Sicherheitskonferenz, die in wenigen Tagen beginnt, dürfte das Thema eine prominente Rolle spielen.

Diese Aufmerksamkeit erweist sich jedoch bei näherem Hinsehen eher als Problem denn als Segen. Ungeachtet der sich weitgehend an einzelnen Phänomenen orientierenden öffentlichen Diskussion fehlt ein konzeptioneller – und damit auch ein politisch-rechtlicher – Grundkonsens darüber, was unter Cybersecurity eigentlich zu verstehen ist, wie sich diese von anderen Sicherheitsherausforderungen unterscheidet, wie unterschiedliche Cyber-Phänomen (z.B. Cybercrime, Cyberwar, Cyberterrorism) voneinander abgegrenzt werden können und wer – Staat und bzw. oder Wirtschaft – wofür welche Kompetenzen bzw. Zuständigkeiten besitzt. Wissenschaftler des Londoner Royal Institute of International Affairs haben den Begriff Cyberspace kürzlich zurecht als „terra nullius" bezeichnet, der sich mangels definitorischer Klarheit gegenwärtig der politischen Diskussion weitgehend entziehe und gerade wegen seiner Vagheit für alle möglichen aggressiven Handlungsformen kulturellen, religiösen, ökonomischen, sozialen und politischen Ursprungs besonders attraktiv sei.[6]

In einer ersten Annäherung an den Begriff erscheint es sinnvoll, zwischen den Faktoren Technik, Mensch und Organisation zu unterscheiden. Diese Dreiteilung schärft das Bewusstsein dafür, dass es eben nicht nur um technische Aspekte und die damit verbundenen Risiken und Gegenmaßnahmen geht. Ebenso wichtig ist die Frage, wie die Technik

[3] Statistisches Jahrbuch 2010 (Wiesebaden: Statistisches Bundesamt, 2010), S. 113-117.
[4] The Information and Communications Technology Industry in Germany (Berlin: Germany Trade & Invest, 2011), S. 3.

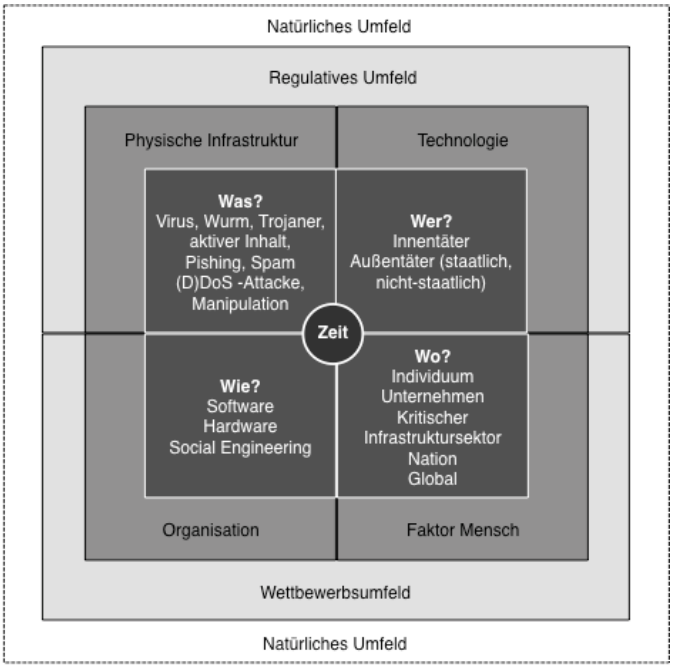
[5] Ein Blick in die Polizeiliche Kriminalstatistik 2009 (Wiesbaden: Bundeskriminalamt, 2009), S. 236-237, verdeutlicht, dass von den knapp 75.000 strafrechtlich relevanten Delikten der Computerkriminalität weniger als die Hälfte aufgeklärt wird. Das verdeutlicht die Probleme der Strafverfolgung im Cyperspace. Im deutschen Recht wird der Begriff Tatraum bzw. Tatort im kriminalwissenschaftlichen Sinne nicht ausdrücklich angesprochen. Soweit von einem „Ort der Tat" die Rede ist, geht es um Fragen der Zuständigkeit für die Strafverfolgung. Nach dem Tatort richtet sich in der Regel die örtliche Zuständigkeit der Polizei oder der Staatsanwaltschaften und damit – nach der gesetzlichen Regelung indirekt – auch der Gerichtsbarkeit. Der Cyberspace ist dagegen weitgehend grenzenlos, und es gibt unzählige Möglichkeiten, die eigene Identität, geografische Lage und die eigenen Systeme zu verschleiern.

[6] Paul Cornish et. al., On Cyber Warfare (London: Royal Institute of International Affairs, 2010), S. viii.

durch den Menschen bedient wird und wie organisatorische Aspekte auf beide – nämlich Mensch und Technik – abgestimmt werden. Allgemein verstanden beschreibt Cybersecurity die Gesamtheit aller erforderlichen Ziele, Mittel und Verfahren, um Computer-, Informations- und Kommunikationssysteme und die darüber transportierten Daten vor Eindringen, Freigabe, Übertragung, Veränderung oder Zerstörung – ob absichtlich oder zufällig – zu schützen.

Auf dieser Basis können wir die für Cybersecurity relevanten Verwundbarkeiten und Risiken näher betrachten und schlagen hierfür das in Abbildung 1 dargestellte Modell vor. Im Zentrum (dunkelgrau) steht die Betrachtung von vier Kernfragen: Welche Instrumente und Methoden stehen für mögliche Angriffe gegen die Cyberinfrastruktur zur Verfügung? Wer sind die Täter und welche Motive verfolgen sie? Wie gehen die Täter vor? Wo machen sich die Auswirkungen schädigender Handlungen bemerkbar? Bei allen vier Fragen ist es besonders wichtig, die zeitliche Dynamik zu berücksichtigen. Nicht jede Maßnahmen, die sich gegen die Computer-, Informations- und Kommunikationsinfrastruktur richtet, wird sofort entdeckt bzw. soll sofort entdeckt werden und führt (un)mittelbar zu einer Wirkung. Gerade für die Früherkennung und die Aufklärung ist die zeitliche Verzögerung zwischen Tat und Ergebnis eine besondere Herausforderung.

Die zweite Dimension (hellgrau) beschreibt das unmittelbare Umfeld, in dem cyber-relevante Infrastrukturkomponenten genutzt werden. Die physische Infrastruktur verweist auf die Einbettung der Computer-, Informations- und Kommunikationskomponenten in andere Infrastrukturelemente. So hat das jüngste Beispiel des Stuxnet-Virus deutlich gemacht, dass es zwischen der „virtuellen" Welt eines Computervirus' und der realen Welt der Zentrifugen eines Atomkraftwerks einen direkten Zusammenhang geben kann. Damit verbunden ist die zweite Teildimension, nämlich die Entwicklung der Technologie. Hierbei geht um Fortschritte in verschiedenen, auch an die Computer-, Informations- und Kommunikationstechnologie angrenzende Wissenschafts- und Technologiedisziplinen (z.B. Quantentechnologie, Energietechnik, Mechatronik, Werkstofftechnologie), aus denen sich neue Gefahren und Chancen im Umgang mit Cyberrisiken ergeben können. Der Faktor Mensch bezieht sich auf die bereits angesprochenen Wechselbeziehungen zwischen Technik und Nutzer.



Abkürzung: (D)DoS Distributed Denial of Service

Abbildung 1: Cybersecurity-Dimensionen

Auch hier machen aktuelle Beispiele deutlich, dass die Gefahr des Innentäters trotz intensiver Diskussion über technische Risiken niemals unterschätzt werden darf. Die Teildimension Organisation verweist schließlich auf die vielfältigen Möglichkeiten der Ausgestaltung arbeitsteiliger Prozesse. Gerade das Drängen nach weltweit vernetzten Arbeits- und Logistikabläufen führt zu vielgliedrigen, global verteilten Wertschöpfungsketten, die ganz spezifischen Sicherheitsrisiken ausgesetzt sind.

Die verbleibenden Dimensionen beschreiben das mittelbare Umfeld. Von besonderer Bedeutung ist der Hinweis auf das regulative Umfeld, denn gerade für Fragen der Cybersecurity gibt es national und international kaum einheitliche Grundlagen. Das schafft Schlupflöcher für Täter und erschwert die grenzüberschreitende Zusammenarbeit der Strafverfolgungsbehörden. Hinzu tritt der Wettbewerbsdruck, der die Probleme, die aus den regulativen Unterschieden resultieren, teilweise noch verschärft. Das gilt z.B. für die unter Sicherheitsgesichtspunkten kritisch zu bewertenden Trends der Auslagerung sensitiver Computer-, Informations- und Kommunikationskomponenten z.B. in Schwellenländer oder den verstärkten Rückgriff auf Commercial-off-the-shelf-Produkte, die zwar kostengünstig, aber keinesfalls frei von Risiken (Stichworte: offene Schnittstellen, offene Programmcodes) sind. Schließlich darf die natürliche Umweltsphäre im Cyber-Kontext nicht vernachlässigt werden. Erdbeben, Unwetter, Überschwemmungen oder das Auftauen des Permafrosts können cyber-relevante Infrastrukturen in Küstennähe oder in alpinem Gelände gefährden. Ebenso sind Stürme im Weltraum geeignet, die Leistungsfähigkeit satellitengestützter Informations- und Kommunikationskomponenten nachhaltig zu beeinträchtigen.

Vorschläge zur Stärkung der Cybersecurity durch öffentlich-private Zusammenarbeit

Weil Cybersecurity für Deutschlands Sicherheit und seine Prosperität gleichermaßen relevant ist, müssen Staat und Wirtschaft gemeinsam nach tragfähigen Lösungen suchen, um den Verwundbarkeiten im Cyberspace zu begegnen. Das ist jedoch leichter gesagt als getan, denn in Anbetracht der bestehenden begrifflichen Unklarheiten fällt eine Aufgaben- und Verantwortungsteilung zwischen Staat und Wirtschaft nicht leicht. Hinzu kommt, dass die öffentlich-private Sicherheitszusammenarbeit zu oft bloß auf die Delegation staatlicher Tätigkeiten an Private reduziert wird. Wir gehen an dieser Stelle jedoch von einem umfassenden Verständnis aus, das sich von der gemeinsamen Lageanalyse und Risikobewertung über die gemeinsame Strategieentwicklung und -umsetzung erstreckt und die Kooperation in den Bereichen Einsätze, Finanzierung, Aus- und Weiterbildung, Forschung und Entwicklung sowie Beschaffung und Unterhalt umfasst.

Vor diesem Hintergrund wollen wir anhand von vier Themenfeldern darstellen, wie Staat und Wirtschaft in Deutschland zur Verbesserung der Cybersecurity zusammenarbeiten könnten. Dabei klammern wir institutionelle Aspekte bewusst aus, da diese gegenwärtig intensiv diskutiert werden. Vielmehr gilt unsere Aufmerksamkeit ausgesuchten Fragestellungen, die in der institutionellen Debatte stärker beachtet werden sollten.

Cyber-Lagebild aufbauen

Lagebewusstsein und Lageverständnis sind zentrale Voraussetzungen erfolgreichen Handelns. Das gilt im Cyberspace ganz besonders. Aufgrund seiner technischen Eigenschaften ist es aber schwierig, Vorgänge im Cyberspace bestimmten Akteuren zuordnen zu können (Non-Attribution). Das ist ein besonderes Problem für rechtsstaatlich legitimiertes Handeln, das eigene Tätigkeiten auf die erkannten Aktionen eines Dritten abstimmen muss. Non-Attribution macht dagegen die Zuweisung von Kausalitäten und Verantwortlichkeiten (z.B. zwischen Akteur, Straftat und Gegenmaßnahme) sehr schwierig. Ein Cyber-Lagebild als ressortgemeinsames Führungsinstrument, das auch die Beiträge nichtstaatlicher Akteure (z.B. im Bereich der Kritischen Infrastrukturen) berücksichtigt, könnte an diesem Punkt ansetzen und in vier Führungsbereichen wichtige Impulse setzen:

- Erkennen
  Mit Hilfe eines Cyber-Lagebildes können staatliche Behörden und Unternehmen erkennen, was, wo und wann im Cyberspace vor sich geht und welche Akteure in die jeweiligen Handlungen involviert sind.

- Bewerten
  Das Erkannte kann interpretiert und bewertet werden. Dabei geht es u.a. um das Gefährdungspotenzial der Handlungen, die konkrete Betroffenheit einzelner Akteure, die von den Handelnden verfolgten Absichten, die vermuteten Wirkungen der Handlungen und die erwartete Entwicklung der Handlungen.

- Entscheiden
  Auf dieser Basis können Entscheidungen über mögliche Maßnahmen der Vorbereitung, als direkte Antwort auf eine mögliche Gefahr oder in deren Nachgang getroffen werden. Ebenso liefert das Cyber-Lagebild wichtige Informationen, um die Erforderlichkeit, Notwendigkeit und Verhältnismäßigkeit der jeweiligen Maßnahmen zu bestimmen.

- Handeln
  Schließlich ist das Cyber-Lagebild auch ein wichtiges Instrument, um die Umsetzung beschlossener Maßnahmen zwischen den beteiligten Akteuren zu koordinieren und den Informationsfluss zwischen diesen jederzeit sicherzustellen.

Das Cyber-Lagebild als Führungsinstrument wird damit zum strategisch relevanten Nukleus der Sicherheits- und Prosperitätsförderung: Das Lagebild erlaubt es einer Vielzahl unterschiedlicher Akteure koordiniert vorzugehen, von der Risikoanalyse bis zur gemeinsamen Umsetzung beschlossener Maßnahmen. Indem das Cyber-Lagebild Auskunft über sich abzeichnende Cybergefahren gibt, stellt es die erforderlichen Informationen bereit, die zur Entwicklung geeigneter Technologien erforderlich sind. Und als innovatives Testbed genutzt, ist das Cyber-Lagebild darüber hinaus geeignet, künftige Anwendungen wie Verfahren, Verhaltensanweisungen, technische Lösungen und sogar organisatorische Maßnahmen vor dem Einsatz auf ihre Eignung zu überprüfen und gegebenenfalls noch konkreter auf die jeweiligen Herausforderungen abzustimmen.

Methoden der vorausschauenden Analytik stärken

Datenströme im Cyberspace sind in ihren Ausmaßen immens. Weil sie gewissen physikalischen Regeln unterliegen, können bestimmte Muster aus der Gesamtmenge der Datenströme erkannt und herausgefiltert werden. Besonders bei Angriffen auf Systeme und Netzwerke wird Mustererkennung (Pattern Recognition) als Frühwarnindikator verwendet. Auch wenn „die üblichen Verdächtigen" agieren und Angriffsvektoren erkannt werden, gibt es stets neue, noch nicht erkannte Formen und Muster, die sich auch bei einer genaueren Betrachtung eines Vorfalls nicht qualifizieren lassen bzw. nicht oder nur nach sehr umfangreichen Analysen erkannt werten.

Um aber unbekannte neue Formen von Verwundbarkeiten zu erkennen, im militärischen Jargon „vor die Lage zu kommen", gibt es Ansätze, die sich mit der vorausschauenden Gefährdungsermittlung (Sequence Prediction) auseinandersetzen. Hierbei werden bekannte Muster, Vektoren, Gefahrenfaktoren, Quellen sowie Ursachenketten für das Auftreten oder Vorhandensein von Gefahrbringenden Faktoren bewerten und gewichtet. Gemeinsame Forschungs- und Technologieanstrengungen von Staat und Wirtschaft könnten in diesem Bereich beispielsweise verstärkt darauf ausgerichtet werden, die Fähigkeit

zu verbessern, um zwischen dem Handeln von Einzelpersonen und Gruppen zu unterscheiden, weil diese Differenzierung für die zu ergreifenden Gegenmaßnahmen entscheidend ist.

Anders verhält es sich in der Kommunikation und im Umgang der Nutzer mit dem Internet. Verhaltensmuster verschiedener Nutzergruppen, sprachliche, zeitliche und thematische Gewohnheiten lassen sich heute sehr schnell bewerten. Hierfür gibt es bereits sehr leistungsfähige Produkte und Lösungen, die auch im Bereich der automatischen Übersetzung respektable Ergebnisse erzielen. Für Staat und Wirtschaft eröffnet sich daraus die Möglichkeit, marktgängige Produkte und Lösungen gemeinsam auf ihre Eignung in den jeweiligen Anwendungsfeldern zu testen und bedarfsorientiert weiterzuentwickeln.

Sicherheit der Hardwarekomponenten konsequent überprüfen

Umgangssprachlich wird Cybersecurity als ein Software-Problem dargestellt. Das ist es auch, aber nicht nur. Zunehmend problematischer ist die Verwundbarkeit kritischer Hardwarekomponenten, die in die Computer-, Informations- und Kommunikationsinfrastruktur eingebaut werden.

Jüngst mehren sich die Berichte über gefälschte Bauteile, die im günstigsten Fall nicht die erwarteten Leistungsparameter erfüllen, im schlimmsten Fall jedoch zur illegalen Informationsabschöpfung genutzt werden.[7] Hardwarebezogene Risiken treffen den Kern des Sicherheits- und Prosperitätsnexus und sind damit für die öffentlich-private Sicherheitszusammenarbeit besonders relevant. Verschiedene Ansätze sind denkbar. Heute gibt es beispielsweise kaum einen Hersteller, der den Weg der Hardwarebauteile über alle Stufen der Wertschöpfungskette verfolgt.[8] Dadurch können Lücken entstehen, die durch enge Informationsflüsse zwischen staatlichen Stellen und Unternehmen geschlossen werden könnten. Gerade bei besonders kritischen Komponenten der Cyber-Infrastruktur erscheint es auch ratsam, der Überprüfung der eingebauten Hardwarekomponenten und ihrer Hersteller mehr Aufmerksamkeit zu schenken. Unternehmensverflechtungen und die Frage, wer woran welche geistigen Eigentumsrechte besitzt, sind in diesem Zusammenhang von besonderer Bedeutung.

Kritische Cyber-Infrastrukturkomponenten identifizieren

Die Debatte über unsichere Hardwarekomponenten ist im Zusammenhang mit der Diskussion über die Sicherheit Kritischer Infrastrukturen zu sehen. Dabei handelt es sich um Einrichtungen, die für die Funktionsfähigkeit von Staat und Wirtschaft sowie für das gesellschaftliche Leben von vitaler Bedeutung sind. Der Prozess der Identifizierung national und europäisch Kritischer Infrastrukturen ist in Deutschland in vollem Gang. Drei Aspekte erscheinen uns für die Cybersecurity besonders wichtig.

Erstens geht es um die Kriterien zur Identifizierung Kritischer Infrastrukturen im Cyber-Kontext. Die Zahl betroffener Nutzer bei Ausfällen könnte ebenso herangezogen werden wie Überlegungen zu den Reservekapazitäten und Substitutionsmöglichkeiten. Wichtig wird es sein, die verschiedenen Komponenten der Cyber-Infrastruktur voneinander zu unterscheiden: Spricht man nur von den Kernnetzen, über die der gesamte Sprach- und Datenverkehr abgewickelt wird? Wie wird das Verhältnis von fixen zu mobilen Infrastrukturen betrachtet? Welche Rolle spielen Unterseekabel und Satelliten? Parallel dazu bedarf es des Dialogs mit den Betreibern über die erwarteten Maßnahmen, die die technische Leistungsfähigkeit zur Vorbeugung bzw. bei Eintritt von Zwischenfällen gewährleisten.

Zweitens ist die Frage nach dem Eigentum an kritischen Cyber-Infrastrukturkomponenten zu stellen. Gerade weil Information in einer globalisierten Weltwirtschaft immer wichtiger wird, ist direkter Zugang zu Informationen – beispielsweise über den Besitz von Infrastrukturkomponenten – kritisch. Komplexe Unternehmensverflechtungen können den Blick für die wahren Motive von Investoren und Betreibern trüben. Hier sind wirtschaftspolitische Interessen am freien Spiel der Marktkräfte gegen sicherheitspolitische Bedenken, die sich u.a. aus der Gefahr der Wirtschaftsspionage ergeben, abzuwägen.

Schließlich ist es auch wichtig, Entwicklungen in anderen Wirtschaftssektoren auf ihre möglichen Folgen für die Cyber-Infrastruktur zu überprüfen. Die Einführung von Smart Grids als wichtiger Bestandteil einer Energiepolitik, die verstärkt auf erneuerbare Energien setzt, ist ein Beispiel. Smart Grids stellen in den Bereichen Sicherheit und Datenschutz teilweise neue Herausforderungen. Gleiches gilt für die Einbindung von Elektroautos in die Smart Grids, denn deren elektronische Steuerungen scheinen noch verwundbar zu sein, so dass darüber Angriffe auf das Stromnetz denkbar sind.[9] Dieses Beispiel verdeutlicht, wie wichtig es ist, umwelt- und energiepolitische mit wirtschafts-, industrie- und sicherheitspolitische relevanten Abwägungen zu verbinden.

Ausblick

Cybersecurity beschreibt eines der zentralen Handlungsfelder, auf dem künftig über die Sicherheit und Prosperität von Nationen und Unternehmen entschieden wird. Im Grundsatz geht es dabei um die strategisch relevante Frage, wie sich Staat und Wirtschaft in Deutschland aufstellen, um Innovationen in den Bereichen der Computer-, Informations- und Kommunikationstechnik zu nutzen und sich gleichzeitig vor den damit einhergehenden Verwundbarkeiten zu schützen. Das ist von fundamentaler Bedeutung, denn der Cyberspace wird im politischen, wirtschaftlichen, gesellschaftlichen und ideellen Wettbewerb der Akteure im 21. Jahrhundert eine

[7] Wesley K. Clark and Peter L. Levin, „Securing the Information Highway. How to Enhance the United States' Electronic Defenses," Foreign Affairs, 88:6 (November/December 2009), S. 2-10.

[8] Cyber Threats to National Security. Countering Challenges to the Global Supply Chain (Arlington: CACI, 2010).

[9] „Außer Kontrolle. Hacker-Angriffe aufs Auto", NZZ, 27. Mai 2010, S. 59.

Kernfunktion spielen. Hierauf muss sich Deutschland vorbereiten. Ein koordinierter nationaler Prozess der engen Zusammenarbeit von Staat und Wirtschaft könnte zielführend sein, weil sich darüber die Risikobewertung, die Strategieentwicklung und die Umsetzung konkreter Maßnahmen im Bereich der Cybersecurity ebenso konkretisieren und abstimmen ließen wie die Entwicklung und Bereitstellung geeigneter Technologien und Systemlösungen, die zukunftsorientierte Antworten auf die Herausforderungen der Verwundbarkeit des Cyberspace geben.

Dr. Heiko Borchert & Felix Juhl, Luzern

Dr. Heiko Borchert leitet ein sicherheitspolitisches Beratungsunternehmen und ist Mitherausgeber der Schriftenreihe Vernetzte Sicherheit (www.vernetzte-sicherheit.net).
Felix Juhl arbeitet im gleichen Beratungsunternehmen, ist Experte für Cybersecurity und externer Fachdozent der Bundeswehr.
Der Beitrag gibt die persönliche Auffassung der Verfasser wieder.

THEMEN

Sparen als Staatsräson
Zur Debatte über die Bundeswehrreform

Es sollten nicht Sparzwänge sein, die über Umfang, Struktur und Ausrüstung der Bundeswehr bestimmen. Ausschlaggebend sind vielmehr eine Analyse der Bedrohungslage und die daraus resultierenden Aufgaben. Doch welchen sicherheitspolitischen Anspruch und welche Bündnisverpflichtungen hat Deutschland überhaupt?

Als im Mai 2010 Etatkürzungen für die Bundesministerien anstanden, bekam Verteidigungsminister Karl-Theodor zu Guttenberg den größten Betrag verordnet: Rund acht Milliarden Euro bis 2014 soll das Verteidigungsministerium künftig einsparen. Seitdem wird die aktuelle Diskussion über die Ausgestaltung deutscher Sicherheits- und Verteidigungspolitik vor allem von Sparzwängen geleitet: Debattiert wird über den Umfang der Streitkräfte und Stellenabbau, die Zahl von Kasernen und Standortschließungen, teure Rüstungsprojekte und Streichlisten. Doch während sich die Debatte auf das finanziell Mögliche konzentriert, wird über das sicherheitspolitisch Nötige viel zu wenig diskutiert.

Besonders deutlich wurde diese Diskrepanz am Beispiel der Wehrpflicht. Obwohl schon die Weizsäcker-Kommission im Jahr 2000 zu dem Ergebnis kam, dass die Wehrform „zu große Personalumfänge bei gleichzeitig zu schwachen Einsatzkräften“ produziere,[10] interessierte dieses sicherheitspolitische Sachargument lange Zeit niemanden in der Union, die im Staatsbürger in Uniform ein Stück ihrer Identität sah. Erst das leere Portemonnaie des Finanzministers und die Schuldenbremse sorgten dafür, dass zu Guttenberg zunächst sich selbst und dann auch seine Parteifreunde Hals über Kopf davon überzeugen konnte, dass die Wehrpflicht überholt ist. Erstaunlich schnell wurde aus der „Identitätsfrage“ Horst Seehofers doch eine Haushaltsfrage.

Nun ist es durchaus begrüßenswert, dass die Sparzwänge die Reformdebatte angestoßen und von einigen Tabus befreit haben. So war die Aussetzung der Wehrpflicht tatsächlich sicherheitspolitisch sinnvoll und lange überfällig. Doch kann Sparen in der Sicherheitspolitik tatsächlich Staatsräson sein? Sollte der eigentliche Impuls für die Reformen nicht vielmehr in den sicherheitspolitischen Veränderungen unserer Zeit bestehen? Und sollte die Ausgestaltung der Bundeswehr nicht eher durch die Bedrohungslage als durch den Rotstift Wolfgang Schäubles bestimmt werden?

Fast schien es zu Beginn der Reformdebatte, als könne der Verteidigungsminister den Sparimpuls nutzen, um jene überfällige Diskussion über Deutschlands Sicherheitspolitik anzustoßen, die seit vielen Jahren von Experten gefordert wird. Allerdings leider nur fast. Zwar hat zu Guttenberg wiederholt betont, dass es ihm in erster Linie um die Einsatzfähigkeit der Truppe gehe. Doch er hat dies – zumindest in der Öffentlichkeit – bisher weder hinlänglich erklärt noch wird darüber ausreichend diskutiert. Beides ist allerdings notwendig, um einen zukunftsfähigen sicherheitspolitischen Konsens herzustellen. Die am Bundeshaushalt orientierten Sparauflagen und ihre Folgen für Personal, Organisation, Struktur und Ausrüstung der Bundeswehr werden isoliert behandelt und eben nicht in einen strategischen Gesamtzusammenhang gestellt.

Rückgriff auf das Weißbuch

Dabei bedarf eine umfassende Reform der Streitkräfte zunächst einmal der Beantwortung einiger grundlegender Fragen: Welche Ziele verfolgt deutsche Sicherheitspolitik? Gegen welche Bedrohungen müssen wir uns verteidigen? Welchen sicherheitspolitischen Ansatz legen wir der Bedrohungsbekämpfung zugrunde? Welche Mittel müssen dafür bereitgestellt werden? Welche Rolle sollen unsere Streitkräfte einnehmen? Welche Verpflichtungen hat sich Deutschland im Rahmen von NATO, EU und UN auferlegt? Vor allem aber: Welche Aufgaben und Verpflichtungen kann die Bundeswehr angesichts der Sparauflagen zukünftig nicht mehr übernehmen? Welche Lehren zieht man aus dem Afghanistan-Einsatz? Will die Bundesregierung nach den dortigen Erfahrungen weiter an den Konzepten „Risiken an der Quelle bekämpfen“ und „Schutz Deutschlands aus der Distanz“ festhalten? Erst wenn diese Fragen beantwortet sind, kann man klären, was personell, organisatorisch und strukturell möglich ist und welche Ausstattung die Bundeswehr braucht.

Doch statt eine Debatte zu führen, die die Vergewisserung oder gar Neudefinition des sicherheitspolitischen Anspruchs der Bundesrepublik zum Ziel hat, diskutiert man in Berlin lieber über Haushaltszahlen und Mannschaftsstärken – und verweist ansonsten gerne auf Altbewährtes: Schließlich habe das Weißbuch von 2006, auf der Grundlage der Verteidigungspolitischen Richtlinien von 2003, alle Fragen bereits beantwortet.

[10] Gemeinsame Sicherheit und Zukunft der Bundeswehr, Bericht der Kommission an die Bundesregierung, 23.5.2000, S. 13.

Deutschland hat sich demnach nichts Geringeres vorgenommen, als das eigene Territorium, seine Bevölkerung und seine Alliierten zu schützen sowie regionale Krisen und Konflikte zu verhindern bzw. zu bewältigen. Daneben will man globalen Herausforderungen wie Terrorismus und Massenvernichtungswaffen wirksam begegnen, zur Achtung der Menschenrechte und zur Stärkung der internationalen Ordnung beitragen, den freien und ungehinderten Welthandel fördern sowie die Kluft zwischen armen und reichen Weltregionen überwinden helfen.

Die Liste der Bedrohungen, denen sich die Bundesrepublik ausgesetzt sieht, ist lang. Sie umfasst neben Terrorismus, Proliferation und regionalen Konflikten auch den illegalen Waffenhandel, „Entwicklungshemmnisse", Failing und Failed States, Ressourcen- und Energieknappheit, Migration, Pandemien und Seuchen. Der sicherheitspolitische Ansatz, der all diesen Bedrohungen entgegenwirken soll, setzt auf Früherkennung, Prävention und Vernetzung und umfasst das gesamte Instrumentarium politischer Macht – einschließlich militärischer Mittel.[11]

Ohne Übertreibung kann man folglich sagen, dass der sicherheits-politische Anspruch Deutschlands nicht gerade bescheiden wirkt. Im Gegenteil: Wir möchten überall auf der Welt zur Stelle sein können, um allen denkbaren Risiken zu begegnen. Unsere Bundeswehr haben wir dabei meistens im Gepäck. Und wir stellen sie im Rahmen unserer Maxime, nur in Bündnissen zu handeln, auch anderen zur Verfügung. In Zahlen ausgedrückt bedeutet dies: Für die NATO Response Force will Deutschland bis zu 15.000 Einsatzkräfte bereithalten,[12] im Rahmen der EU-Battlegroups sind es bis zu 18.000, das UN Standby Arrangement System verlangt weitere 1.000 Soldatinnen und Soldaten. Dazu kommen noch einmal 1.000 Kräfte für die Evakuierung deutscher Staatsbürger. In diesen Zahlen sind die Kräftebeiträge für laufende Einsätze wie in Afghanistan und auf dem Balkan nicht einmal enthalten.[13]

Da Gegenteiliges von der Bundesregierung nicht vernommen wurde, kann man davon ausgehen, dass Deutschland in Anbetracht der komplexer werdenden internationalen Lage auf diesem Anspruch beharrt – und ihn noch erweitern muss. So zumindest ist das Ja zum neuen Strategischen Konzept der NATO zu verstehen, das nicht nur die Liste der Bedrohungen ausdehnt (Cyber-Attacken), sondern entgegen mancher Vorhersagen neben der Bündnisverteidigung auch die Bereitschaft zur internationalen Krisenprävention und zum Krisenmanagement aufrechterhält.[14] Auch in diesem Zusammenhang wurde der „Level of Ambition", den die NATO 2006 festgelegt hat, bislang nicht geändert: Neben einer groß angelegten Operation zur Bündnisverteidigung haben sich die Bündnismitglieder verpflichtet, gleichzeitig (!) zwei größere Operationen mit jeweils bis zu 60.000 Einsatzkräften und sechs „kleinere" Operationen mit jeweils 20.000 bis 30.000 Einsatzkräften außerhalb des Bündnisgebiets durchführen zu können.[15]

Für Deutschland sind dies keine bloßen Lippenbekenntnisse, sondern Verpflichtungen, die Geld kosten. Zwei aktuelle Beispiele: Im Zuge der allgemeinen finanziellen Zwänge beabsichtigt die NATO, ihre Kommandostruktur zu reformieren. Das Ergebnis könnte allerdings für die einzelnen Bündnismitglieder zusätzliche Kosten nach sich ziehen. Geplant ist eine massive Reduzierung der bestehenden zehn Hauptquartiere auf fünf – bei gleich bleibendem „Level of Ambition". Die daraus entstehende Fähigkeitslücke gedenkt die NATO auf einfache Weise zu schließen. Sobald die im Bündnis vorhandenen Fähigkeiten aufgebraucht bzw. gebunden sind, wird sie ihre Mitglieder um die Bereitstellung fehlender Hauptquartiere bitten. Die Forderungen der NATO an die Mitglieder – und damit auch an Deutschland – könnten sich durch die Straffung der NATO-Kommandostruktur also noch erhöhen.

Auf dem Lissabonner Gipfel hat sich die NATO zudem entschlossen, ein territoriales Raketenabwehrsystem aufzubauen, um sich gegen die wachsende Gefahr durch ballistische Raketen zu schützen. Obwohl die USA einen erheblichen Beitrag zu diesem längst überfälligen Projekt leisten werden, ist derzeit noch nicht geklärt, wie die Lasten der restlichen Komponenten, die man für die Erhöhung der Systemeffektivität benötigt, aufgeteilt werden (z.B. weitere Abfangraketen). Fest steht, dass auch Deutschland einen gewichtigen Beitrag leisten muss, wenn es seine Bündnisverpflichtungen erfüllen will. Gemeinsam verteidigen heißt eben auch, die politische Zustimmung in konkrete finanzielle und personelle Beteiligung umzumünzen.

Anspruch und Wirklichkeit

Betrachtet man den deutschen sicherheitspolitischen Anspruch und die Sparpläne, die dem Verteidigungsministerium auferlegt wurden, erkennt man einen gravierenden Widerspruch. Zum einen folgt aus der Vielzahl der möglichen Bedrohungen, dass die Bundeswehr die ganze Bandbreite des Einsatzspektrums abdecken muss – von hochintensiven Kampfeinsätzen bis hin zu humanitären Hilfseinsätzen. Dafür muss sie kurzfristig einsetzbar, über lange Distanzen verlegbar und durchhaltefähig sein.

Zum anderen kann die Bundeswehr schon heute die an sie gestellten Ansprüche kaum erfüllen – das zeigt der Afghanistan-Einsatz ganz deutlich (Verfügbarkeit von einsatzfähigen Soldaten, Einsatzvorbehalte, qualitative und quantitative Materialmängel, Ausbil-

[11] Vgl. Bundesministerium der Verteidigung: Weißbuch 2006 zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr, Berlin 2006, S. 19 ff.

[12] Davon 5000 in Bereitschaft, 10 000 in Vor- und Nachbereitung. Vgl. ebda, S. 77.

[13] Vgl. ebda.

[14] Vgl. Heads of State and Government: Active Engagement, Modern Defence – Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, Lissabon 2010, Abs. 4 und 20–25.

[15] Vgl. Press Briefing by NATO Spokesman James Appathurai after the Meeting of the North Atlantic Council at the Level of Defence Ministers, Brüssel 2006, www.nato.int/docu/speech72006/s060608m.htm.

dungsmängel, mangelnde Rechtssicherheit für Soldaten etc.). Sie muss daher dringend weiter optimiert werden. Allerdings erfordert diese Reform erst einmal genau das Geld, das der Schäublesche Rotstift dem Verteidigungsetat entzieht. Dieser Widerspruch ist bei Aufrechterhaltung beider Ansprüche – Optimierung der Bundeswehr und schnelle Einsparungen – nicht aufzulösen. Damit die Schere zwischen sicherheitspolitischem Anspruch und finanzpolitischer Wirklichkeit nicht noch weiter auseinander geht, sind nur zwei Optionen denkbar.

Eine erste Option wäre, den eigenen sicherheitspolitischen Anspruch herunterzuschrauben – mit allen Konsequenzen, die eine solche Entscheidung mit sich brächte. Dies würde vor allem Deutschlands militärisches Engagement in den Bündnissen betreffen. Es liegt auf der Hand, dass eine abgespeckte Bundeswehr weniger Verpflichtungen in NATO, EU und UN übernehmen könnte. Auch wenn sich das deutsche Gewicht in der Allianz nicht allein am Streitkräfteumfang messen lässt, so wird Deutschland doch erheblich an Einfluss und Glaubwürdigkeit verlieren, wenn es seine politischen Verpflichtungen nicht finanziell und personell untermauert. Diese Zusammenhänge sollten offen diskutiert werden. Betrachtet man aber den Verlauf der deutschen Reformdebatte über die letzten Monate hinweg, fällt auf, dass die Bündnisverpflichtungen darin kaum eine Rolle spielen. Die Bundeswehrreform wird als rein nationales Projekt betrachtet.

Die zweite Option wäre, die Bundeswehr nach dem eigenen sicherheitspolitischen Anspruch auszurichten. Dies hieße zunächst, den finanziellen Druck vom Verteidigungsminister zu nehmen und ihm mehr Zeit zu geben, bevor eventuelle Einsparungen wirksam werden müssen. Diese Zeit könnte er nutzen, um die Reformvorschläge, die auf dem Tisch liegen, zu durchdenken und Entscheidungen gemäß den strategischen Leitfragen zu treffen. Dass zu Guttenberg die Bundeswehr einsatzfähiger machen will, ist im Grundsatz richtig. Allerdings ist ein solcher Umbau nicht billig zu haben. Auch die Reformvorschläge der Weise-Kommission,[16] wie zum Beispiel der groß angelegte Personalabbau, kosten zunächst einmal mehr Geld, bevor sie langfristige Sparperspektiven eröffnen – das hat die Kommission selbst immer wieder betont.

Doch diese Investition ist erforderlich: Denn Massenvernichtungswaffen und Terrorismus sind keine Phantasien, sondern spiegeln heute mehr denn je die sicherheitspolitische Wirklichkeit wider, die man sich nicht je nach Kassenlage zurechtbiegen kann. Genauso wie internationale Krisen und Konflikte lassen sich diese Bedrohungen nicht auf Eis legen, bis Deutschland seine Staatsfinanzen saniert hat. Als regionale Mittelmacht mit globaler Verantwortung kann Deutschland die Bekämpfung dieser Bedrohungen nicht anderen überlassen und sicherheitspolitisch Trittbrett fahren. Umfang, Organisation, Struktur und Ausrüstung der Bundeswehr müssen daher konsequent durch die Bedrohungslage und die daraus resultierenden Aufgaben bestimmt sein – nicht durch die Sparmaßnahmen des Finanzministers.

Die politische Führung in Berlin muss offen darüber reden, was genau die Bundeswehr zukünftig überhaupt leisten soll und was nicht. Denn wer sagt, mit dem Weißbuch von 2006 seien die entscheidenden Fragen abschließend beantwortet, hat offensichtlich vergessen, dies der Bevölkerung in überzeugendem Maße nahe zu bringen.

Wie wenig dies bislang geschehen ist, zeigten die Reaktionen auf die Äußerung von Bundespräsident Horst Köhler, der über die Andeutung stürzte, deutsche Soldaten notfalls auch zur Absicherung von Handelswegen einzusetzen. Damit bezog er sich auf das Weißbuch 2006. Einer Öffentlichkeit, die ihn heftig ins Visier nahm und seinen Rücktritt forderte, war das offensichtlich nicht bewusst.

[16] Vgl. Bericht der Strukturkommission der Bundeswehr: Vom Einsatz her denken – Konzentration, Flexibilität, Effizienz, Oktober 2010.

Dr. des. Jana Puglierin,
Svenja Sinjen,
Berlin

Dr. des. Jana Puglierin ist wissenschaftliche Mitarbeiterin im Berliner Forum Zukunft (BFZ) im Forschungsinstitut der DGAP.
Svenja Sinjen leitet das Berliner Forum Zukunft (BFZ) im Forschungsinstitut der DGAP.
Der Beitrag gibt ausschließlich die persönliche Auffassung der Autoren wieder.
Dieser Beitrag erschein erstmalig in: IP Internationale Politik Januar/Februar 2011.

THEMEN

Iran: Foreign and Security Policy Aspects

I have already been able to comment on *Maritime Security – A Threat to World Trade?* in a previous forum at this conference. Following the discussions in Roundtable 4 "Atom in the 21st Century: Problems and Prospects" I would now like to add to the technical questions some aspects of political, economic and military nature. I think it is right to say that the international community is viewing the nuclear activities of Iran with some trepidation.

Iran's Threat Perception

If one wants to understand Iran's current threat perception it is necessary to examine the thinking of the current political and military leaders in the country. When looking at the deployment of American forces in the region and the scale of conventional rearmament of neighbouring states it is almost understandable that Iran's leadership feels both encircled and thus frightened. The recent American decision to supply Saudi-Arabia with new weapon systems to the value of 60 billion US $ will hardly diminish any fears. Tehran is also well aware that Iran is very much on the target planning agenda of both Washington and Tel Aviv.

The primary foreign policy goal of Tehran is thus to reduce and weaken U.S. presence in the region and to strengthen Iran's po-

sition as a significant regional power.

Iran is deeply suspicious of the West, especially of the "great Satan" U.S.A. and the "little Satan" Israel. The use of the word "Satan" is not necessarily directed against the U.S.A. as it is against Western politics, democracy, freedom of thought and emancipation. Such terms have much to do with what we in the West term "restoration", a concept alien to the Iranian leadership. The current Iranian leadership is less frightened of an Israeli attack; it however greatly fears a war with the United States.

Iran has not forgotten Western support for Iraq during the Iranian-Iraqi war in the 80ies. It has also not forgotten the U.S. embargo following the hostage taking at the U.S. embassy in Tehran from November 4, 1979 until January 20, 1981 which limited Iran's access to Western technology.

Iran's Ambitions

In order to achieve the status of a regional power the current Iranian leadership is using following strategy:

- Expansion of the nuclear and missile programs
- Concentration on asymmetric military operations
- Opportunistic use of oil as a weapon
- Empowerment of the Shiite population both in the region and globally.

Iran's Nuclear Program

The Iranian nuclear program goes back to the days of the late Shah in the 1960ies. Following the 1979 revolution the program was ended and it was only in the 1990s that Tehran embarked on a new nuclear program. In 2002 confidential documents were released by an Iranian group of exiles which hinted at a new and secret Iranian nuclear program. In 2003 the government of Mohamed Khatami agreed to cease the enrichment of uranium; in January 2006 president Mahmoud Ahmadinejad proudly announced that his country would once again restart its program of uranium enrichment.

There have however been numerous indications of secret and not so secret attempts of Iran to acquire crucial components for both the missile and nuclear programmes since 2003. These efforts underscore the Iranian desire to become a military nuclear power. In 2009 the new head of the International Atomic Energy Agency (IAEA), Yukia Amamo, announced that "Information available to the IAEA raises concern about the possible existence in Iran of past or current undisclosed activities related to the deployment of a nuclear payload for a missile." Experts are now of the opinion that Iran will have such a capability sometime between 2010 and 2015.

Iran's military nuclear ambitions cannot be viewed separately from its missile program. Both are expressions of Iranian ambition to be a regional power. Its missile program is largely based on the modified Shahab-3 rocket with a range of up to 2,000 kilometres and on mobile missiles with a similar range. The solid fuel missile Sajji-2 is similar in payload and range to the Shahab-3, but is however less vulnerable to preemptive strikes due to short launch cycles. The development of intercontinental missiles appears to have run into problems and the developments of such systems has fallen behind U.S. expectations. As a result, the main threat comes from Iranian short and medium range missiles.

North Korea and China are supporting Iran in the development of these programs; there are also rumours that the Ukraine has also delivered some key components. Russia has remained on the fence. On the one hand, Moscow is interested in strengthening its political influence and economic interest both in Iran and in the region. On the other hand, Russia is concerned about the military nuclear program as it unfolds in Iran. The decision not to supply Iran with state-of-the-art S-300 ground-to-air missiles is a testimony both to Moscow's concerns and an improvement in relations between Russia and the United States.

Iran's Asymmetric Warfare

Iran is well aware that both the United States and Israel enjoy a significant military position of superiority. For this reason Iran lays great value and is concentrated on asymmetric war-fare. This explains Iran's support for Hezbollah in Lebanon and why it supports Hezbollah in its conflict with Israel. Iran has invested significant sums of money in the building of the Hezbollah organisation and has supplied weapons, communications technology and training. It is estimated that Iran supports Hezbollah with approximately 100 million US $ every year.

Such support has resulted in Israel not being able to fully realize its military ambitions in Lebanon, the asymmetric warfare strategies of Hezbollah have both forced Israel to accept the situation, and this in turn is celebrated as a victory in Tehran and the Arabian world. Tehran sees itself confirmed in its decision to concentrate on asymmetric warfare in order to achieve its stated security policy goals.

Oil as a Weapon

Iran has the second largest oil reserves behind Saudi-Arabia and the second largest gas reserves behind Russia. This position of power has resulted in Iranian threats to use oil as a weapon in the case of a military attack on the country. In spite of an estimated 18 % decline in the Iranian oil capacity by 2015, such a threat would have global implications. Should Iranian oil be removed from the market the results would be a dramatic increase in the oil price and a new international economic and financial crisis. Saudi-Arabia, in the past a swing provider, would not be able to compensate for the short fall.

Iranian Options

An attack by the USA or Israel on Iran would not cause a third world war. Nevertheless, Iran has the

capacity to create a high degree of uncertainty and insecurity. It could, for example, ramp up its support for militant elements in Iraq and thus exert the pressure on the U.S. Iran furthermore has the capability to close the Straits of Hormuz, which, coupled with an oil export embargo, would further reduce the availability of oil as significant volumes of non-Iranian oil are shipped through the Straits.

Iran could also increase its support for Hezbollah and Hamas and encourage such groups to mount attacks against Israel. The recent visit of Iranian president Ahmadinejad to Lebanon, who sees himself as the successor of Ayatollah Khomeini, in October 2010, clearly illustrates the potential Iran sees in the mobilisation of the 80 million Shiites in the Near and Middle East for Iranian purposes. On 8 October 2010 United Nations Secretary General Ban Ki-Moon said that he is very concerned by rising tensions in Lebanon and "that the country should not be used as a staging ground for further regional aspirations or to promote conflict." Furthermore, attacks of Iranian extremists cannot be excluded.

Consequences of Iran as a Nuclear Power

Should Iran achieve its aims and become a regional nuclear atomic power this would have a significant impact on the distribution of military power in the region and on the possibilities open to the Iranian armed forces. Israel has frequently made it known that it would not tolerate such a situation. A conventional arms race in the region is apparent today; should Iran become a nuclear military power we can expect a similar development on the nuclear front. Countries such as Saudi-Arabia, Egypt and Syria would seek individually or jointly to develop similar weapon systems. This would make an already instable region yet more instable. In the event of Iran achieving its aims, an attack by the United States and/or Israel on the nuclear infrastructure and oil facilities of the country are likely. The economic consequences of such an attack would be similar to an oil embargo.

Iran is an important trading partner for China and Beijing has invested approximately 40 billion US $ in the oil and gas sector of Iran. An interruption of energy supplies caused by an embargo or a military strike would mean a short fall of 12 % in Beijing's oil imports. Furthermore, 80 billion US $ in development aid and hundreds of billions of US $ linked to future energy shipments would be at risk. This situation explains China's insistence on a continued dialogue with Iran and a deep reluctance to any further escalation of sanctions. Having said that, it is worth remembering that China's relationship with the United States is of far greater importance to China than the relationship with Iran.

Any analysis of the future role of a nuclear Iran cannot ignore the one-million-dollar-question relating to the political rationality of the current leadership in Iran. The crucial question is whether the leadership would behave in a rational and predictable manner if in the possession of nuclear weapons. Israel clearly is not of the opinion and has little trust in the current leadership in Tehran. The U.S., ever hopeful, is of the conviction that diplomacy can win the day. Some political analysts believe that Iran is only seeking to become a nuclear power in order to use this as a political weapon. The two main aims are to secure the position of the religious leadership in the country and to become the major regional power. This latter point is of crucial importance for countries such as Saudi-Arabia, Iraq and the Gulf states, all of whom are deeply suspicious of Iran's intentions. Should Iran become a nuclear power, the degrees of freedom for the non-nuclear countries in the region would become severely limited. The nuclear powers U.S.A. and Israel would also have more limited options but these would not be as severe as those of the non-nuclear states in the region.

Finally, it needs to be said that sanctions and threats as well as offers of cooperation by the West have had little or no impact on the Iranian leadership. Some would argue that the threats have in fact convinced the Iranian leadership that the West is truly frightened by the prospect of a nuclear armed Iran. This in turn confirms the Iranian view that only a nuclear armed Iran is taken seriously and respected. It remains to be seen if the international community will accept an Iran which has nuclear capability but not necessarily nuclear weapons. Such a situation could be a possible compromise solution which could be acceptable to the West but possibly not to Israel. The West, together with Russia, will continue the containment policy and at the same time offer the possibility of continued dialogue. This policy is expressed clearly in the plans to jointly develop and deploy a missile defence system in Europe which is aimed at defeating the Iranian threat. Countries in the Middle East, such as Saudi-Arabia and the U.A.E., are investing heavily in missile defence systems, also aimed at containing the Iranian threat.

In our preoccupation with the Iranian missile threat we have somewhat forgotten that Iran has huge internal, structural, economic and social problems. The nuclear debate has deflected the analysis of these problems both nationally and internationally. The perceived "Western" threat serves to domestically gloss over such problems. It would make a great deal of sense for the West to include possible solutions to such problems as a part of the continued dialogue to reduce the threat of a regional nuclear conflict in the near future.

_____

Dr. Peter Roell, Berlin

Dr. Peter Roell is President of the ISPSW Institute for Strategic, Political, Security and Economic Consultancy, Berlin www.ispsw.de
Opinions expressed in this statement are those of the author.
This paper was presented at the Rhodes Forum VIII Annual Session, World Public Forum „Dialogue of Civilizations", October 7-11 2010, Rhodes, Greece

THEMEN

Iraq – the Ignored Market

There used to be an American saying in the 1980s that you could conduct business in any trouble spot as long as the calibre of munitions did not exceed 20 mm. This pearl of wisdom is as relevant today as it was then and applies to Iraq in particular.

Iraq today has come a long way from the days when most if not all cars on Route Irish from Baghdad Airport into town were fired upon or subjected to IED attacks. Not that the country is safe and peaceful, far from it, but given sensible and robust precautions business can be conducted in Iraq today.

During the week ending 3rd December 2010 there were 157 reported incidences in Iraq, 36% of which took place in Baghdad. A further hot spot is the northern city of Mosul. In contrast the Kurdish Region is peaceful, and in Basra, the oil capital and port city, visitors can even risk a visit to restaurants in the city. This is a huge step in the right direction when one considers that it was only three years ago when anti-Western Shia militants controlled the streets.

Many of the attacks are aimed at the Iraqi Armed Forces and other representatives of the elected government. Kidnapping of high value foreigners for money and political motives remains a major threat, as does the risk of being involved in an attack on government forces. In a recent survey conducted by the Economist Intelligence Unit (EIU) violence is seen to be the biggest threat to business in Iraq, closely followed by the level of corruption and lack of infrastructure.

Iraq now has a Government in place, a process which took time and complex manoeuvring by all parties involved. Prime Minister Maliki has reportedly fired hundreds of intelligence and security officials and has replaced these with less capable political loyalists from his own Da`wa Party. According to local sources some of the replacements have doubtful qualifications and are clearly political appointees. These dismissals come as the US is shifting greater responsibility for Iraq's security to the same institutions which are now being purged for political reasons.

A further development is the increased importance of the Sadrist movement in the Government since the return of Sadr from Iran in early January 2011. Sadr is a fierce opponent of continued American presence in Iraq beyond 2011, Maliki however depends upon Sadr in order to remain in power. Among the Iraqi Shia population Sadr is a hero as he opposed the American presence in Iraq both with words and deeds.

The future role of the United States in Iraq remains unclear. Clearly Iraqi politicians are no longer only consulting with America but are turning more and more for advice to their neighbours in other countries in the region such as Iran. It was after all Iran which brokered the power-sharing deal between Maliki and Sadr, a development which represents a major defeat for the US.

America has made it known that it might be willing to stay on in Iraq past the deadline of end 2011 if asked by the Iraqi Government. Ryan Crocker, the veteran US diplomat who was Ambassador to Iraq during the surge years 2007 – 2009, expects that the Iraqi Government will ask the Americans to stay on if the security situation fails to improve by that time. Such a move would be opposed by the Sadrists who threaten to attack US troops in Iraq should they remain in country past 2011.

Clearly the security situation is volatile to say the least. If the Iraqi Government continue to purge the key Ministries of Defence and Interior the security situation is likely to worsen. If as a result the Americans are asked to stay, the attacks on both Americans and Iraqi Forces are likely to increase. None of these developments are attractive to potential investors from Germany or elsewhere.

Almost every industry needs modernising, from health care to tourism. The latter sounds surprising, it should not be forgotten that more than one million Iranians visit Iraq's holy sites every year. Anybody who has recently visited the country will recognise that the roads and public infrastructure need a complete overhaul. Only few Iraqis have access to canalisation, fresh water and health care, major investments are desperately needed.

Investments that bring know-how would be useful. But that would require skilled foreigners to move to a country whose own engineers and doctors have fled in droves. Few are tempted; those who take the plunge are mainly in the safer Kurdish region. Investors are also put off by the high level of corruption – Iraq was fifth from bottom of last years Transparency International corruption-perception index.

Other than a few large multinationals such as Siemens and Daimler, as well as a small number of brave mid-size companies, few German companies show much of an interest in investing in a country which has the second-largest oil reserves in the world. They are leaving the market to others such as the Americans, French and Turkish companies who are much in evidence in Iraq.

In the 1980s German exports to Iraq amounted to around 4 Billion Euros, in 2010 German exports to the country are estimated to have come to around 580 Million Euros. The Iraqis have a high regard for German products and expertise in areas such as construction, education, and health care, all fields where Iraq needs support sooner rather than later. German companies cannot expect to wait until the security situation has normalised and then bid for contracts, the competition will have picked up many of such contracts and will have consolidated their hold on the market.

The tricky security situation in Iraq, especially in Baghdad, makes for a business environment which has to be approached with caution and sound planning. What

has to be understood is that security comes at a price and that this needs to be factored into the cost of doing business in Iraq in advance. You can't simply take a taxi from the Airport to the Hotel or from the Hotel to an appointment. To undertake such a trip involves an armed security detail, consisting of up to four armoured vehicles and professional guards. The cost of such a detail can run to $ 4000 per day and represents the most costly of all possible Taxi journeys. Hotels are expensive and not very comfortable and the recreational factor is negligible. Accommodation in Camps run by the numerous western security companies is safe, for those accustomed to luxury Hotels however an acquired taste. In short, Iraq is not an ideal place to do business.

In spite of these factors business is booming, largely thanks to the signing of a number of oil contracts last year. Construction too is booming thanks to government contracts, even if funds keep go missing. Mobile phone penetration is surging due to the lack of land lines and the need to have three different phones in Baghdad to ensure coverage. Consumer goods are pouring into the country. Iraqis crave Western brands they could not buy during the embargo, an era referred to as the "Chinese years" for all the cheap Asian goods on the shelves.

The huge investments of foreign oil companies from the US, the UK, France and China have created a new Wild West in cities such as Basra, a place in Iraq where savvy businessmen are prepared to work in difficult surroundings in order to enter the market at an early stage. Much the same can be seen in Baghdad where delegations of business people lobby the Ministries for lucrative contracts.

On their way to their appointments such people pass through miles of slums, polluted canals and rivers and uncollected garbage. They will drive on crumbling roads past derelict housing and stay in Hotels which were last renovated in the 1980s. If they are lucky enough to have a Government helicopter at their disposal they will fly over poverty-stricken villages and small towns lacking any form of infrastructure.

Iraq for all these reasons and in spite of the security situation represents a huge market of the future and has been so far ignored by German companies. Such companies should no longer look for reasons why they can't conduct business in this lucrative market; they should ask themselves how they can enter the market before it is too late. Iraq will welcome German companies, they will however not wait.

_____

Maxim Worcester, Berlin

Maxim Worcester is Senior Advisor at ISPSW, Berlin. Before, he was Senior Manager for Advisory Forensic at KPMG International. In the past he was Managing Director of Control Risks Germany, and held senior positions at the Economist Intelligence Unit, the Frankfurter Allgemeine Zeitung and Deutsche Börse AG. Opinions expressed in this contribution are those of the author.

IMPRESSUM

Denk*würdigkeiten*

Journal der
Politisch-Militärischen
Gesellschaft e.V.

Herausgeber
Der Vorstand der **pmg**

Redaktion
Ralph Thiele (V.i.S.d.P.)
Tel.: +49 (221) 8875920
E-Mail: info@pmg-ev.com
Webseite: www.pmg-ev.com

Die **Denk*würdigkeiten*** erscheinen mehrfach jährlich nach den Veranstaltungen der **pmg**.