Denkwürdigkeiten

Journal der Politisch-Militärischen Gesellschaft

Nr. 63
April
2010

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

ISSN 1436-3070

LEADOFF

Liebe Mitglieder,

mit Entsetzen und Grauen, aber nicht gänzlich unerwartet, drängt sich in diesen Wochen der Tod als Begleiter der deutschen Afghanistan-Mission in den Vordergrund. Nicht nur Anteilnahme und Mitgefühl für die Hinterbliebenen – dies gilt in gleichem Maße für die Verwundeten – gebieten genaues Hinsehen; auch Verantwortung verpflichtet.

Verteidigungsminister Dr. Karl-Theodor Freiherr von und zu Guttenberg hat Frank-Jürgen Weise, Chef der Bundesagentur für Arbeit, beauftragt, als Vorsitzender einer Strukturkommission die Struktur der Bundeswehr auf den Prüfstand zu stellen. Diese soll bis Ende 2010 Eckpunkte für eine effiziente Organisation der Bundeswehr erarbeiten. Die Bundeswehr müsse besser als bisher auf die Aufgaben einer Armee im Einsatz eingestellt werden. So die Vorgabe des Ministers.

In dieser Ausgabe zeigt Heiko Borchert in seinem Beitrag auf, dass einer konsequenten Einsatzorientierung bisher tradiertes gesellschaftliches Rollenverständnis im Wege steht. Die zu beklagenden Opfer zwingen zur Frage, wie viel uns dieses Verständnis wert ist oder ob wir nicht doch dringend an unserer Einstellung arbeiten müssen? Zudem bürstet Heiko Borchert eine Reihe von Fragestellungen für die Kommission quer und kommt zu bemerkenswerten Folgerungen.

Bemerkenswert ist auch, wie unsere britischen Nachbarn Einsatzaufgaben untersuchen. britannicus gibt uns Einsicht in die Arbeit der unabhängigen Untersuchungskommission zum Irakeinsatz, die eine tiefgehende Analyse sowie Lehren erarbeiten soll als Beitrag zu verbesserter Regierungsführung und Entscheidungsfindung in ähnlichen künftigen Fällen. Viele „Findings“ lesen sich wie ein „Blueprint“ für deutsche Auslandseinsätze. Auch daraus lassen sich Erkenntnisse für die Kommissionsarbeit schöpfen.

Ein weiteres Einsatzfeld, mitten unter uns, ist das Thema „Red Guests“. Wer sich beobachtet fühlt bei seiner Arbeit am Computer in Business und Administration muss nicht unbedingt an Halluzinationen leiden. „Red Guests“ sind ein Thema, das – wie uns Sheo Nandan Pandey vermittelt – zunehmend ernsthafte Betrachtung verdient.

Viel ist zu tun.

Ralph Thiele, *Vorstandsvorsitzender*

In dieser Ausgabe

1 Quo Vadis Bundeswehr?
Dr. Heiko Borchert

5 Richtige Entscheidung – Richtige Fehler
britannicus

8 Red Guests
Dr. Sheo Nandan Pandey

THEMEN

Quo Vadis Bundeswehr?

Die Strukturkommission als Chance

Zwischen der Teilnahme der Bundeswehr an der NATO geführten Operation Allied Force im Kosovo und den Luftangriffen gegen Aufständische in Kunduz liegen zehn Jahre. Beide Ereignisse sind Wegmarken in der Entwicklung der Bundeswehr. In beiden Fällen geht es um eine für die Zukunft der deutschen Streitkräfte zentrale Frage: Was soll die Bundeswehr können dürfen, und welches sind die Bezugsgrößen, um diese Frage zu beantworten? Die Antwort darauf ist wegweisend, denn es geht um nichts Geringeres als die Abkehr vom Kalten Krieg – in Denken, Struktur und Ausrüstung der Bundeswehr.

Zwischen Einsatzorientierung und gesellschaftlicher Akzeptanz

Kritiker der Kosovo-Intervention (1999) befürchteten, dass die Bundeswehr damit zur weltweit einsetzbaren Interventionsarmee umgebaut werde. Das ist nicht geschehen, auch wenn die internationale Ausrichtung der Bundeswehr seither deutlich gestärkt wurde. Zehn Jahre später ist es erneut ein Kampfeinsatz, der zu einer Kontroverse führt. Als Reaktion auf die Ereignisse in Kunduz wird die von der Bundeswehr im Norden Afghanistans betriebene Quick Reaction Force aufgelöst und damit der militärische Kampf gegen Aufständische als Streitkräfteauftrag zurückgestuft.

Kampf ist nicht die einzige Einsatzmöglichkeit der Bundeswehr. Aber dieser Auftrag zeigt, dass sich die deutsche Politik auch gut zwanzig Jahre nach dem Ende des Kalten Krieges immer noch schwer tut mit dem Rollenverständnis der Bundeswehr. Im Spannungsverhältnis zwischen Einsatzorientierung auf der einen und gesellschaftlich-politischer Akzeptanz auf der anderen Seite hat die Bundeswehr ihr inneres Gleichgewicht noch nicht gefunden. Nach wie vor ist der politische Konsens für gewisse Formen der Einsatzorientierung brüchig.

In diesem Umfeld nimmt die Bundeswehrstrukturkommission ihre Arbeit auf. Der Koalitionsvertrag von CDU/CSU und FDP sieht vor, dass die Kommission bis zum Jahresende Eckpunkte einer neuen Organisationsstruktur der Bundeswehr erarbeiten soll. Würde die Arbeit der Strukturkommission von den Ereignissen in Kunduz dominiert, wäre eine große Chance vertan. Wünschenswerter wäre es, die im Weißbuch der Bundesregierung (2006) aufgezeigte Entwicklungslinie für die Bundeswehr fortzuschreiben und zu konkretisieren. Dieses Grundlagendokument der schwarz-roten Vorgängerregierung ist nicht obsolet. Seit seiner Veröffentlichung sind allerdings Entwicklungen zu beobachten, die Anpassungen der Bundeswehr erforderlich machen könnten. Um zu bestimmen, was die Bundeswehr künftig können soll, wäre es wichtig, dass die Strukturkommission ihre Diskussion breit anlegt, um daraus Leitlinien für Auftrag, Fähigkeiten und Struktur der deutschen Streitkräfte abzuleiten. Welche Fragen könnten in diesem Zusammenhang diskutiert werden?

Während der internationale Ordnungsrahmen an Orientierungskraft verliert....

Die internationalen Beziehungen befinden sich im Umbruch. Neue Akteure drängen auf die internationale Bühne und versuchen, die Spielregeln der internationalen Beziehungen nach ihren Interessen zu beeinflussen. Arrivierte Akteure geraten unter Druck. Sie kämpfen nicht nur um ihre bisherige Position, sondern auch damit, dass ihre eigenen Kräfte in immer zahlreicheren internationalen Krisenherden gebunden sind. Die aktuellen Wirtschafts- und Finanzprobleme verstärken den Trend, dass sich westliche Demokratien zusehends mit sich selbst beschäftigen. Es wird schwieriger, internationales Engagement innenpolitisch zu rechtfertigen. Die Bekämpfung von Armut im Ausland, die Stabilisierung von Krisenherden weitab der Heimat oder der Abbau der Arbeitslosigkeit im Inland erscheinen angesichts knapper Kassen als Gegensatz, der nicht einfach aufzulösen ist.

Anders als in der Vergangenheit gibt es auch zwischen den verbündeten westlichen Staaten kaum Konsens darüber, ob und wie man gemeinsam auf die Umbrüche antworten will. Weder die NATO noch die Europäische Union vermitteln im Moment die notwendige strategische Orientierung, an die nationale Sicherheitspolitik anschließen könnte. Deutschland muss daher Grundlagenarbeit leisten, um seine eigene Position in einer Phase des strategischen Umbruchs zu definieren.

.... haben sich europäische Partner bereits positioniert

Die Zeit hierfür drängt, denn wichtige europäische Verbündete haben sich in den letzten Jahren bereits entsprechend positioniert. London setzt auf sein traditionell enges Verhältnis zu den USA und hat sich über den Verkauf von Rüstungstechnologie nach Saudi Arabien im Nahen und Mittleren Osten strategisch aufgestellt – wohl auch, um von dort stärker nach Südostasien vorzustoßen. Finanzielle Probleme machen aber den britischen Streitkräften zu schaffen, so dass hinter Großbritanniens Führungsanspruch ein großes Fragezeichen steht. Frankreich scheint im Moment die bessern Karten zu besitzen. Die Übernahme des Allied Command Transformation in der NATO, die energie- und rüstungstechnologisch vorangetriebene Zusammenarbeit mit Brasilien, Russland und den Vereinigten Arabischen Emiraten sowie die Avancen gegenüber Indien und Pakistan kennzeichnen die Achsen der französischen Einflussnahme. Auf einen ähnlichen Politikmix setzt auch Italien, wenngleich Rom mit Hilfe seiner Energie- und Rüstungsunternehmen strategische Beziehungen mit Partnern aus Russland, Libyen, Kasachstan und Weißrussland eingeht.

Wirtschaftspolitisch begründete Sicherheitspolitik?

Auf diese konsequent vorangetriebenen Positionsbezüge seiner europäischen Partner hat Berlin bislang keine hinreichende Antwort. Damit sind wir bei der ersten Frage. Sollte Deutschlands Sicherheitspolitik nicht stärker wirtschaftspolitisch begründet werden?

Deutschland ist eine führende Exportnation und als solche von weltwirtschaftlicher Prosperität abhängig. Neben seiner sehr starken wirtschaftlichen Verflechtung mit den europäischen Nachbarn ist Deutschland wichtiger Handelspartner von Schlüsselländern wie Brasilien, China, Iran, Russland, Saudi-Arabien und Südafrika. Eine exportorientierte Volkswirtschaft braucht maritime Sicherheit für

den Zugang zu Absatzmärkten und die gesicherte Energie- bzw. Rohstoffversorgung. Das Weißbuch 2006 erwähnt diese Aufgabe, doch spiegelt sie sich auch in der aktuellen Ausrichtung der Marine? Wäre die heutige Marine beispielsweise in der Lage, einen Beitrag zur Sicherheit der sich am Nordpol möglicherweise öffnenden neuen Seewege zu leisten? Welche Sicherheitslösungen könnten deutsche Unternehmen zum Schutz der Logistikkette zur See – von sicheren Hafeninfrastrukturen über die Verbesserung des maritimen Lagebildes und die Aufklärung von Seewegen aus Luft und Weltraum bis zum Schutz von Schiffen – in Zusammenarbeit mit staatlichen Partnern international anbieten?

Können Streitkräfte umweltfreundliche Mobilitätskonzepte fördern?

Eng mit der Wirtschaftspolitik sind die Umwelt- und Energiepolitik verknüpft. Beide Felder werden die Sicherheitspolitik im 21. Jahrhundert prägen. Im Energiebereich erleben wir derzeit, wie die Verfügungsmacht über Energierohstoffe genutzt wird, um die Spielregeln der internationalen Politik neu zu definieren. Gleiches zeichnet sich auch für andere Rohstoffbereiche ab.

Dort, wo Energierohstoffe auf dem Seeweg transportiert werden, gewährleisten Streitkräfte durch ihren Beitrag zur maritimen Sicherheit auch die Energieversorgungssicherheit.
Schon heute haben die NATO-Seestreitkräfte den Auftrag, Energieinfrastrukturen in der Nordsee zu schützen. Strategisch bedeutsame Fragestellungen ergeben sich für die Bundeswehr zum Beispiel durch den Ausbau der zivilen und militärisch genutzten Hafeninfrastruktur Chinas in Südostasien. Wie will Berlin darauf reagieren? Welches wären die Konsequenzen für die deutsche Wirtschaft, wenn China wirtschaftspolitische Interessen an offenen Seewegen mit eigenen sicherheitspolitischen Mitteln durchsetzen würde?

Eine andere Facette des Energiethemas gewinnt auch für die Streitkräfte immer mehr an Relevanz: umweltverträgliche Mobilitätskonzepte. Alternative Antriebe, Speicherkapazitäten von Batterien oder neue Werkstofftechnologien gelten als Zukunftsthemen. Ihr Mobilitätsbedarf macht die Bundeswehr zu einem idealen Testfeld, um technische Innovationen zu erproben. Wäre dies ein Themenfeld, in dem die Bundeswehr mit Automobil-, Energie-, und Rüstungskonzernen sowie mit wissenschaftlichen Einrichtungen in Deutschland stärker kooperieren könnte?

Macht Klimaveränderung Deutschland und Indien zu Partnern?

Die Sorge um globale Klimaveränderungen drückt der Energiediskussion ihren Stempel auf. Die Auswirkungen von Dürre, Nahrungsmittel- und Wasserknappheit auf die regionale Stabilität werden sicherheitspolitisch bereits thematisiert. Daneben sollten zwei weitere Aspekte mehr Beachtung finden.

Klimaveränderung bedeutet, dass Geopolitik nicht länger konstant bleibt! Wenn Meeresspiegel steigen, können sich Landesgrenzen verschieben, mit Auswirkungen beispielsweise auf die wirtschaftlichen Nutzungszonen zur See. Konflikte um rohstoffreiche Unterseegebiete könnten daraus resultieren. Wie bereitet sich Deutschland auf die damit verbundenen möglichen Konsequenzen für die Freiheit der Hohen See vor?

Klimaveränderungen werden auch Europa treffen. Winterstürme, Trockenheit und Hochwasser haben in den letzten Jahren bereits gezeigt, wie verwundbar unsere Infrastrukturen sind. Verfügt Deutschland wirklich über genügend zivile Hilfskräfte und -mittel, um umweltbedingte Infrastrukturausfälle über lange Zeit zu verkraften? Wie steht es um die innereuropäische Solidarität im Bereich des Katastrophen- und Bevölkerungsschutzes? Wer hält hierfür die benötigten Mittel vor? Indische und deutsche Streitkräfte unterhalten seit Jahren eine Partnerschaft. Was könnten die Bundeswehr und andere deutsche Hilfskräfte von den indischen Streitkräften lernen, die spezielle Einheiten für die Katastrophenhilfe bei Überschwemmungen unterhalten?

Sicherheit von Mega-Städten: Von Brasilien lernen?

Der Hinweis auf Umweltprobleme bringt uns zur demografischen Entwicklung. Mega-Städte mit dreißig oder noch mehr Millionen Einwohnern werden in den Industrieländern, aber vor allem in den Schwellenländern noch stärker wachsen. Viele dieser Mega-Städte liegen in Küstennähe und sind damit von der Gefahr steigender Meeresspiegel unmittelbar betroffen. Ist es, um beim indischen Beispiel zu bleiben, denkbar, dass indisch-deutsche Streitkräfteeinheiten einen Beitrag leisten könnten, um solche Mega-Städte schnell zu versorgen und Infrastrukturelemente bereitzustellen, die zerstört wurden? Welchen Nutzen könnte Berlin im Hinblick auf seinen Einfluss in Schwellenländern aus einer solchen Zusammenarbeit ziehen?

Die Sicherheit der Mega-Städte ist eine weitere Herausforderung. Die Erfahrungen aus Lateinamerika verdeutlichen, dass Polizeikräfte in diesem Aufgabenfeld an ihre Grenzen stoßen können und daher Streitkräfte eingesetzt werden. Insbesondere die brasilianischen Kommandeure der UN-Schutztruppen auf Haiti verweisen darauf, dass Erfahrungen aus der heimischen Kriminalitätsbekämpfung für den internationalen Stabilisierungsauftrag auf der Karibikinsel relevant sind. Dieses Argument ließe sich analog auf andere Konfliktregionen übertragen. Dahinter steckt die Frage, welche Staaten künftig mit welchen Konzepten welche Aufgaben in internationalen Einsätzen übernehmen wollen. Welche Vorstellungen hat Deutschland dazu? Sollen der Bundeswehr polizeiliche Aufgaben übertragen werden, oder soll die Bundespolizei verstärkt im Ausland genutzt werden? Welche

Konsequenzen hätte dies für die Personalanforderungen der Bundespolizei? Wäre der Wirtschaftspartner Brasilien vor diesem Hintergrund auch ein Sicherheitspartner für die Bundeswehr in internationalen Einsätzen?

Wie nutzen wir den Weltraum?

Überlagert werden die vorangehenden Überlegungen durch eine sicherheitspolitisch relevante Dimension, die sich die Bundeswehr schrittweise erschließt: den Weltraum. Geht es um die Aufklärung von Umweltveränderungen durch Satellitenaufnahmen, die Übertragung von Information und Kommunikation oder die korrekte Positionsbestimmung von Flugzeugen, Schiffen und Fahrzeugen, weltraumgestützte Fähigkeiten sind aus unserem Alltag kaum mehr wegzudenken. Werden Satelliten immer wichtiger, müssen sie leistungsfähig und sicher sein. Wer den Weltraum nutzen will, muss daher wissen, welche anderen Akteure sich dort aufhalten, welche Absichten sie verfolgen und welchen Gefahren (z. B. Weltraumschrott) die Satelliten ausgesetzt sind. Der von der Bundeswehr vorangetriebene Aufbau eines Weltraumlagebildes ist deshalb unerlässlich für alle staatlichen und wirtschaftlichen Aktivitäten, die auf Unterstützung aus dem Weltall bauen.

Das Potenzial der Weltraumnutzung scheint noch nicht ausgeschöpft. Ein neues Zeitalter dürfte anbrechen, wenn François Auque, Chef des Weltraumunternehmens Astrium, mit seiner Vision recht behält, dass der Weltraum dereinst auch für die Energieversorgung genutzt wird. Wenn es technisch gelänge, Energie im Weltraum zu gewinnen und zur Erde zu transportieren, wäre die Energieversorgung weitgehend unabhängig von der bisherigen Infrastruktur am Boden möglich. Hat Deutschland für diese kühne Vision eine adäquate industriepolitische Antwort, insbesondere auch mit Blick auf die enge französisch-italienische Weltraumzusammenarbeit? Könnte die Bundeswehr mit ihrem ausgeprägten Mobilitätsbedarf ein Schlüsselkunde für weltraumbasierte Energieversorgungskonzepte werden?

Wie gewährleisten wir Sicherheit im Informationsraum?

Eng verbunden mit der Nutzung des Weltraums ist schließlich auch die Frage, wie wir uns auf die sicherheitspolitischen Herausforderungen im Informationsraum (Cyber Space) vorbereiten. Jüngst fällt die Zunahme von Medienberichten über Cyber-Angriffe gegen Behörden und Unternehmen auf. Oft ist nicht klar, wer die Angriffe auslöst und durchgeführt bzw. welche direkten und indirekten Schäden damit verbunden sind. Die Vorgänge unterstreichen aber, dass eine Reihe von Akteuren die Verwundbarkeit westlicher Länder aus dem Informationsraum als Chance für sich selbst versteht und aktiv ausnutzt.

Risiken aus dem Informationsraum treffen die Exportnation Deutschland an ihrer Achillesferse. Ein möglicher Verlust des Vertrauens in die Sicherheit und Zuverlässigkeit des Informationsraums, über den der elektronische Handels- und Zahlungsverkehr abgewickelt wird, hätte gravierende Folgen. Aber bei wem liegen in Deutschland die Zuständigkeiten, um gezielte Computerangriffe zu erkennen, abzuwehren und geeignete Gegenmaßnahmen zu ergreifen? Wer verfügt hierzu über welche Mittel? Welche Rolle soll die Bundeswehr im Rahmen der nationalen Sicherheitsvorsorge im Informationsraum spielen, und wie könnten ihre vorhandenen bzw. aufwachsenden Fähigkeiten zum Schutz im Informationsraum ressortübergreifend genutzt werden? Welche Konsequenzen zieht die deutsche Politik aus dem Umstand, dass China mit der Bündelung seiner Anstrengungen in den Bereichen Energie, Weltraum und Informationsraum genau jene Handlungsfelder priorisiert, die den Aktionsradius' Pekings erweitern und gleichzeitig jenen seiner möglichen Gegner einschränken können?

Bundeswehr klug nutzen

Mit den Stichworten Dynamik und Komplexität beschreibt der neue, mehrjährige US-Verteidigungsplan das strategische Umfeld der Zukunft. Streitkräfte müssen in diesem Umfeld vor allem eines sein – flexibel. Flexibilität bedeutet rasche Verfügbarkeit, hohe Einsatzbereitschaft, modularer Aufbau, agile Zusammenarbeit mit wechselnden Partnern, vernetzte Abläufe und qualitativ anspruchsvollere Anforderungen an die Angehörigen der Streitkräfte, um vielfältige Aufgaben zu erfüllen.

Die Forderung nach Flexibilität birgt für die Bundeswehr Chancen und Risiken: Chancen, weil ein multifunktionales Einsatzspektrum den politischen Nutzen der Bundeswehr erhöht; Risiken, weil bei unklarer Prioritätensetzung die Verzettelung droht. Eines ist heute schon klar: Veränderung wird die Bundeswehr künftig noch viel stärker prägen als in der Vergangenheit. Diese Veränderung und den damit verbundenen Wandel erfolgreich zu gestalten, wird damit zur wichtigsten Zukunftsaufgabe für die deutschen Streitkräfte. Genau deshalb ist die Arbeit der Strukturkommission so wichtig. Mit ihren Empfehlungen kann sie die Bundeswehr flexibler machen und gleichzeitig konkretisieren, welche Beiträge die Bundeswehr im Sinn der Vernetzten Sicherheit für andere Politikbereiche leisten kann.

Dr. Heiko Borchert, Luzern/Berlin

Dr. Heiko Borchert leitet ein sicherheitspolitisches Beratungsunternehmen und ist Mitherausgeber der Schriftenreihe Vernetzte Sicherheit (www.vernetzte-sicherheit.net).
Der Beitrag gibt die persönliche Auffassung des Verfassers wieder.

THEMEN

Richtige Entscheidung – Richtige Fehler

Die Chilcot-Untersuchung zur britischen Rolle im Irak

Im Juni 2009 kündigte Premierminister Brown im Unterhaus in Reaktion auf die schlechten öffentlichen Umfragewerte zum Irakeinsatz eine unabhängige Untersuchungskommission zur britischen Politik zwischen Sommer 2001 und Mitte 2009 an. An der Spitze der von Brown benannten Kommissionsmitglieder steht mit John Chilcot einer der erfahrensten "Mandarine" der britischen Ministerialverwaltung. Zu den fünf Mitgliedern gehören auch der Kriegsforscher Lawrence Freedman, unter anderem Verfasser der offiziellen Geschichte des Falklandkrieges, sowie der Churchill-Biograph und Nahost-Historiker Martin Gilbert. Als Geheime Staatsräte (Privy Counsellors) haben sie uneingeschränkten Zugriff auf alle Verschlusssachen, von denen bereits Zehntausende ausgewertet werden, einschließlich solche höchster Geheimhaltungsstufe.

Die Aufgabe lautet, eine tiefgehende Analyse sowie Lehren zu erarbeiten als Beitrag zu verbesserter Regierungsführung und Entscheidungsfindung in ähnlichen künftigen Fällen. Die Untersuchung deckt ein wesentlich breiteres Feld ab als vorangegangene verwandte Untersuchungen, etwa zu den methodischen Schwächen nachrichtendienstlicher Bewertung der durch Saddams Verschleierungstaktik verursachten Ungewissheit über Massenvernichtungswaffen-Programme.

Von November 2009 bis März 2010 befragte die Kommission rund 80 der Hauptakteure des britischen Regierungsapparats öffentlich als Zeugen. Das Spektrum reicht von Premierministern, Kabinettsmitgliedern und Staatsministern über leitende Ministerialbeamte aller relevanten Ressorts, Streitkräfteführung, Truppenkommandeure, Verbindungsoffiziere, Nachrichtendienstkoordinatoren, Leiter der Ziviloperationen, Botschafter und diplomatische Verhandlungsführer bis hin zu Rechtsberatern sowie einer Reihe von Blairs ehemaligen engen Mitarbeitern. Hinzu kommen Gespräche mit Kriegsveteranen, Angehörigen von Gefallenen sowie Experten.

Das Verfahren der Anhörungen

Entgegen Browns ursprünglicher Absicht werden die Anhörungen öffentlich gehalten. Auch von ausnahmsweise geschlossenen Sitzungen sollen so viele Teile veröffentlicht werden wie rechtlich und unter Sicherheitsgesichtspunkten möglich. Erstmals werden die Anhörungen im Fernsehen ausgestrahlt und als Video ins Internet gestellt (www.iraqinquiry.org.uk). Dort finden sich auch binnen eines Tages die kompletten Wortprotokolle der Anhörungen sowie deklassifizierte Dokumente.

Die Art der Fragestellung ist fair, unvoreingenommen und ohne politische Zielsetzung, greift jedoch mit großer Energie die wichtigen Kritikpunkte und Themen öffentlicher Sorge auf. Die Zeugen werden im Vorfeld auf die zu erwartenden Schwerpunktfragen zu ihren damaligen Kenntnissen und Handlungen und rückblickenden Einschätzungen hingewiesen. Bei strittigen Punkten wird nachgehakt, um klare Aussagen zu bekommen. Es handelt sich nicht um ein Rechtstribunal, das Anschuldigungen oder Fehlverhalten untersucht. Ausgeklammert von der Untersuchung sind Vorwürfe wegen Missbrauch und unerlaubtem Gewalteinsatz durch Soldaten, die Gegenstand laufender Rechtsverfahren sind.

Bedingt vor allem auch durch die solide Sachkenntnis der Kommissionsmitglieder ist es vielen der befragten Persönlichkeiten gelungen, die Anhörung als Plattform zur Vermittlung respektabler, zum Teil sogar brillanter Arbeit im Umgang mit sehr schwierigen Herausforderungen zu nutzen. Das vorliegende Material belegt im Schnitt einen Grad an Ernsthaftigkeit und Professionalität, der aller Fehlbarkeit und allen enttäuschten Hoffnungen zum Trotz in erfreulichem Kontrast steht zu den in der Öffentlichkeit vorherrschenden Zerrbildern von politischer Führung.

Der Weg zum Krieg

Eine Hauptaufgabe der Untersuchung besteht in der Rekonstruktion und Dokumentation der durch polarisierte Debatten, selektive Berichterstattung und die menschlichen Kosten des Krieges verschütteten Ausgangspunkte des Irak-Engagements und seines Verlaufs. An die Stelle von Schwarzweiß-Malerei setzen die Anhörungen ein vollständigeres Bild mit vielen Schattierungen. Die Zielsetzungen und Abwägungen, aber auch die Fehleinschätzungen und blinden Flecken werden im Detail nachvollziehbar.

Das Protokoll der Aussage von Tony Blair füllt allein fast 250 Seiten, in denen er in gewohnt luzidem Vortrag den Irak-Einsatz in den strategischen Kontext des Bemühens um wertorientierten Wandel im Nahen und Mittleren Osten im Widerstreit mit entgegenwirkenden Kräften wie Al Qaida oder dem iranischen Regime einordnet. Mit dem aus dem Terrorangriff vom 11. September 2001 folgenden neuen unmittelbaren Sicherheitsinteresse der USA am Mittleren Osten schied im Umgang mit Irak eine Fortschreibung der vormaligen bloßen Eindämmungspolitik als Option aus. Es war offenkundig, dass für die USA die offenen Risiken dieser Politik nicht mehr hinnehmbar sein würden, vor allem auch wegen der befürchteten Weiterverbreitung von Massenvernichtungswaffen in Terroristenhand. Saddams langjährige, fortgesetzte Brüskierung des UN-Sicherheitsrates in Bezug auf die verhängten Abrüstungs- und Nichtverbreitungsverpflichtungen machte Irak, wie es der amtierende Premierminister Gordon Brown nun formuliert, zu einem „*Aggressorstaat, der sich nicht an die Regeln der Staatengemeinschaft hält*."

Ab dem Frühjahr 2002 waren die USA darauf festgelegt, falls sich nicht kurzfristig ein anderer Weg eröffnet, den politischen Wandel im Irak mit militärischen Mitteln zu erzwingen. Die Frage war nicht mehr Ob, sondern Wann. Aus Blairs Sicht ging es darum, diesen Impuls zur Stärkung der Staatengemeinschaft zu nutzen und im britischen Interesse zu verhindern, dass in den USA Unilateralismus von einer Versuchung zur Notwendigkeit wurde: „*Ich wollte nicht, dass Amerika glaubt es habe keine andere Wahl als es alleine zu tun.*"

Ab Februar 2002 wirkte die britische Diplomatie gemeinsam mit anderen auf die USA ein, bis Präsident Bush schließlich im September den multilateralen Weg in den UN-Sicherheitsrat einschlug. Diese aktive Einbettung der USA war verbunden mit der Hoffnung, dass sich durch demonstrative Einigkeit der P-5 doch noch ein friedlicher Weg zur Überwindung der von Saddams Politik ausgehenden Sicherheitsbedrohungen ergeben könnte.

Die Aussagen von Blairs Stabschef Jonathan Powell und des außenpolitischen Beraters David Manning über die vertraulichen Gespräche mit der amerikanischen Regierung im Jahr 2002, ebenso wie zahlreiche andere Aussagen von Diplomaten und Militärs über spätere Phasen bieten außerordentlich interessante Einblicke in die Modalitäten der Abstimmung und Zusammenarbeit mit den USA und den stetigen Versuch, zum Vorteil der Sache das Beste aus dieser ungleichen Partnerschaft zu machen.

Die Frage der Rechtmäßigkeit

Die Anhörung dokumentiert, dass es 2003 wie heute unter den Völkerrechtsexperten der britischen Regierung zwei Meinungen über die Rechtmäßigkeit der Invasion gibt aufgrund unterschiedlicher Interpretationen der Sicherheitsrats-Resolution 1441 vom November 2002. Die von britischer Seite an der Aushandlung dieser Resolution damals selbst Beteiligten, allen voran UNO-Botschafter Jeremy Greenstock und Außenminister Jack Straw, unterstützen jedoch konsistent in nachvollziehbarer, vertretbarer Weise die bekannte Position der britischen Regierung und ihres damaligen Generalanwalts Lord Goldsmith, wonach der Resolutionstext am Ende bewusst so aushandelt wurde, dass eine spätere zweite Resolution zwar politisch sehr wünschenswert, aber rechtlich nicht notwendig war.

Rechtlich dauerte der Irak-Krieg von 1990/91 demnach in Form der an strikte Bedingungen und weitreichende Sanktionen geknüpften Waffenstillstandsregelung des Sicherheitsrats fort. Wie zuvor bei anderen Anlässen bereits 1993 und 1998 lebte die ruhende Ermächtigung zum Einsatz militärischer Gewalt aus der ursprünglichen Resolution 678 durch die Feststellung in Resolution 1441, dass mangelhafte Kooperation mit den Inspektoren eine weitere „erhebliche Pflichtverletzung" wäre, angesichts des nachfolgenden unbefriedigenden irakischen Verhaltens wieder auf.

Die Enttäuschung über die damalige französische Haltung, die aus britischer Sicht die Legitimität sowohl der Koalition als auch des Sicherheitsrates schwächte, ist noch immer nicht ganz überwunden. Jack Straw glaubt weiterhin, dass bei einer Einigung der P-5 auf die vorgeschlagene zweite Resolution „*das Saddam-Regime sehr schnell kollabiert wäre und der Krieg wahrscheinlich nicht notwendig gewesen wäre*."

Das lange Durchhalten

Die nach der Invasion schließlich im Mai 2003 beschlossene Multilateralisierung des Neubeginns im befreiten Irak wurde schon im August 2003 durch die Ermordung des UNO-Repräsentanten Sergio Vieira de Mello und seiner Mitarbeiter durch Zarkawis Al-Qaida-Gruppe in Bagdad im Keim erstickt. Die unerwartet stark verrottete Infrastruktur des Landes und die unzureichende Kontrolle über die öffentliche Ordnung stellten die Koalition schon zu Beginn des Nachkriegsaufbaus vor praktisch unlösbare Schwierigkeiten. Lesenswert sind in diesem Zusammenhang die differenzierten Korrekturen von John Sawers, 2003 britischer Sonderbeauftragter in Paul Bremers Zivilverwaltung, an der vorherrschenden Meinung zur damaliger Vorgehensweise, vor allem auch zur Entba'athisierung und Auflösung der alten Armee.

Für die britischen Truppen im Südirak ging es angesichts der von April 2004 an eskalierenden Gewalt durch lokalen Widerstand, internationalen Terrorismus und rivalisierende Milizen mit ausländischer (vor allem iranischer) Unterstützung in den sehr schwierigen Jahren bis 2007 vor allem darum, die Stellung zu halten, bis sich auf nationaler Ebene ein handlungsfähiger irakischer Staat rekonstituierte. Erst nach der militärischen Zerschlagung der schiitischen Milizen auf Initiative von Premierminister Maliki durch die irakischen Streitkräfte mit britischer Hilfe und unter Nutzung amerikanischen Militärmaterials kam 2008 auch in Basra der friedliche Wiederaufbau in Gang.

General Graeme Lamb, 2006/07 stellvertretender Kommandeur der multinationalen Streitkräfte im Irak, betont als entscheidenden Faktor für die Überwindung von eskalierendem Aufstand und mörderischem Chaos ab 2007 die Kombination der neugewonnenen irakischer Führungsbereitschaft mit dem von den Irakern zunehmend geachteten professionellen Einsatzwillen vor allem der amerikanischen Streitkräfte auch unter schlimmsten Bedingungen zur Herstellung der notwendigen Rahmenbedingungen für eine stabile Entwicklung.

Zeichen des Erfolges

Die ursprüngliche britische Zieldefinition des Einsatzes lautete: "*Ein stabiler, einiger und gesetzestreuer Irak in unveränderten Grenzen, der mit der internationalen Staatengemeinschaft zusammenarbeitet, keine Bedrohung mehr für seine Nach-*

barn oder die internationale Sicherheit darstellt, sich an alle seine internationalen Verpflichtungen hält und allen seinen Bevölkerungsgruppen ein effektives repräsentatives Regierungssystem, nachhaltiges Wirtschaftswachstum und steigenden Lebensstandard bietet."

Gemessen an dieser Vorgabe kann heute, wenn auch noch mit einigen Vorbehalten und unter Achtung der zwischenzeitlichen sehr hohen menschlichen Verluste durch Terror und Gewalt, die Operation insgesamt als Erfolg gelten. Seit Mitte 2007 ist die Zahl neuer Opfer drastisch zurückgegangen. Die Indikatoren für die wirtschaftliche Entwicklung haben sich deutlich verbessert. Das durchschnittliche Pro-Kopf-Einkommen ist jetzt deutlich höher als unter Saddam und die Kindersterblichkeit um ein Vielfaches niedriger. Der Grundstein ist gelegt für ein funktionierendes repräsentatives Regierungssystem, in dem erstmals die Angehörigen aller Bevölkerungsgruppen ihre politischen Rechte ausüben können. Die meisten Iraker leben lieber in der Ungewissheit des heutigen Systems als in der Gewissheit der Unterdrückung unter Saddam.

In Bezug auf die so heftig umstrittene Frage der Massenvernichtungswaffen, Trägerraketen und zugehörigem Material und Einrichtungen ist die inzwischen bekannte Faktenlage, die sich aus der Iraq Survey Group (Duelfer-Bericht) und vor allem den Aussagen von Saddam Hussein nach seiner Verhaftung über seine Beweggründe und Absichten ergibt, von der Öffentlichkeit noch nicht zur Kenntnis genommen worden. Am Ende hat sich die damalige Einschätzung bestätigt, dass Saddam entschlossen war, nach Aufhebung der Sanktionen die eingestellten verbotenen Waffenprogramme wieder aufzunehmen. Premierminister Gordon Brown, der trotz der bevorstehenden Wahlen ausdrücklich um eine Chance zur Aussage im Rahmen der Chilcot-Untersuchung bat, nennt den Irak-Krieg folglich heute die "richtige Entscheidung aus den richtigen Gründen".

In den Anhörungen wurde auch die Frage gestellt, ob der Irak-Krieg dem britischen Ansehen geschadet hat. In der Einschätzung der befragten britischen Diplomaten trifft dies aus heutiger Sicht unter dem Strich nicht zu, vor allem nicht im arabischen Raum selbst, wo im Gegenteil die gezeigte Handlungsfähigkeit und unmittelbare Vertrautheit mit der Region eher als positive Qualitäten wirken.

Viele Schwachpunkte

Der Regierungsapparat in Whitehall war zu keiner Zeit hinreichend "mobilisiert" zur erfolgreichen Durchführung einer integrierten zivil-militärischen Strategie im Anschluss an die Invasion. Im Alltagsbetrieb des Regierens in London stand Irak trotz allen politischen Leitvorgaben nicht immer weit genug oben auf der Prioritätenskala. Das Grundproblem, das sich noch viel mehr in den USA zeigte und auch in anderen Ländern in ähnlicher Weise weiter besteht, ist das Fehlen ausreichender Planungs- und Einsatzführungsstrukturen für gemischte zivil-militärische Einsätze.

Im Einsatzraum fehlte es an einer wirksamen Kommunikationsstrategie. Das Versagen der Informationspolitik im Irak und in der Region ließ die Initiative entgleiten und Erfolge verpuffen. Kritische Fragen stellen sich auch im Hinblick auf die Abläufe der Ausrüstungsbeschaffung im Verteidigungsministerium und den zielgerichteten Einsatz von Entwicklungshilfemitteln.

Vergleichsweise unterbelichtet bleiben in den bisherigen Anhörungen die militärischen Erfahrungen unterhalb der politisch-strategischen Ebene. Hier könnte sich das in den Rängen bisweilen beklagte Problem widerspiegeln, dass die zivile und militärische Führung sich unzureichend um die praktischen Details der Missionserfüllung vor Ort kümmert. Der frühere Verteidigungsminister John Reid erkennt zumindest an, dass die US-Streitkräfte "aufgeweckter, schneller und besser" ihre Lehren aus der im Irak angetroffenen Situation gezogen haben.

Es bleibt abzuwarten, inwieweit die Chilcot-Untersuchung auch die in den Aussagen angesprochenen militärischen Erfahrungen aufarbeiten wird. Strukturelle Probleme zeigten sich z. B. in der Logistik, wo allzu oft falsche Rückmeldungen suggerierten, das Material sei da, wo es sein sollte – mit fatalen Folgen für die eigenen Soldaten. Angesichts der Doppelbelastung in Afghanistan und Irak bestanden akute Mängel bei Kräftemultiplikatoren (ISTAR, UAVs, Hubschrauber, Transportflugzeuge).

Ausblick

Nach Abschluss der ersten Anhörungsrunde konzentriert sich die Arbeit nun auf die Auswertung der Dokumente, gefolgt von einer weiteren vertiefenden und ergänzenden Anhörungsrunde Mitte 2010. Der Abschlussbericht mit Schlussfolgerungen und Empfehlungen ist frühestens Ende 2010 zu erwarten. Ob das Format der Untersuchung den von der britischen Regierung erhofften positiven Effekt auf die öffentliche Wahrnehmung und Wertschätzung der Politik haben wird, muss sich noch zeigen, auch in den im Mai bevorstehenden Parlamentswahlen. Man kann jedoch erwarten, dass der Chilcot-Bericht am Ende Lehren präsentieren wird, die über britische Zwecke hinaus auch für andere in komplexen Einsätzen engagierte Länder von Interesse sind.

Breitere Bedeutung hat die Untersuchung als ein innovativer Versuch, den richtigen Umgang mit der neuen Herausforderung zu finden, dass auch in einst sakrosankten Bereichen der Sicherheitspolitik Unangenehmes nicht mehr einfach unter den Teppich gekehrt werden kann. Die Öffentlichkeit erhebt Anspruch auf detaillierte Transparenz sicherheitspolitischer Entscheidungen und Maßnahmen. Dies ist nicht nur ein britisches

Phänomen. Das Experiment der Chilcot-Kommission wird z. B. von der amerikanischen Nachrichtendienst-Gemeinde sorgfältig verfolgt als möglicher Vorläufer künftiger Untersuchungen auf ihrem eigenen Feld.

Für Zeitgeschichtler, Politikwissenschaftler, Völkerrechtler und Praktiker der internationalen Beziehungen stellt die Untersuchung eine unerschöpfliche Ressource dar, nicht nur als Steinbruch zur Stützung eigener Meinungen, sondern als ein komplexes Lehrstück von hohem Wert. Vor allem findet sich einzigartiges Material zur Innenansicht britischer Außenpolitik und Verteidigung. Bedenkt man, dass die weltpolitische Medienberichterstattung im deutschsprachigen Raum seit 2003 einen deutlich anderen Blickwinkel als in Großbritannien eingenommen hat, bietet sich hier eine Aufgabe und Chance gerade auch für deutsche Beobachter. Ein unvermitteltes Fortdauern der erheblichen Unterschiede in der Wahrnehmung der tatsachlichen Entwicklungen wäre kein guter Ausgangspunkt für die Gemeinsamkeit im Bündnis und in Europa.

britannicus

Klaus Becher schreibt als britannicus aus London, wo er das sicherheits- und technologiepolitische Beratungsunternehmen Knowledge & Analysis LLP leitet.
Der Beitrag gibt die persönliche Auffassung des Verfassers wieder.

THEMEN

Red Guests

Hacktivism of Chinese Characteristics and the Google Inc. Cyber Attack Episode

Introduction

China's legions of hackers, known as *Hongke* (Red Guests), hit headlines across the world on Jan 12, 2010. David Drummond, the Senior Vice President, Corporate Development and Chief Legal Officer of Google Inc. revealed that a "sophisticated" cyber attack had taken place on its infrastructure.[1] Google Inc. engineers, as reported in *The Washington Post*, *The New York Times* and *Marketwatch*, had suspected where the attack had come from in Dec 2009 and identified the location of the attackers in the People's Republic of China (PRC).

According to U.S. Congressional sources, reported subsequently in U.S. print media, the Chinese cyber attacks had targeted at least 34 U.S. companies including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical. Eli Jellenc of VeriSign's iDefese Labs, who helped some firms to investigate the attacks, and stated that the Chinese hackers were after the 'source code' of the targeted U.S. companies. The attackers employed multiple types of malicious codes against multiple targets. Security experts in the field believe that the cyber attacks constitute part of China's 'concerted political and corporate espionage' against its adversaries.[2]

The attacks resulted in a retaliation from Google Inc. and a reaction from the U.S. administration and the PRC, which exceeded all the past acrimonious exchanges. The development is a substantial change in the US threat perception against Chinese 'hacktivism'.[3]

Amidst China's denials and counter claims, several countries including India have since complained vigorusly about Chinese hackers.[4]

According to a release of IT security firm Sophos on Feb 3, 2010, China ranked third with 11.2% share after the U.S. (37.4%) and Russia (12.8%) among the top 10 malware hosting countries on the web across the world during Jan - Dec, 2009. There has been decline in China's share from 51.4% in 2007 and 27.7% in 2008. Inspite of official Chinese denials, the evidence of the role of China in the world of cyber warfare is quite clear.

The Google Inc. Cyber Attack Episode reveals both defensive and offensive character of China's computer network operations (CNO) against its targets. 'Self-Censorship' stipulation, which Google Inc. refused to comply with and threatened to leave China unless dropped and its Golden Shield (*jindungongcheng*) Project, some times referred as 'Great Firewall of China', operating directly under the command and controls of the

---

[1] http://googleblog.blogspot.cpm/2010/01/new-approach-to-china.html

[2] http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

[3] "Hacktivism" is a portmanteau of 'hack' and 'activism'. It carries a positive as well as negative connotation. However in both case, it relates to electronic direct action, combining programming skills and critical thinking. It is more often than not synonymous to malicious and destructive acts that could undermine the security of internet a technical, economic and political platform. The term was coined by techno-culture writer Jason Sack in a piece about media artist Shu Lea Cheang, published in InfoNation in 1995 while the first act of 'Hacktivism, as documented by Julian Assang, relate to 1989 incident of 'anti-nuclear WANK worm penetrated log screen of American DOE, HEPNET, and SPAN (NASA) connected with VMS world wide. Chinese "Hacktivists" made slightly late but sure footed debut right in 1997 and have, of late, added substantial technological muscles to their capabilities.

[4] The computers in the Prime Minister Office (PMO) were hacked on Dec 15, 2009. As per the statement of the then Indian National Security Advisor (NSA) M. K Naryanan, the attack came in the form of e-mail with a PDF attachment, containing a Trojan virus, which allows a hacker to access and to control a computer remotely and down load or delete files. Chinese Foreign Ministry spokesman Ma Zhaoxu formally denied China's hands. This was not the first time the Chinese hackers attacked Indian computer networks. Computers of nine key Indian embassies, including offices in the US, UK and Germany were infected by the mysterious GhostNet, A China based cyber espionage network. In the past three years, the GhostNet has infected Indian Informatics Centre (NIC) several times.

Chinese intelligence organization the Ministry of Public Security (MPS), happened to be at the core of all organized defensive efforts.[5] Cyber force, entrusted with computer network operations (CNO) discernibly holds the character for offensive operations. There are also Psychological Operations (PSYOPS) troops, mobilized to provide propaganda covers, to play an offensive-defensive role with a difference.

The paper is aimed at understanding the 'distinctive character' of 'Chinese Hacktivism', both in terms of institutional and individual activities and operations. There is essentially a 'pre-event hard side' and 'post-event soft side' of the operations. Leaving aside the specific 'pre-event hard side' of the Google Inc. episode, the paper will look into and focus on the basics of the Chinese cyber warfare infrastructure including the doctrine, responsible in part or entirely for the growth and development Chinese hacker organisations.

'Post-event soft side' of the Google Inc. episode has shown Chinese media, academic circle and the government machinery speaking as with one voice, characteristic of Chinese political governance. It lends credence to the explicit and/or implicit culpability of the Chinese state in the development of the Chinese hacker community. In turn, it arouses academic concern to understand whether the Chinese state could declare a cyber war against its potent adversaries with capability to disguise the origin of a so called distribution denial of service' (DDOS) attacks such as Russian government reportedly conducted in the case of the Baltic state of Estonia in April 2007 and Georgia in July 2008.[6]

The study has thus been organized to focus on: the Pool Size and Antecedents of Hacktivists; State Leverage and Synergy; and, Sources and Methods of Attacks. Postulates include: the Chinese hacktivism has grown in the past as a weapon of future war; the state and non-state hacktivists enjoy favourable policy and technical support for future growth and development. Even under permanent observation and with hi-tech security mechanism in place, China's competitors and adversaries, including India, face the prospect of continued cyber attacks.

Pool Size and Antecedents of Hacktivists

Chinese hacktivists tend to multiply fast both in number and skills. They constitute many layers of interest groups: malware tool developers, security researchers, and those in training. Since 1997, the notoriety of the Chinese hacktivists has come to encompass quite a large area of global cyber warfare activity.

James Mulvenon of the Center for Intelligence Research and Analysis, a consultant to U.S. intelligence agencies, put the number of trained Chinese military hackers at around 50,000 in 2008.[7] The U.S. Federal Bureau of Investigation had earlier put their number at 30,000 in 2003.[8] They have benefited from professional training at People's Liberation Army (PLA) Communication Command Academy, Wuhan, Hubei Province, National University of Defence Technology (NUDT), Changsha, Hunan Province, PLA University of Science and Engineering, Nanjing, Jiangsu Province, PLA Information Engineering University, Zhengzhou, Henan Province, to name only a few. China's People's Armed Police Force (PAPF), entrusted, inter alia, with the task of 'preservation of public order and security', hold 'several tens of thousands of cyber cops', who can at will switch from policing the Chinese web space to cyber warfare.[9]

There are some non-state hacktivist groups, operating across China. Scott J. Henderson has listed as many as 189 hacker groups in his seminal work, the Dark Visitor: Inside the World of Chinese Hackers, on the basis of their websites. Other estimates put the number Chinese non-state hacktivists at 250 groups. One of the prominent groups, China Red Hacker Alliance (*zhongguo hongke lianmeng*), has staggering over 400,000 individual hackers as its member.[10]

Some of the top Chinese hacker groups known for their proficiency, collaborate with the Alliance included Xfocus, Black Eagle Honker Base, NSFOCUS, Venus Technology, Evil Octal, and others. Further prominent Chinese hacker groups making their presence felt in the game include Goodwell, Lonely Swordsman, Glacier, Leaf, Flyingfox, Coolswallow, China Eagle Group, Wicked Rose, the NCPH Hacking Group, and Hacksa.cn. These and hundreds of Chinese hacker groups use, one way or the other, a large pool of 384 millions internet users, sharing some of the 232,446 million IP (Internet Protocol) addresses, 16,818 million

[5] PRC carries out internet censorship under a wide variety of laws and administrative regulations, which included Article 12, Article 14 and article 15 of the State Council Order No. 292, issued in September 2000 that makes it incumbent upon IIS provider to censor information as per the wishes of the Chinese government. Golden Shield project, launched in 1998 involved altogether 30,000 experts. The first part of the project lasted eight years and could be completed only in 2006. The work on the second part began in 2006 and completed in 2008. according to the CCTV, the project has cost China 6.4 billion YUAN (US$800 million)

[6] In May 2007, Urmas Paet, the Estonian Foreign Minister, accused the Kremlin of direct involvement in the attack of Estonian government sites and telephone networks in retaliation to the decision of the Estonian government to shift the Bronze Soldier Statue from the centre of the capital city Tallinn to a suburb, which the Russians considered disrespect.

[7] http://www.chinapost.com.tw/commentary/reuters/2010/01/22/241862/p2/Google-hacked.htm

[8] http://www.chinapost.com.tw/commentary/reuters/2010/01/22/241861/p2/US-fears.htm

[9] The evidence is borne of a statement of the Chinese Minister of Public Security Meng Jainzhu in the presence of several senior police officers while touring Anhui Province in Nov 2009. As reported in Chinese media (People's Daily, November 1, 2009; Ming Bao, November 2, 2009), Meng had then called upon 'several tens of thousands of cyber cops' to boost cooperation with companies in electronics and IT fields for the job in the presence of se

[10] Wendel Minnick, "Is Beijing behind Cyber Attacks on Pentagon", *DefenseNews*, June 2, 2008 http://www. defensenews. Com/story. php?i=3576373

domain names and 3,232 million websites.[11]

State Leverage and Synergy

The state leverage of Chinese hacktivists, both within and beyond the government is discernible at various levels and forms. The same holds true where it relates inter-group synergy. The PRC is however making a clear cut distinction between cyber crimes and cyber war, the former to safeguard its interests and the latter to impinge on the interests of the adversaries.[12]

China's non-state cyber groups have constantly attacked adversaries on issues that stand in the way of state policy. They have, accordingly, come to earn the honorific title of "patriotic hackers", whom China's military or state security departments turn to for their operations.[13] Elements of the present day China Red Hacker Alliance while part of Honker Union engaged U.S. hackers over the Hainan Island Incident, which related to a mid-air collision of U.S. Navy EP-3E Aries II signals surveillance aircraft with PLA Navy J-811 Interceptor fighter jet on April 1, 2001. They altered the page of the U.S. government website.[14]

They also altered the page of the U.S. Department of Labour and Department of Health and Human Services to display a picture of Wang Wei, the Chinese pilot who died in the collision. The page was titled "China hack!", and read in English: "The whole country is sorry for losing the best son of China – Wang Wei for ever. We will miss you until the day". Chinese hackers, masquerading under pseudonym of "Chinese Honker Team", quite possibly affiliated to China Red Hacker Alliance showed up and attacked Iranian websites in retaliation to Iranian hackers, pseudonym Iranian Cyber Army, venturing to take over China's search engine Baidu on Jan 12, 2010.[15] There are many such stories from Taiwan, Japan and other countries including India, involving one or the other Chinese hacker entities.

Notwithstanding, there is a move in China for the state and non-state hacktivist groups to evolve and work in a public private partnership (PPP) model, in particular where it relates to Research and Development (R&D). This is evident from China's preferential policies, extended to commercial computer and electronic enterprises, who share their resources and data with relevant units in the PLA, the Para-military People's Armed Police Force (PPF), the Ministry of State Security (MSS), and the Ministry of Public Security (MPS) and others. [16]

The First Research Institute of the MPS was of late in the forefront of recruiting Chinese graduates in areas including computers, engineering, mathematics and foreign languages. The same hold true about research units with the MSS. The advertisements are placed on government and private websites. The recruitment of such hackers is carried out under the guise of software engineers and Net-related security experts. The symbiotic relationship of the Chinese state with the Chinese hacktivists is equally evident in their training programmes, be it formal as part of information warfare (IW) or informal hacking training outfits.[17]

The Chinese hackers quite often hold seminars and run magazines with names such as Hacker X Files, Hacker Defense and the like and provide tips on how to break into computers and/or build a Trojan horse step by step. In the 'pre-event hard side' of the game, as per Willy Lam, senior cadres, such as Dr Jiang Mianheng, the eldest son of former Chinese President Jiang Zemin and the Vice Principal of the Chinese Academy of Sciences play a major role.[18] The process is bound to gather momentum as the 12th Five Year Plan (2011 - 2015) of the PLA on net-based combat systems, including cyber espionage and counter-espionage, is put in place.

In the 'post-event soft side' of the game, the Chinese hacking community draws on national support, far exceeding the symbiotic relations evident in the course of 'pre-event hard side'. It is a battle where the Chinese media, academia and officials come out in total denial and try to find even scape-goat whenever at all possible.

The Google Inc. Cyber Attack Episode stands as a clear testimony to the role of the Chinese media in Cyber Warfare. Using studied rhetoric, it sought to convince the world that Google Inc. was working on behalf of the U.S. administration to 'impose its values on other cultures in the

---

[11] http://www.marketreportchina.com/market/article/content/3376/201001/217340.html

[12] As China turned a virtual haven for internet crimes, China introduced three new articles to its criminal code, which has provision of seven years of imprisonment. Further, China has also broadened its definition of crimes committed on computers.

[13] New York Times, February 3; China News Service, January 25; Cnjz.cn [Beijing], November 1, 2009; Guofang.info [Beijing], September 17, 2009.

[14] http://www.china.org.cn/english/12150.htm

[15] The hack of Baidu.com has been authenticated by the Chinese print media, in particular the People's Daily, which published a screen grab showing a message reading: "This site has been hacked by the "Iranian Cyber Army", along side a picture of the Iranian flag. In a statement the company said, "Services on Baidu main website www.baidu.com were interrupted due to external manipulation of its DNS (Domain Name Server) in the US. Baidu has been resolving this issue and majority of services have been restored". Iranian hackers had reportedly retaliated Chinese Twitter users who used #CN4Iran hash tag to express support for opposition candidate promising reforms.

[16] China.com.cn, November 3, 2009; Apple Daily [Hong Kong], January 29, 2010; Asiasentinel.com [Hong Kong], January 22, 2010.

[17] China shut down Black Hawk Safety Net (3800cc.com), a group that sold training materials and malicious codes for illegal hacking in Feb 2010. Established in 2005, the group had 12000 paid and 170,000 members. There are yet tens of academies operating through out China. Some of the important non-state hacker training facilities, making news in the Chinese media for different reasons included Yinhe Info and Tech Academy and Beida Qingniao. The Chinese government entities known for turning out a larger number of hackers included Shanghai Jiaotong University and Lanxiang vocational school. Among Chinese military outfits, the China Academy of Military Sciences has earned equal notoriety.

[18] Willy Lam, "Beijing Bones up its Cyber Warfare Capacity", *China Brief*, Volume:10 Issue:3, February 4, 2010.

name of democracy'. *Global Times,* a tabloid owned by *People's Daily*, the mouthpiece of the communist Party of China (CPC), ran a number of articles including an editorial with the headline: "The world does not welcome the White House's Google".[19]

It sought to justify both Chinese censorship of internet content and cyber attacks as such with a difference. In a calculated defensive offensive, the *Global Times* named the U.S. as the very first country in the world to have created 'cyber army of 80,000 people equipped with over 2,000 computer viruses. Even where if true, a supposedly unscrupulous act of 'X' can not legally justify an unscrupulous act of 'Y'.

Chinese officials and experts stood behind the media offensive. In a statement, Zhou Yonglin, the Deputy Operations Director of the National Computer Network Emergency Response Centre (NCNERC), said: "Everyone with technical knowledge of computers knows that just because a hacker used an internet protocol (IP) address in China, the attack was not necessarily launched by a Chinese hacker." iDefense Labs among other security firms have testified that the IP addresses of attack on Google Inc. and other targets corresponded to 'single foreign entity consisting of either of agents of Chinese state or proxies there off'. Chinese Foreign Ministry spokesman Ma Zhaoxu justified the sordid game with a difference. He found gagging of internet contents as being necessary, in tandem with China's 'national conditions and cultural traditions'. As for the offensives of the Chinese hacktivists, Ma cited exiting legal stipulations that renders hacking a punishable crime in China.[20]

Going a step forward, Chinese academia in the field has been busy finding a scape-goat. Peter Lee, for example, found it expedient to suggest that the Google Inc. episode was a help to India, the 'U.S. ally' and 'China's emerging rival' and borne of two hard realities: U.S. business tycoon Google Inc. not 'doing well in China' and U.S. President Barrack Obama not 'doing well in United States'.

In the 'high profile confrontation with China',[21] Wang Yizhou, deputy chief of the Institute of World Politics and Economy at the Chinese Academy of Social Sciences characteristically tried to turn the table against the U.S. and said: "In the U.S., a country that boasts its Internet freedom, governmental supervision virtually infiltrates across the nation, and its influence further extends to worldwide servers. Information-searching via Google and online chatting through Windows Live Messenger are all under stringent surveillance, and the relevant agencies are tasked with compiling backups." Even if true, it can not justify China's actions.

In fact, Chinese hacktivism of the kind finds justification as being non-kinetic and are in tandem with China's two strategic doctrines: first, 'Gaining Information Dominance' (*zhi xinxi quan*) against potential adversaries; and secondly, adhering to 'Three Warfare' (*san zhong zhanfa*). [22] It is then in tandem with one of the 36 strategies of China's age old wisdom to 'kill with a borrowed sword'.[23]

Sources and Methods of Attacks

While not yet conclusive, Shanghai Jiaotong University and the Lanxiang Vocational School working closely together in the Google Inc. Cyber Attack Episode.[24] In the break-in, as Joe Stewart, a malware specialist with Atlanta based computer security firm SecureWorks, says, the hacktivists, in question, used a programme, based on an unusual algorithm, once discovered in a Chinese technical paper, published exclusively on Chinese language websites. The malware was a "Trojan Horse", capable of opening a backdoor of a computer on the Internet.

Beginning May 1999 when the Chinese hacktivists attacked U.S. government sites in retaliation to the accidental bombing of China's Embassy in Serbia, Belgrade, and through many of the 35 well known incidents, until the Jan 12, 2010 Google Inc. Cyber Attack Episode, and also including attacks in the U.S., Taiwan, Japan, New Zealand, Australia, South Korea, France, Germany and India, the methods, brought to bear upon for the purpose by the state and/or non-state Chinese hackers community fall into three major categories: the first is the use of e-mails for planting viruses; then phishing and lastly, the introduction of 'intelligent trojans' and 'vacuum trojans'. Tools employed, thus far, range from robotic and simple to brainy and sophisticated. For instance, Chinese hackers have quite frequently used a 'vacuum Trojan' to extract information from a pen drive automatically when connected to a USB port. It is also believed that the next step could be planting the targeted sites with the more difficult to detect fake data or partially fake data.

[19] Chinadigitaltimes.net/china-news/main/world

[20] Chinese official response to Google Inc. threat to pull out of China unless China allowed Google search engine to run uncensored came characteristically 11 days later on 24th Jan 2010 in almost premeditated way in the course of two interviews.

[21] Peter Lee, "Winner of Google-China Feud is India", *Asia Times*, Jan 28, 2010.

[22] "Three Warfare" doctrine combines psychological, media and legal warfare. Psychological warfare relates to use of propaganda, deception, threats, and coercion to degrade the ability of China's adversary to understand the objective situation and to make appropriate and effective decisions; media warfare pertains to dissemination of information to sway public opinion and obtain support from domestic and foreign audiences for China's forward actions; and, legal warfare stretches forth to use available domestic and international laws to substantiate legality of its operations.

[23] Sun Zi' s The Art of War lists 36 strategies, each of them expressed as proverbs and a story borne of on ground experiences through out the ages. "Kill with Borrowed Sword" is the third in sequence after 'Fool the Emperor to Cross the Sea' and 'Besiege Wei to Rescue Zhao'.

[24] Xinhua News Agency carried a rebuttal of the report in *New York Times* about the involvements of the two elite Chinese schools having close relation with the PLA. Quoting unnamed representative, the report said:"The report of the *New York Times* was based on an IP address. Given the highly developed network technology today, such a report is neither objective nor balanced".

China's cyber weapon capabilities have come to be considered quite advanced, assessed to be so far the fifth in ranking and making all out efforts to rival the U.S., the technological leader in the world of IW capabilities. The arsenal, in order of threats, encompasses and included: large, advanced BotNet for DDos and espionage, electromagnetic non-nuclear pulse weapons; compromised counterfeit computer hardware; compromised peripheral devices; compromised counterfeit computer software; zero-day exploitation development framework; advanced dynamic exploitation capabilities; wireless data communication jammers; computer virus and worms; cyber data collection exploits; computer and networks reconnaissance tools; embedded Trojan time bombs; and, compromised micro-processors and other chips.

Chinese media reports suggests that the Chinese IW units have been accessing, if not out sourcing R&D for developing viruses to attack the computer systems and networks of the adversaries, and tactics to protect friendly computer systems and networks. In Nanjing, the PLA has developed more than 250 trojans and similar tools. The Chinese Academy of Sciences, which provides suggestions about national information security policy and law, has established the State Lab for Information Security with 'National Attack Project' as one of its research programmes. Recently held military exercises bear out that the PLA has since increased the role of CNO and has been concentrating on offensive operations, primarily as first strikes against the networks of adversaries. The state and non-state Chinese hacktivist thus constitute a real threat to their adversaries until they are technologically matched and surpassed both in defensive and offensive operations.

Dr. Sheo Nandan Pandey,
Faridabad, India

Dr. Sheo Nandan Pandey, born Jan 14, 1947, served both institutions of higher learnings and the bureaucratic set up as member of Civil Services in India. He speaks several languages including Chinese mandarine. In area studies, China is his first love.

This analysis has been published by ISPSW/ETH Zürich on 8 March 2010.
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**.