Die Zukunft des Krieges –

Strategische Konzepte und strukturelle Probleme des Cyberwarfare

Dr. Sandro Gaycken

Universität Stuttgart / CCC

sandro.gaycken@philo.uni-stuttgart.de

Einleitung

Bereits in einigen gegenwärtigen, mit Sicherheit aber in immer mehr zukünftigen Konflikten wird vernetzte Informationstechnik eine wichtige Rolle spielen. Der Grund ist einfach. Wirtschaftliche, politische und militärische Prozesse des Steuerns und Entscheidens, des Kommandierens und des Wahrnehmens sind inzwischen informationstechnisch gestützt und über weitreichende Vernetzung prinzipiell zugänglich. So symbiotisch sind die Verbindungen teilweise schon geworden, dass ein Ausfall oder die Übernahme der Informationstechnik in diesen Bereichen oft dem Ausfall oder der Kontrolle ganzer gesellschaftlicher Grundlagen gleichkäme. Damit ist die militärische Bedeutung klar. Informationstechnologien sind zu attraktiven Zielen gewachsen, die in der Zukunft im Rahmen von Konflikten mit angegriffen werden können. Weiter besonders attraktiv ist, dass die Komplexität und Globalität der Vernetzung gut getarnte und außerordentlich differenzierte Angriffe auf verschiedenste Ziele an jedem Punkt der Erde von jedem Punkt der Erde möglich machen. Sowohl Reichweite als auch strukturelle Eigenständigkeit rechtfertigen dabei die Kondensation entsprechender militärischer Überlegungen in einem eigenen und neuen Bereich der Kriegsführung, der sich gegenwärtig etabliert: Cyberwarfare. Cyberwarfare bezeichnet die Kriegsführung unter Einbindung vernetzter Information als Waffe und Ziel. Die Begriffsführung ist im militärischen Bereich allerdings nicht besonders streng. In verschiedenen Variationen kann Cyberwarfare auch als Begriff für rein physische Angriffe auf Computersysteme genutzt werden wie auch für Operationen, die traditionell dem Electronic Warfare zugerechnet wurden. Die erste Verwendung scheint allerdings sinnvoller. An ihr entlang soll im Folgenden eine kurze Skizze dazu gezeichnet werden, wie sich dieser Bereich versteht, mit was für Problemen er zu tun hat und was bereits passiert ist und wozu er in der Zukunft werden könnte.

Ziele und Operationstypen des Cyberwarfare in der 3I-Heuristik

Der Einsatz von Cyberwarfare ist aus militärischer Perspektive dort sinnvoll, wo militärisch relevante gegnerische Strukturen wesentlich unter

dem Einfluss von Informationstechnik stehen. Das reale Spektrum möglicher Ziele ist damit erst einmal breit[1], was zu einer Unübersichtlichkeit des Feldes führt, die gegenwärtig als eine zentrale Schwierigkeit für schnelles, strategisches Denken erachtet wird. Eine heuristische Zusammenfassung soll in einem „3I-Ansatz“ versucht werden. Als wesentliche Ziele werden in diesem Ansatz Infrastrukturen, Informationen und Identitäten aufgeführt.

Der Begriff der Infrastruktur muss zunächst erweitert werden. Während die klassische Definition einer Infrastruktur diese großformatig als Grundstruktur technischer oder organisatorischer Art begreift, von der erst in der Größendimension von Staaten sinnvoll gesprochen werden kann, soll präzise die Größendimension in der hiesigen Verwendung ausgeklammert werden. Als Infrastruktur soll eine jede technische oder organisatorische Grundstruktur unterschiedlicher Konglomerate sozialer Prozesse verstanden werden, sofern sie für die auf ihnen aufbauenden Prozesse notwendige, ermöglichende Bedingungen herstellt. So verstanden stellt das Börsensystem mit seinen organisatorischen Strukturen wie den Handelszeiten und einigen technischen Prozessen wie dem Large-Value-Transfer-System (LVTS) eine Infrastruktur für eine Reihe nationaler und globaler finanzieller Prozesse dar. Aber auch die Menge der operativen technischen Systeme und Organisationsstrukturen einer Militäroperation als (vage) umrissenes Konglomerat sozialer Handlungen kann als Infrastruktur verstanden werden, die sich in diesem Fall lediglich auf lokal spezifische Prozesse bezieht. Die Größenbestimmung kann schließlich als Zusatzmerkmal wieder eingeführt, in drei zu berücksichtigenden Größenordnungen: global, national und lokal. Drei weitere wichtige Merkmale bei Infrastrukturen sind der Mangel von Redundanzen, enge Kopplungen und Unintelligibilität. Der Mangel von Redundanzen bezeichnet den Umstand, dass Infrastrukturen in der Regel ohne Ausfallsysteme existieren. Zwar gibt es innerhalb der meisten Infrastrukturen mehrere Redundanzen für deren Teilprozesse. Fallen die Systeme allerdings vollständig und dauerhaft aus, sind die durch sie ermöglichten Prozesse in der Regel nicht mehr durchführbar. Durch den mit der Technisierung zusammenhängenden Kompetenzverlust sind außerdem auch kaum mehr Prozessalternativen bekannt. Nahrungsbeschaffung für Großstädter ohne Logistik, Strom und sonstige Energie wäre ein Beispiel. Bei derartigen Ausfällen kann dann zusätzlich das zweite Merkmal der engen Kopplungen relevant werden. So gilt von den meisten Infrastrukturen, dass sie eng mit verschiedenen anderen Infrastrukturen verbunden sind. Beinahe alle Infrastrukturen etwa hängen von der Funktionalität der Strominfrastruktur ab, die Finanzinfrastruktur

[1] Vgl. etwa Clay Wilson, „Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues“, CRS Report for Congress RL 31787, Washington 2007

aber auch schon von der Logistikinfrastruktur. Der Ausfall einer Infrastruktur kann also interinfrastrukturelle Kaskadeneffekte verursachen, die sich durch verschiedene weitere Infrastrukturen fortsetzen und unvorhersehbare Schäden bis zu katastrophalem Ausmaß verursachen können.[2] Schließlich kommt das dritte Merkmal hinzu, dass Infrastrukturen aufgrund ihrer zahlreichen Kopplungen nicht mehr vollständig intelligibel sind, so dass eine Vorhersage des Verhaltens von Infrastrukturausfällen oder eine präzise Bestimmung möglicher Fehler auch mit vielen Experten in komplexen Fällen eher Glückssache als planvoll durchführbare Unternehmung sein wird. Zu diesem Merkmal der Komplexität wird später noch mehr zu sagen sein. Indem informationstechnische Netze ebenfalls komplex sind, wird Komplexität zu einer Basiseigenschaft für alle Formen von Cyberwarfare.

Der Zusammenhang zwischen Infrastrukturen und Cyberwarfare kommt schließlich dadurch zustande, dass Infrastrukturen in der Regel vernetzt und informationstechnisch gestützt sind. Aufgrund des prozessualen Charakters von Infrastrukturen spielen bei dieser technischen Stützung vor allem Steuerungen eine zentrale Rolle. SCADA-Verfahren sind hier ein gutes Beispiel. Dies gilt für lokale, nationale und globale Infrastrukturen gleichermaßen, so dass die Steuerung von Infrastrukturen über Cyberwarfare als prinzipiell angreifbar gelten muss. Die Steuerung von Infrastrukturen kann folgend verschiedenartig militärisch interessieren und strategisch eingebunden werden. Die Ausschaltung nationaler oder operativer Infrastrukturen kann etwa im Rahmen von Shock-&-Awe-Operationen erwogen werden, die mit massiven Militärschlägen eine möglichst rapide Demoralisierung des Gegners beabsichtigen. Schon die kurzfristige Ausschaltung nationaler Infrastrukturen würde aufgrund der skizzierten Merkmale zu erheblichen Bindungen von Kräften führen (der Great Northeast Blackout (2003) war vermutlich so ein Angriff[3]), während langfristige Ausfälle (als langfristig wird bereits ein Zeitraum von zwei Wochen erachtet) katastrophale Auswirkungen auf eine Bevölkerung oder – lokal – auf eine soziale Struktur haben. Analyst Clay Wilson hat die Auswirkung eines dreiwöchigen Stromausfalls in einer Großstadt einmal (nicht wissenschaftlich, aber sicher treffend) mit der Wirkung von „50 hurricanes“ verglichen.

[2] Vgl. Charles Perrow, Normal Accidents, Princeton 1984. Oder für globale komplexe Systeme: Chris Demchak, Sandro Gaycken, „Critical Public Systems’ Adaptation for the Emerging Global Socio-Technical Infrastructure”, in: Public Administration Review, Special Issue – The Future of Public Administration in 2020, i.E.

[3] Siehe Shane Harris, “China’s Cyber-Militia”, in: National Journal Magazine May 2008, online unter: http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php, Zugriff: 21.10.2008

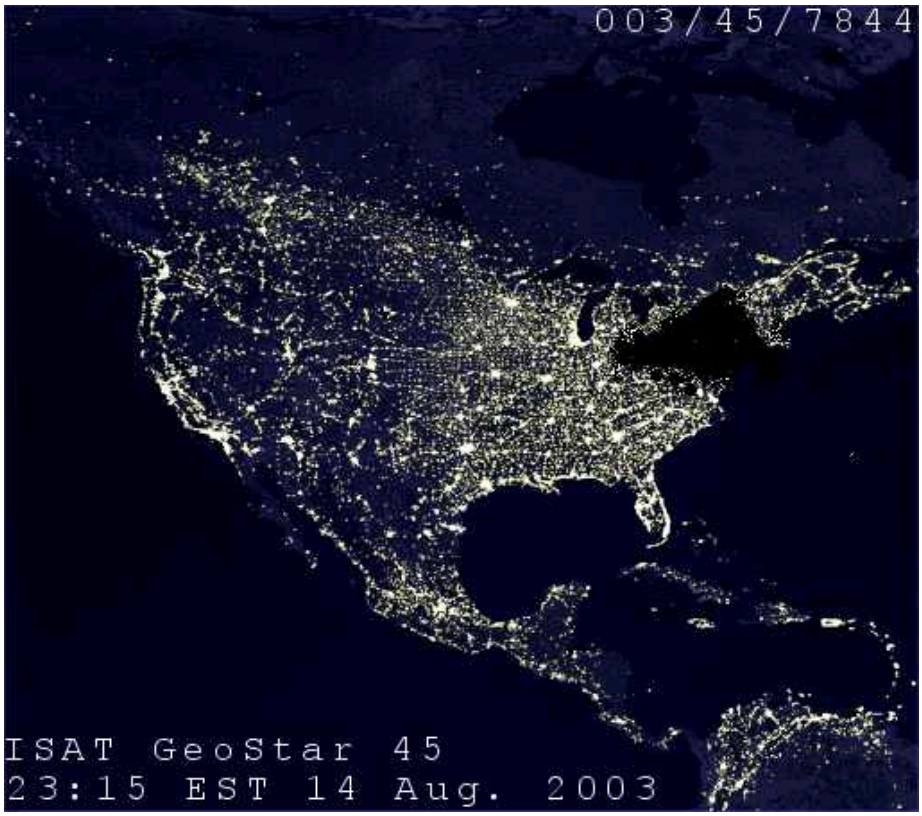

Abbildung: Der Great Northeast Blackout 2003

Gezieltere Kontrolle spezifischer nationaler Infrastrukturen kann im Verbund mit besonderen Strategietypen militärisch relevant werden. So ist die Kontrolle von Wirtschaftsinfrastrukturen im Rahmen einer wie von den USA nach Eisenhower verfolgten „Grand Strategy“ interessant, wenn wesentlich wirtschaftliche Elemente als Mittel der Außenpolitik einbezogen werden. Die Kontrolle von Medieninfrastrukturen kann im Rahmen von Information Operations und Psychological Operations erstrebenswert sein, indem über die kontrollierten Medien – je nach taktischer Stoßrichtung – ausgewählte Wahrheiten, Propaganda und Desinformationen verbreitet werden können. Allerdings soll dieser Aspekt erst näher unter dem nächsten Unterpunkt „Information“ besprochen werden. Wichtig ist noch der Hinweis auf die Möglichkeit von Cyberangriffen auf operative militärische Infrastrukturen. Bekannt sind derzeit Angriffe auf Logistiksysteme, sowie Hacks von Drohnen oder auch von Blue-Force-Tracking-Systemen, einem High-Tech-System, das dem Soldaten über einen Minibildschirm mit blauen und roten Punkten in einer Geländeabbildung anzeigt, wo Freund und Feind stehen und wo der Abgrund anfängt. Cyberangriffe auf operative militärische Systeme sind auch bereits als Dienstleistungen durch spezialisierte Söldnereinheiten käuflich.

Zum zweiten Punkt: Informationen. Auch hier muss der Begriff spezifisch erweitert werden. Er soll nicht nur einzelne Informationen, sondern auch

zu Wissen konglomerierte Informationen umfassen. Als militärisch relevante Ausdehnungen ergeben sich drei Formen von Wissen. Erstens ist Wissen als Wissen von Grundlagen zu nennen. Es liegt in grundlegenden Meinungen, Einstellungen und Expertisen vor und findet sich etwa als naturwissenschaftliches, technikwissenschaftliches oder als soziokulturelles oder politisches Basiswissen. Zweitens ist Wissen als Wissen von Verfahren zu nennen. Dieses Wissen ist Wissen als Knowhow oder in Plänen und gibt die konkreten Verfahren von Gestaltungen oder Organisationen an. Drittens schließlich ist Wissen als Wissen von Situationen zu nennen, das sich auf die aktuelle Bekanntheit mit situativen Parametern bezieht. Die militärische Relevanz dieser drei Wissensformen ergibt sich durch ihre enge Einbindung in gesellschaftliche Prozesse. Besonders in der Wissensgesellschaft sind gesellschaftliche Empfindungen und Entscheidungen eng an eine solide Fundierung durch Wissen gekoppelt. Wissen tritt so als Entscheidungsgrundlage für Politik, Öffentlichkeit und Militär in Erscheinung, als Produktionsgrundlage der Wirtschaft (den Thesen der Wissensgesellschaft folgend sogar als inzwischen primär relevanter Marktvorteil) oder als Gestaltungsgrundlage technischer und organisatorischer Strukturen und Prozesse.[4] Es bildet eine ökonomische, strukturelle und dezisionale Basis der Wissensgesellschaft. Der Zusammenhang zu Cyberwarfare ergibt sich, indem Wissen zunehmend vernetzt und informationstechnisch verwaltet und verbreitet wird. So ergeben sich technische Eingriffsmöglichkeiten in die wissensbasierten gesellschaftlichen Prozesse. „Information Superiority“, beziehungsweise „Information Dominance“ werden zu einer Untermenge von Zielen des Cyberwarfare.[5] Die bereits genannten Information Operations etwa wenden sich bevorzugt an Grundlagenwissen, indem sie auf verschiedenen Wegen wahre oder falsche Sachlagen im eigenen Interesse verbreiten.[6] Das kann sich an Medien richten, bei deren Übernahme eine Reihe von Operationen mit verschiedenen Zielen zwischen Propaganda, Demoralisierung und Verwirrung (FUD-Strategien) möglich werden.[7] Es kann aber auch wissenschaftliches und operatives

[4] Vgl. auch Christoph Hubig, Unterwegs zur Wissensgesellschaft – Grundlagen, Trends, Probleme, Düsseldorf 2000

[5] Vgl. DOD Information Operations Roadmap, online unter: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf, Zugriff: 12.10.2008

[6] Vgl. für einige Szenarien: Threats Working Group, „Threats Posed by the Internet“, CSIS Commission on Cybersecurity Report, online unter: http://www.csis.org/media/csis/pubs/081028_threats_working_group.pdf, Zugriff: 11.12.2008

[7] Obwohl die in den USA vertretene Meinung, dass mit dem internetbedingten Verlust der Mediendominanz durch Massenmedien die Terrorgefahr allgemein steige, faktisch falsch und freiheitsrechtlich hochbedenklich ist. Vlg. John Arquilla, David Ronfeldt, Networks and Netwars: The Future of Terror, Crime and Militancy, Santa Monica 2002 sowie das Soldatenhandbuch zu Cyber Operations der US-Armee, DCSINT Handbook No. 1.02, “Cyber Operations and Cyberterror”, online unter: http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA456238&Location=U2&doc=GetTRDoc.pdf, Zugriff: 10.01.2009

Verfahrenswissen angegriffen werden, wie im Fall der bekannten Operationen Titan Rain[8] und GhostNet[9]. Bei beiden scheinbar aus China stammenden Angriffen wurden nicht nur Informationen abgerufen und damit Investitionen in nationale Innovationsvorsprünge nivelliert (was zur Einführung des neuen Schadenstyps „Informationelle Verluste“ geführt hat[10]).

Abbildung: Spiegel-Illustration zu chinesischen Hacker-Angriffen

Es besteht auch der Verdacht, dass bestehende strategische oder Rüstungsinformationen gelöscht oder sabotiert wurden. Die dabei entstehenden Schäden sind besonders hoch, da Fehler, die mit wissenschaftlicher Sorgfalt in ein Verfahrenswissen eingebaut wurden, auch durch die ohnehin schon kosten- und zeitintensiven Prüfungen kaum zu entdecken sind und ihre defektierende Wirkung folglich oft erst im Einsatz entfalten. Derartige Sabotageakte an Verfahrenswissen können also situatives Versagen vorprogrammieren. Alternativ ist bei dieser Form des Angriffs auch der Einbau „systemischen Versagens“ möglich, das präzise auf die Verursachung von Cross-System- oder intra- und interinfrastrukturellen Kaskadeneffekten abzielt. Dabei wäre auch die bisher noch wenig diskutierte Option der Sabotage grundlagenwissenschaftlichen Wissens zu bedenken, wenn es sich um Wissen handelt, dass in Entscheidungs- und Gestaltungsprozesse einfließt. Die Erstellung falschen Situationswissens kann schließlich als eine klassische Täuschungsoption in verschiedenen operativen und taktischen Kontexten interessant sein. Als Beispiel wurde oben bereits der Hack des Blue-Force-Tracking-Systems beschrieben. Drohnen und andere

[8] Die Operation „Titan Rain“ beschreibt eine Serie von über 79.000 Angriffen aus US-Regierungs- und Rüstungsrechner im Jahr 2004, von denen 1300 erfolgreich waren.
[9] GhostNet ist ein netzwerkartiger Angriff mit dem Spionagevirus Gh0stRAT, entdeckt im März 2009, der auf diversen Rechnersystemen weltweit Spionage betrieben und ein Botnet aufgebaut hat.
[10] Vgl. James Lewis et al, “Securing Cyberspace for the 44th Presidency“, CSIS Commission on Cyber Security Report, online unter: http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf, Zugriff: 11.01.2009

Aufklärungssysteme bis hin zu Satelliten[11] sind weitere attraktive Ziele. Eine mit allen Wissensformen befasste Form der Kriegsführung, in der Cyberoperationen inzwischen eng eingebunden sind, ist der gegenwärtig noch junge Control-&-Command-Warfare (C2W). In den dazu existierenden Doktrinen wird davon ausgegangen, dass nicht primär die technischen, sondern die menschlichen Potentiale eines Gegners angegriffen werden müssen und unter diesen wiederum primär die Fähigkeiten zur Entscheidung und Kontrolle, was wesentlich über die Kontrolle von kommandorelevanten Systemen und Informationen Weisen passieren soll. Dabei kann C2W in Kriegs- ebenso wie präventiv in Friedenszeiten gegen Feinde oder potentielle Feinde ausgerichtet werden und umfasst neben Cyberoperations eine Reihe weiterer Operationstypen wie die Sicherung der eigenen Operationsfähigkeit (Operation Security (OPSEC)), Military Deception, Psychological Operations (PSYOPS) oder Electronic Warfare.

Schließlich kann Identität als Zielgruppe verstanden werden. Dieser Bereich ist insgesamt noch gering beforscht. Es sollte aber eigenständig betont werden, dass in informationstechnischen Netzen neben den skizzierten Formen von Wissen auch eine besondere Unterform von Informationen verfügbar ist, nämlich Informationen über Identitäten. Ihre Besonderheit liegt insbesondere darin, dass sie quer zu den beiden anderen Kategorien liegen. Zum einen stellen sie selbst militärisch nutzbare Informationen dar, zum anderen besteht ihre Relevanz aber primär auch durch die Möglichkeit des Zugriffs auf Infrastrukturen. Damit ist auch bereits ein militärischer Nutzen von Identitätsinformationen erwähnt. Identity Theft und Identity Fake können genutzt werden, um eine Reihe cybermilitärischer Ziele zu realisieren, da man sich damit Zugang zu Infrastrukturen und Informationen verschaffen kann. Daneben bieten Identitäten aber auch noch andere Optionen. So können über kriminalistisch bereits vorhandene Systeme des Rasterns oder Profilings präzise Informationen über strategisch relevante Personen und Netzwerke erstellt werden. In Verbindung mit eventuell verfügbaren Positionsdaten können diese sogar für direkte militärische Angriffe genutzt werden. So hat die russische Armee in ihrem Tschetschenien-Feldzug einen Tschetschenenführer in einer strategisch günstigen Versammlung mit anderen Anführern mit einer Precision-Guided-Missile direkt an seinem Handy ausschalten können. Allerdings benutzen die Tschetschen (wie seit einer Weile auch alle Terroristen, Taliban und aufständischen Iraker) seitdem keine Handys mehr. Der Fall zeigt aber, dass der digitalen Identität, dem Data Double, eigenständige militärische Bedeutung beizumessen ist.

Strategische Besonderheiten des Cyberwarfare

[11] Die Falun Gong-Sekte hatte im August 2003 bereits kurzfristig den chinesischen Fensehsatelliten „Sino“ in ihrer Hand.

Für Cyberoperations wird also ein großes Spektrum möglicher Ziele sichtbar. Bei allen Formen von Cyberoperationen müssen allerdings die besonderen Strukturen des Cyberspace als neue Umgebungsbedingungen mit teilweise recht spezifischen Problemen berücksichtigt werden. Insbesondere die veränderten Raum- und Zeitverhältnisse, mögliche Folgen der Komplexität informationstechnischer Systeme und Netze, die Abwesenheit effizienter Verteidigungs- und Attributionskonzepte sowie die spezifische Kostenstruktur von Cyberoperationen stellen gegenwärtig noch Probleme für klassisches strategisches Denken dar.

Die veränderten Raum- und Zeitverhältnisse sind häufig problematisch, da Militärs derzeit noch dazu tendieren, den Cyberspace als einen zusätzlichen Operationsraum zu behandeln (die anderen sind Land, Wasser, Luft und Weltraum), was zu Assoziationen mit normalen raumzeitlichen Verhältnissen führt und in der Folge zu konzeptionellen und Verständnisschwierigkeiten.[12] Unter veränderten Raumbedingungen wäre etwa die rhizomatische Struktur des Netzes anzuführen[13], die auch nur bereichsspezifisch zentralisierte Kontrolle zu Verteidigungs- oder Angriffszwecken unmöglich macht. Außerdem werden durch die Globalität und die durch Normierung produzierte globale Homogenität des Netzes räumliche Entfernungen und Hürden bedeutungslos. Das Pentagon ist von jedem Punkt der Erde erreichbar. Als neue Zeitbedingung muss etwa berücksichtigt werden, dass Cyberangriffe auch aus großen Entfernungen und unter Einbindung vieler hundertausender Akteure (in einem Botnet zum Beispiel) instantan stattfinden können, allerdings ebenso auch spezifisch verzögert werden können. Auch die folgenden Schäden können noch recht spezifisch zeitlich gesteuert werden, indem sie situativ-temporär oder dauerhaft gestaltet werden können. Weitere Zeitfaktoren sind Veränderungen in der Reaktivität, die mit der noch zu besprechenden Attributionsproblematik zusammenhängen. So können Cyberangriffe nur unter erheblichem Zeitaufwand überhaupt auf einen konkreten Angreifer zurückgeführt werden, was schnelle Reaktionen grundlegend verhindert. Schließlich kommt die hohe Entwicklungs- und Wandlungsrate von informationstechnischen Programmen und Strukturen dazu. Ein Angriffstyp kann durch Neuentwicklungen über Nacht sinnlos werden.

---

[12] Siehe etwa Rati Bishnoi, “Navy Eyes Fighting in Cyberspace”, in: Inside Defense, online unter: http://www.military.com/features/0,15240,119664,00.html, Zugriff: 15.2.2009. Michael Wynne „Cyberspace as a Domain in which the Airforce Flies and Fights”, Kommentar zur C4ISR Integration Conference, Crystal City, Va., Nov. 2, 2006, online unter: http://www.iwar.org.uk/iwar/resources/cybercommand/speech.htm, Zugriff: 28.1.2009

[13] Ein Rhizom bezeichnet ein natürlich gewachsenes Geflecht. Zur Übertragung auf gesellschaftliche und technische Zusammenhänge siehe Gilles Deleuze, Felix Guattari, Rhizom, Berlin 1977 oder Gilles Deleuze, Felix Guattari, 1000 Plateaus – Kapitalismus und Schizophrenie, Berlin 1992

Komplexität spielt wie bereits angedeutet eine essentielle Rolle im Cyberwarfare, indem die informationstechnischen Netze durchgehend als komplex einzuschätzen sind. Sie sind eng gekoppelt, unübersichtlich und unverständlich und teilweise ohne Redundanzen, so dass sich Fehler kaskadenförmig ausbreiten können, nur schwer gefunden und aufgehalten werden können und katastrophale Wirkungen auf die betroffenen Prozesse haben können. Auch menschliche Faktoren sind einzurechnen, die sich im Angriffsfall über Social Engineering einbeziehen lassen. Ein Angriffsszenario auf ein Kraftwerk etwa hat sowohl normale technische Prozesse als auch die operativen Abläufe des Accident Managements genutzt, um mittels eines Cyberangriffs auf verschiedene Pumpen und die Schadensanzeigen im Kraftwerksraum die Operatoren zur Initiation einer Kaskadenkatastrophe zu veranlassen. Für strategisches Denken ist diese soziotechnische Komplexität bedeutsam, da sie ein „hackishes“ und holistisches Verständnis vom Cyberspace als Operationsraum einfordert, das selbst kleinste und abwegige technische und soziale Kausalverhältnisse einbezieht. Zudem muss das operative Verständnis auch eine möglichst vollständige Kenntnis aller Teilstreitkräfte umfassen, da der Cyberoperationsraum durch die Informatisierung aller mit anderen Operationsräumen befassten Teilstreitkräfte quer zu diesen liegt und mittelbar eben auch nicht-technische oder Low-Tech-Bereiche erreichen kann. Angriffe können also ihre Kernwirkungen in außergewöhnlich abwegigen Zielen zeitigen und auf exotischen Wegen ablaufen. Das gilt auch für Schadenstypen. So wurde im aktuellen CSIS-Report zur Situation des Cyberwarfare in den USA mit Bestürzung konstatiert, dass man sich auf infrastrukturelle Schäden eingerichtet hatte, während man aber bereits seit einigen Jahren den neuen und unerwarteten Schadenstyp der „informationellen Verluste“ durch Verlust und Sabotage von Verfahrenswissen erlitt.[14] Die Möglichkeit von Kaskadeneffekten ist außerdem in zwei weiteren Hinsichten bedeutsam. Zum einen – das haben die Untersuchungen großtechnischer Unfälle gezeigt – sind es vor allem kleine und scheinbar unbedeutende Funktionen, die katastrophale Kaskaden auslösen oder ihre Bewältigung verhindern. Eine Kernproblematik bei diesen kleinen Funktionen ist dabei der Umstand, dass diese Funktionen im normalen Betrieb bereits zahlreich gelegentlich ausfallen und daher vom Operationspersonal als normale Ablaufsfehler interpretiert werden. Bestimmte strukturelle Verbindungen kleiner Fehlfunktionen können allerdings leicht zu katastrophalen Unfällen führen. Gute Cyberangriffe werden sich also mit strukturellen Angriffen über unbedeutende Funktionen hervorragend tarnen können, unter Umständen bis zu einem point of no return. Eine weitere Konsequenz der Kaskadenfehler ist, dass weder Angreifer noch Verteidiger zu irgendeinem Zeitpunkt die genauen Auswirkungen eines Cyberangriffs vorhersagen

[14] Siehe Bemerkung Fußnote Zehn.

können. Dabei spielen auch die veränderten Raum- und Zeitbedingungen eine Rolle. Cyberangriffe können unter Umständen sofort oder mit Verzögerung in vollkommen unbeteiligten Ländern noch große Schäden anrichten. Aus diesem Grund wurden auch geplante Cyberangriffe im Kontext der Operation Iraqi Freedom auf irakische Finanzinfrastrukturen nicht durchgeführt. Analysen zeigten enge strukturelle Kopplungen zu europäischen Finanzsystemen, so dass ein Angriff unter Umständen Teile des europäischen Bankenwesens zu Fall gebracht hätten.[15] Damit entsteht auch ein wichtiges kriegsrechtliches Problem. Die Haager Landkriegsordnung ebenso wie die Genfer Konvention sehen nämlich die klare Unterscheidung von Kombattanten und Nicht-Kombattanten vor, wobei Angriffe auf zivile, nicht kämpfende Ziele entsprechend zu ahndende Verstöße gegen internationales Kriegsrecht darstellen. Da vollkommen präzise Schläge im Cyberspace prinzipiell nicht möglich sind, ist die Gefahr des Verstoßes gegen Kriegsrecht also latent.

Ein weiteres zentrales Problem stellt der Mangel an effizienten Verteidigungskonzepten gegen Cyberangriffe dar. Denn während zwar die Blockierung von Exploits und Backdoors einmal aktiver und erkannter Angriffe verhältnismäßig einfach ist, ist das primär relevante präventive Entdecken und Vermeiden erheblich schwieriger.[16] Für Exploits schaffen Softwarediversitäten wie verschiedene Programme, Programmversionen, Operationssysteme oder Kompositionen immer noch ausbeutbare Fehler, deren Entdeckung nach wie vor viel Zeit, Mühe und Knowhow erfordert – vor allem bei Closed Source Software. Ohne Ansätze zur homogenisierten, entkomplexierten Nutzung von Open Source Software in strategisch relevanten Bereichen sind diese Schwächen also nicht ausräumbar und Cyberdefense wenig effizient. Verteidigungskonzepte wie das „Defense-In-Depth“ bauen zwar derzeit auf eine schichtenartige Erhöhung von Sicherheitsprogrammen auf sensible Systeme. Allerdings wird damit zum einen für Exploits nur der Zeitaufwand erhöht, ohne qualitativ hochwertigere Sicherheit zu gewährleisten. Zum anderen sorgen die vielen Schichten für einen erhöhten Rechenaufwand und eine verbreiterte Angriffsfläche für Anfragen, so dass entsprechend geschützte Systeme immer noch leicht mit Denial Of Service-Angriffen lahmgelegt werden können – nach Untersuchungen sogar um einiges leichter als nicht entsprechend verteidigte Systeme.[17] Andere effiziente Verfahren sind derzeit kaum in Sicht.[18]

[15] Siehe Charles Smith, „Cyber War Against Iraq “, in: NewsMax.com, online unter: http://archive.newsmax.com/archives/articles/2003/3/12/134712.shtml, Zugriff: 23.8.2008
[16] Vgl. Center for Strategic and International Studies (CSIS), Cybercrime…, Cyberterrorism…, Cyberwarfare…: Averting an Electronic Waterloo, Washington 1998
[17] Vgl. Dorene Kewley, John Lowry, “Observations on the effects of defense in depth on adversary behavior in cyber warfare”, online unter: www.bbn.com/resources/pdf/USMA_IEEE02.pdf, Zugriff: 21.10.2008

Backdoors schließlich sind derzeit für Verteidigungskonzepte ein noch größeres Problem. Solange strategisch relevante Rechensysteme auch nur minimal mit Commercial Of The Shelf-(COTS-)-Produkten betrieben werden, deren Herstellung nicht im Bereich und unter der Kontrolle nationaler Souveränität liegt, können Backdoors nicht ausgeschlossen werden. Ohne vollständig eigenständige Hardware wird außerdem auch jede Nutzung von Open Source Software zur Vermeidung von Exploits sinnlos, da der von der Hardware mitgebrachte Code jederzeit eine Backdoor enthalten kann, was die Mühen eines Exploits überflüssig macht.

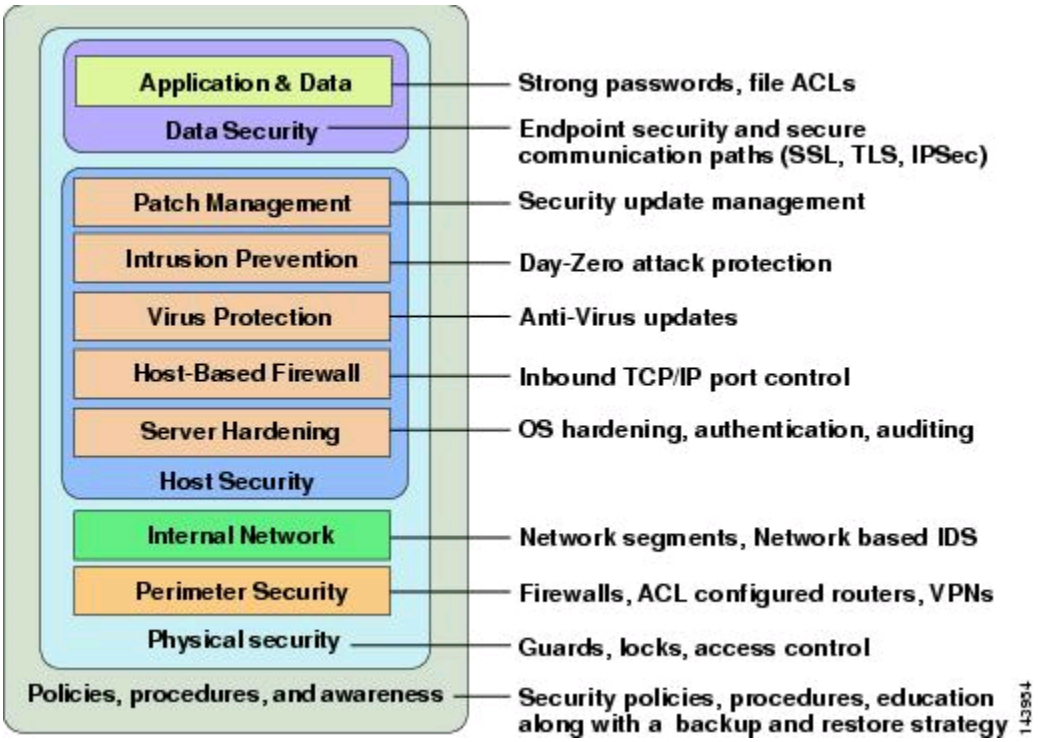

Abbildung: Defense in Depth

Die Attribution von Angriffen, also die Identifikation von Angreifern, ist schließlich ein weiteres strategisches Problem. Die Attribution von Cyberangriffen ist notwendig unsicher. Zum einen haben Angreifer mehrere nur schwer und zeitaufwändig rekonstruierbare und zudem mehrfach miteinander kombinierbare Möglichkeiten der technischen Tarnung ihrer Identität. Verschiedene Formen des Spoofing, die Nutzung von Reflektor-, Stepstone- oder Zombiehosts oder normale Netzwerkzeuge wie Network Address Translation können hier gut genutzt werden, so dass

[18] Siehe Walt Tirenin, Don Faatz, „A Concept for Strategic Cyber Defense“, in: Military Communications Conference Proceedings MILCOM 1999, online unter: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=822725, Zugriff: 21.20.2008 oder Sami Saydjari, “Structuring for Strategic Cyber Defense: A Cyber Manhattan Project Blueprint”, Proceedings 2008 Annual Computer Security Applications Conference, online unter: http://www.acsac.org/2008/program/keynotes/saydjari.pdf, Zugriff: 10.1.2009

nahezu sichere Identifizierungen oft nur durch physischen Zugriff auf die entsprechenden Rechner und durch die Unterstützung klassischer Aufklärung zu leisten sind. Zum anderen wird jede Attribution zusätzlich durch die mögliche Globalität von Angriffen erschwert. Angriffe können prinzipiell durch mehrere Länder geroutet werden, wodurch Identifikation nahezu unmöglich wird, sobald eines dieser Länder seine Kooperation in der Aufklärung verweigert. Außerdem ist unter diesem Punkt auch erneut die kriegsrechtliche Problematik der Unterscheidung von Kombattanten und Nicht-Kombattanten zu nennen. Kriegerische Rückschläge gegen Cyberangriffe würden eine zumindest hohe Attribuierbarkeit voraussetzen müssen, was aber nicht gewährleistet werden kann. In allen bisherigen Fällen konnte nicht einmal ein Staat als prinzipieller Akteur nachgewiesen werden.

Zuletzt ist die spezifische Kostenstruktur des Cyberwarfare als relevanter Punkt zu nennen. Die Entwicklung von gezielten Cyberangriffen ist verhältnismäßig teuer und aufwändig. Ein Klasse IV (die höchste Klasse) Angriff allein umfasst bereits eine komplexe Abfolge von Schritten, bei denen jeder einzelne mit hohem Zeitaufwand, Kosten und Knowhow zu assoziieren ist. Die einmal entwickelten Angriffstools haben außerdem noch eine Menge verschiedener Nachteile. Erstens sind sie meist nur für eine bestimmte und unter Umständen kurze Zeit überhaupt nutzbar, nämlich solange, bis der Fehler oder die Backdoor gefunden wurde, der oder die genutzt werden sollte. Zweitens gilt für einen einmal aktivierten und beobachtbaren Angriff, dass der Gegner relativ leicht weitere Angriffsziele als das erste gegen einen fortgesetzten Angriff schützen kann. Jeder Angriff ist also „One-Use“, was schon das Beispiel mit den über das Handy angegriffenen Tschetschenen zeigt, die seit diesem Angriff keine Handys mehr benutzen.Und drittens schließlich gibt die Art und Weise des Angriffs Verteidigern auch Auskunft über typische Methoden des Angreifers und ermöglicht so die Deduktion und den präventiven Schutz weiterer Ziele. Mögliche Angriffe müssen also bereits beim ersten Schlag maximal effizient sein, da andernfalls der unter Umständen nur geringe Nutzen die hohen Kosten nicht rechtfertigt. Dieser Umstand ist auch der Grund dafür, dass Zwangs- oder Abschreckungsstrategien im Cyberwarfare bisher wenig applizierbar schienen. Abschreckung wurde bislang ausschließlich so betrieben, dass verschiedene Länder ihre Investments in den Bereich offenlegten. Allerdings deutet der Wurm „Conficker“ aufgrund seines hohen Entwicklungsstandes auf die Ressourcen und Möglichkeiten eines Nationalstaates hin, so dass nach einigen Schätzungen in diesem Wurm ein erster „Atomtest“ des Cyberwarfare zu beobachten ist.

Die hohen Kosten effizienter Cyberangriffe legen außerdem nahe, dass Cyberterror entgegen vieler Behauptungen ein unwahrscheinliches Szenario ist. Entsprechend gibt es auch bis dato keinerlei Hinweise auf entsprechende Bemühungen durch Terroristen. Zwar hat der für die Terrorattentate auf Bali verantwortliche Iman Samudra Cyberterror in seinem Buch „Ich gegen die Terroristen“ (in dem Fall die Amerikaner) empfohlen, und es wurden Computerhandbücher in einer Terrorzelle der Al-Qiada in Kabul 2001 sowie Internetaufrufe zur Gründung einer „Islamist Hacker Army“ auf der Terrorwebseite Al-Farooq gefunden. Allerdings waren alle Materialien und Aufrufe nur indikativ und in keiner Weise professionell oder ernst zu nehmen. Ein weiteres wichtiges Indiz für die Abwesenheit entsprechender Bemühungen ist der kriminalistisch gut bekannte Umstand, dass es bislang keinerlei nachweisbare Verbindungen zwischen Cyberkriminellen und Terroristen gibt – ein Weg, den Terroristen als erstes einschlagen müssten. Der Cyberspace wird von Terroristen lediglich gelegentlich zur Finanzierung terroristischer Aktivitäten durch Identity Theft genutzt, wobei diese Aktivitäten aufgrund der gesteigerten Verfolgbarkeit durch wachsende internationale Kooperation in diesem Bereich stark im Rückgang begriffen sind.

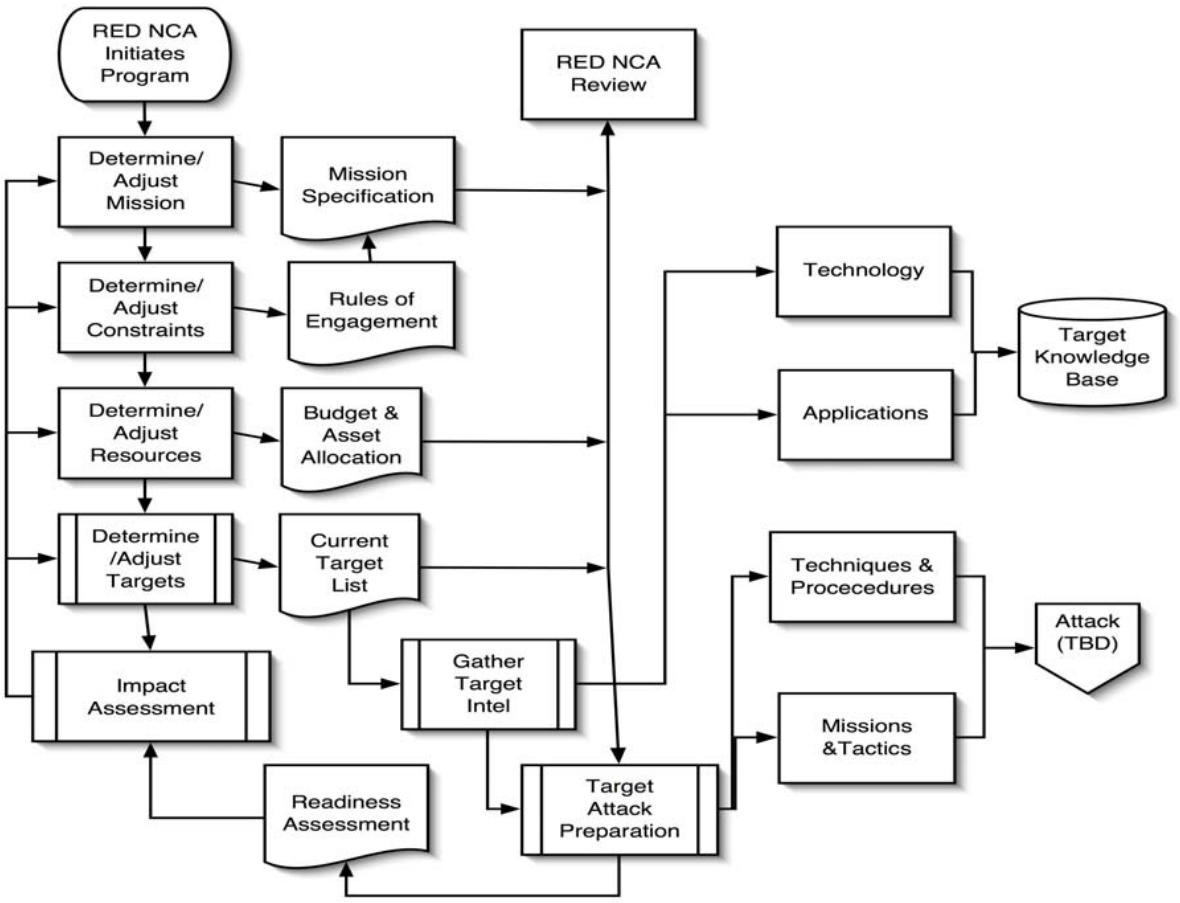

Abbildung: Ein Klasse IV Cyber Network Attack (CNA)-Plan

Die Zukunft: Genuine Cyberstrategien?

Der Militärstratege Basil Henry Liddell Hart nennt als erste Essenz von Strategie und Taktik: „Adjust your end to your means“[19]. Das ist bislang im Bereich Cyberwarfare noch nicht geschehen. Die informationstechnische Kriegsführung ist gegenwärtig noch eng in klassische Operationstypen eingebunden und bezieht sich nur auf den Aspekt der Informatisierung der klassischen Ziele dieser Operationstypen. Genuine Cyberstrategien fehlen ebenso wie Konzepte für ein greifbares und intuitives Verständnis des neuen Operationsraums für kommandierende Offiziere.[20] Während an dieser Stelle noch keine Vorschläge für genuine Cyberstrategien gemacht werden sollen, können doch aus dem Genannten einige Grundlinien skizziert werden, entlang derer sich zukünftige Cyberstrategien ausrichten werden.

Im taktischen und operativen Bereich sind die veränderten Umgebungsbedingungen des Cyberspace als Operationsraum besonders relevant. Die informationstechnische Technikstruktur in Hardware und Software, räumliche und zeitliche Flexibilität und Komplexität sind hier als Cyberterrain und Cyberphysik anzunehmen, wobei die Ausdehnung des Cyberterrain wie erwähnt als querliegend zu allen anderen Operationsräumen vorgestellt werden muss. Die gedankliche Begrenzung auf das Element der Information – als Daten für Steuerung oder Basis von Wissen und Identität – kann vorerst hilfreich sein, muss aber aufgrund der soziotechnischen Ausdehnung informationstechnischer Komplexität als prinzipiell ungenügend empfunden werden. Ein Cyberangriff kann mittelbar auch an vollständig menschlichen und analogen Stellen seine Wirkung entfalten. Das alles erfordert erhebliche Variationen des Verständnisses traditionell strategisch bedeutsamer Elemente. Entfernung etwa wird weitestgehend bedeutungslos, ebenso wie sich das Verhältnis zu Geschwindigkeit als vollständig steuerbar ändern muss. Präzision wird nahezu unmöglich, Verteidigung durch Hürden und Schichten ist nicht mehr im herkömmlichen Sinne effizient, da selbst kleinste Schlupflöcher für maximale Angriffe ausreichen und bestimmte Angriffsformen dadurch sogar noch gesteigert möglich werden. Erwartung und Flexibilität müssen sich vollständig holistisch bilden, da die Trennung von Operationsräumen nicht mehr haltbar ist und Cyberangriffe auch nicht auf das Element der technischen Information beschränkt sein müssen.

[19] Basil Henry Liddell Hart, Strategy, New York 1991, S. 335
[20] Ein Problem, das mehrfach angemahnt wurde. Vgl. etwa Clay Wilson, Clay Wilson, „Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues“, a.a.O.

Im größeren, strategischen Rahmen ist schließlich zu bedenken, dass die Wissensgesellschaft als Informationsgesellschaft über ihr Element der Informatisierung strukturell in verschiedenen Punkten angreifbar ist. Erwähnt wurden oben bereits ökonomische und militärische Bereiche, denkbar sind aber aufgrund der starken Ausbreitung von Informationstechnologien in diesen Bereichen auch Operationen, die in Kultur und Wissenschaft vordringen. Die Fälschung wissenschaftlicher Daten und Studien etwa wäre in einer Wissensgesellschaft eine hervorragende Möglichkeit der Einflusseinnahme auf Entscheidungen, wenn die anvisierten Studien Grundlagen politischer Entscheidungen darstellen. Manipulationen dieser Art werden ja auch bereits von wissenschaftlichen Fake-Instituten wie dem CATO-Institut auf Bestellung hergestellt.[21] Auch die systemische Nutzung von Web 2.0-Anwendungen zur Verbreitung von Schadsoftware oder Falschmeldungen oder zur Genese von Profilen und Rastern sozialer Netzwerke sind neue Herausforderungen, allerdings auch bedenkliche neue Optionen für die Kriegsführung. Hier empfiehlt es sich also dringend, im Rahmen einer „Grand Strategy“ zu denken, die um die 3I’s: Infrastrukturen, Informationen und Identitäten als eigenständige Assets erweitert ist, an denen eben nicht nur Gelder und politische oder militärische Entscheidungen hängen, sondern auch geistige Haltungen, verschiedenste Lebensräume, Kultur und gesellschaftliche Wertekonstellationen.

Privatheit als Angelegenheit der Verteidigung

Dieser letzte Aspekt des Zusammenhangs von Wertekonstellationen mit verschiedenen Ausprägungen der Informatisierung der Wissensgesellschaft ist zuletzt auch für die sensible Einrichtung eigener Kapazitäten bedeutsam. Der Trade-Off zwischen Freiheit und Sicherheit kann in allen informationstechnischen Zusammenhängen schon durch kleine technische Maßnahmen empfindlich gestört werden, und Cyberstrategien ohne Berücksichtigung von Privatheit und informationstechnischen Freiheitsrechten sind – wie auch schon der CSIS-Report für die USA konstatiert – abzulehnen. Allerdings sind im Fall von Cyberwarfare Interessen an Privatheit und Verteidigung gerade optimal verbunden. Primäres Ziel jeder Cyberdefense muss die maximale Unangreifbarkeit und Unzugänglichkeit von Daten sein. Eine grundlegende Ausstattung der landeseigenen IT-Infrastruktur mit hochqualitativen, von Staatsakteure nicht zu durchbrechenden Kryptographieverfahren wäre also aus Verteidigungsperspektive exakt sinnvoll und für Privatheit

[21] Vgl. etwa die Positionen von Thomas Moore in einer Auftragsstudie zum Klimawandel von der Energieindustrie Amerikas: Thomas G. Moore, „Climate of Fear - Why We Shouldn't Worry about Global Warming“, Washington 1998. Oder zur Kritik: Peter Weingart, Petra Pansegrau, Anita Engels, Von der Hypothese zur Katastrophe: Der anthropogene Klimawandel im Diskurs zwischen Wissenschaft, Politik und Massenmedien, Leverkusen 2007

wünschenswert. Dabei kommt hinzu, dass eine prima facie Unterscheidung von militärisch relevanten und militärischen irrelevanten IT-Strukturen nicht konsequent haltbar ist. Zum einen müssen aufgrund des Gedankens einer erweiterten Grand Strategy, die Informationen und Identitäten als gesellschaftliche Werte einer Informationsgesellschaft einschließt, jedem Bürger normativ Ansprüche auf die Verteidigung seiner privater Daten gegen Eingriffe von Außen eingeräumt werden. Zum anderen sind aufgrund der Schadenskategorie der Informationellen Verluste wirtschaftliche Daten so großflächig zu schützen, dass ohnehin ein Großteil der Bevölkerung darunter fiele. Denn es kann keine Argumentationsbasis dafür gefunden werden, dass nur Daten großer Unternehmen zu schützen seien und die kleinerer nicht, so dass also alle wirtschaftlichen Unternehmen zu schützen sind, wobei weiter aufgrund der häufigen Auslagerung beruflicher Daten auf private Rechner zur Arbeit zu Hause auch alle Privatrechner aller Angestellten als schützenswert erachtet werden müssen.

Damit entsteht allerdings ein nicht lösbarer struktureller Konflikt mit kriminalistischen Interessen. Die Kriminalisten haben in den vergangenen Jahren wiederholt Bedürfnisse nach Zugriff auf alle Formen informationstechnischer Kommunikation zu Überwachungszwecken geäußert. Präzise gegen diese Form des Zugriffs durch diese Art von Akteur (mit nationalstaatlichen Ressourcen) muss aber Cyberdefense arbeiten. Nur gegen staatliche Zugriffe vollständig geschützte IuK-Technologien bilden eine präventiv gut verteidigte IT-Infrastruktur. Der Erhalt oder sogar die Beförderung einer kriminalistisch zugänglichen IuK-Technik ist also militärisch exakt kontraintuitiv. Dieser strukturelle Widerspruch ist nicht auszuräumen, auch nicht durch Konzepte zentralisiert verwalteter, spezifischer Zugänge (wie etwa spezifisch entwickelte BKA-Backdoors auf Hardware oder in Programmen), da gerade solche Zugänge militärisch ausgezeichnete Ziele abgeben würden, die durch gezielte Aufklärung mit hohen Ressourcen und Möglichkeiten sicher erreichbar wären.

Die Informationsgesellschaft kann also nur eines von beidem sein: militärisch sicher oder kriminalistisch zugänglich. Da allerdings einerseits die kriminalistischen Eingriffe in diese Form der Kommunikation wenig effizient[22] und ohnehin grundrechtsbedenklich sind[23] und da andererseits das Risiko militärischer Cyberangriffe aufgrund der massiven Schadenshöhe und Schadensbreite als erheblich größer als jeder Schaden durch Cyberkriminalität einzustufen ist, ist die Präferenz klar zugunsten einer soliden Cyberdefense und zuungunsten kriminalistischer

[22] Siehe Hans-Jörg Albrecht, Kosten und Nutzen technisierter Überwachung. In: Sandro Gaycken/Konstanze Kurz (Hg.): 1984.exe, Bielefeld 2008
[23] Siehe Sandro Gaycken, Constanze Kurz, 1984.exe, Bielefeld 2008

Überwachungsbemühungen auszusprechen. Aufgrund des strategischen 3I-Elements der „Identität“ sind aus militärischer Perspektive außerdem die technische Ermöglichung sowie die Verwendung von Raster- und Profiling-Verfahren und besonders die zentrale Speicherung identitätsbezogener Daten wie im Rahmen der Vorratsdatenspeicherung als selbstgefährdend einzustufen. Und indem auch hier – je nach strategischen Ausrichtungen des Gegners – sowohl normativ als auch technisch nur schwer zwischen relevanten und irrelevanten Personen unterschieden werden kann, kommt es ebenfalls zum strukturellen Widerspruch. Da im Falle dieser identifizierungsbezogenen Verfahrenstypen erneut die kriminalistische Ineffizienz der Verfahren hinzukommt, ist aus Verteidigungsperspektive auch für diesen Fall die Wiederabschaffung der kriminalistischen Maßnahmen und der entsprechenden technischen Einrichtungen sinnvoll.

Referenzen

Albrecht, Hans-Jörg, „Kosten und Nutzen technisierter Überwachung“, in: Sandro Gaycken/Konstanze Kurz (Hg.), 1984.exe, Bielefeld 2008

Arquilla, John, Ronfeldt, David, Networks and Netwars: The Future of Terror, Crime and Militancy, Santa Monica 2002

Bishnoi, Rati, “Navy Eyes Fighting in Cyberspace”, in: Inside Defense, online unter: http://www.military.com/features/0,15240,119664,00.html, Zugriff: 15.2.2009

Center for Strategic and International Studies (CSIS), Cybercrime…, Cyberterrorism…, Cyberwarfare…: Averting an Electronic Waterloo, Washington 1998

DCSINT Handbook No. 1.02, „Cyber Operations and Cyberterror“, online unter: http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA456238&Location=U2&doc=GetTRDoc.pdf, Zugriff: 10.01.2009

Deleuze, Gilles, Guattari, Felix, Rhizom, Berlin 1977

Deleuze, Gilles, Guattari, Felix, 1000 Plateaus – Kapitalismus und Schizophrenie, Berlin 1992

Demchak, Chris, Gaycken, Sandro, „Critical Public Systems’ Adaptation for the Emerging Global Socio-Technical Infrastructure”, in: Public Administration Review, Special Issue – The Future of Public Administration in 2020, i.E.

DOD Information Operations Roadmap, online unter: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf, Zugriff: 12.10.2008

Gaycken, Sandro, Kurz, Constanze, 1984.exe, Bielefeld 2008

Harris, Shane, “China’s Cyber-Militia”, in: National Journal Magazine May 2008, online unter: http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php, Zugriff: 21.10.2008

Hubig, Christoph, Unterwegs zur Wissensgesellschaft – Grundlagen, Trends, Probleme, Düsseldorf 2000

Kewley, Dorene, Lowry, John, “Observations on the effects of defense in depth on adversary behavior in cyber warfare”, online unter: www.bbn.com/resources/pdf/USMA_IEEE02.pdf, Zugriff: 21.10.2008

Lewis, James, et al, “Securing Cyberspace for the 44th Presidency“, CSIS Commission on Cyber Security Report, online unter: http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf, Zugriff: 11.01.2009

Liddell Hart, Basil Henry, Strategy, New York 1991

Moore, Thomas G., „Climate of Fear - Why We Shouldn't Worry about Global Warming“, Washington 1998.

Perrow, Charles, Normal Accidents, Princeton 1984

Saydjari, Sami, “Structuring for Strategic Cyber Defense: A Cyber Manhattan Project Blueprint”, Proceedings 2008 Annual Computer Security Applications Conference, online unter: http://www.acsac.org/2008/program/keynotes/saydjari.pdf, Zugriff: 10.1.2009

Smith, Charles, „Cyber War Against Iraq “, in: NewsMax.com, online unter: http://archive.newsmax.com/archives/articles/2003/3/12/134712.shtml, Zugriff: 23.8.2008

Threats Working Group, „Threats Posed by the Internet“, CSIS Commission on Cybersecurity Report, online unter: http://www.csis.org/media/csis/pubs/081028_threats_working_group.pdf, Zugriff: 11.12.2008

Tirenin, Walt, Faatz, Don, „A Concept for Strategic Cyber Defense“, in: Military Communications Conference Proceedings MILCOM 1999, online unter: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=822725, Zugriff: 21.20.2008

Weingart, Peter, Pansegrau, Petra, Engels, Anita, Von der Hypothese zur Katastrophe: Der anthropogene Klimawandel im Diskurs zwischen Wissenschaft, Politik und Massenmedien, Leverkusen 2007

Wilson, Clay, „Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues“, CRS Report for Congress RL 31787, Washington 2007

Wynne, Michael, „Cyberspace as a Domain in which the Airforce Flies and Fights”, Kommentar zur C4ISR Integration Conference, Crystal City, Va., Nov. 2, 2006, online unter: http://www.iwar.org.uk/iwar/resources/cybercommand/speech.htm, Zugriff: 28.1.2009