SÜDWESTRUNDFUNK
SWR2 WISSEN - Manuskriptdienst

„Krieg und Frieden im Netz - Cyberwar und seine Folgen“

Autor und Sprecher: Kai Laufen
Redaktion: Sonja Striegl
Sendung: Mittwoch, 13. März 2013, 08.30 Uhr, SWR2

O-Ton 1 - Thomas Rid:
Die These ist, dass Cyberkrieg nicht stattfindet.

Sprecher:
Thomas Rid aus Aach im Hegau, Professor für Kriegsstudien am King's College in London.

O-Ton 2 - Thomas Rid:
Cyberwar will not take place.

Sprecher:
Das Department of War Studies ist eines der größten Institute für Sicherheitsforschung weltweit.

O-Ton 3 - Thomas Rid:
Und die These ist ganz einfach: Wir haben in der Vergangenheit noch nie einen Fall gehabt, in dem ein Computerangriff physischen Schaden größeren Ausmaßes angerichtet hat: Insbesondere hatten wir noch nie einen Computerangriff oder Schadsoftware, die Menschenleben gekostet hat oder jemanden verletzt hat.

Sprecher:
Thomas Rid will mit seiner These nicht die Fakten herunterspielen: Natürlich gebe es aggressives staatliches Verhalten im Internet oder grundsätzlich gegen digitale Netze. Aber aus Sicht der Konfliktforschung sei der Begriff des „Krieges" in diesem Zusammenhang nicht angebracht - aus zwei Gründen:

O-Ton 4 - Thomas Rid:
Clausewitz sagt: „Krieg ist ein Akt der Gewalt um den Gegner zum Erfüllen unseres Willens zu zwingen." Es geht um eine Instrumentalität: Man wendet Gewalt an, um damit etwas zu erzielen. Und es geht darum, sich politisch dafür verantwortlich zu zeigen, dass man sagt: Ich habe dies und das gemacht, um dich zu dem und dem Verhalten zu zwingen.

Sprecher 2 (Ansage):
„Krieg und Frieden im Netz - Cyberwar und seine Folgen". Eine Sendung von Kai Laufen.

Atmos...

Sprecher:
Die verspielte viktorianische Fassade des mächtigen Russell Hotels blickt auf den Russell Square, mitten in der Londoner Innenstadt, unweit des King's College, an dem Thomas Rid den Cyberwar erforscht.

Atmo: Restaurant

Sprecher:
... über dicke plüschige Teppiche und durch marmorstarrende Gänge geht es tief hinein in den Konferenzbereich.

Atmo: Shea

Sprecher:
100, vielleicht 120 Teilnehmer haben sich mit Kaffee und Säften an den rund 20 großen runden Tischen eingerichtet, gerade spricht Jamie Shea, dem deutschen Publikum als Sprecher der NATO während des Kosovo-Krieges vertraut. Aber heute sitzen fast keine Deutschen im Publikum, dafür Briten und Amerikaner, Skandinavier und Niederländer, ein brasilianischer Oberst, eine Delegation aus den Philippinen. Cyber Defense and Network Security 2013 heißt der Kongress.

O-Ton 5 - Richard de Silva (ohne Übersetzung)

Sprecher:
Richard de Silva ist ein charmanter, umgänglicher Gentleman. Er vertritt das Londoner Unternehmen DefenceIQ, eine Nachrichtenplattform für Militärische Themen, die auch Fachkongresse weltweit organisiert. Hier treffen sich Militärs und Politikberater, hohe Verwaltungsbeamte mit Budget und Marketingleute von der Sicherheitsindustrie.

Moderiert werden die zwei Kongresstage von einem ehemaligen Oberst der amerikanischen Armee, Bill Hagestad. Der Terrorismusexperte spricht fließend Mandarin und vergleicht in seinem eigenen Vortrag die chinesischen Cyberwar-Aktivitäten mit denen Russlands und des Irans:

O-Ton 6 - Bill Hagestad (Sprecher Overvoice):
In China haben wir Hacker, die vier verschiedenen Gruppierungen angehören: Der Kommunistischen Partei, der Volksarmee, staatlichen Unternehmen und den Hacktivists, also Privatleute. Jede dieser Gruppierungen hat einen anderen Ansatz, die Regierungsziele zu verfolgen, die politischen, wirtschaftlichen oder kulturellen Zwecken dienen. Alle wollen Überlegenheit in ihrer jeweiligen virtuellen Sphäre erreichen und auf jeden Fall vermeiden, dass sie gegenüber dem Westen ins Hintertreffen geraten, so wie es in der physischen Welt geschehen ist, zum Beispiel gegenüber den USA, England, Deutschland oder anderen Ländern.

Sprecher:
China holt zwar auch in der klassischen Waffentechnik auf, baut Flugzeugträger und Tarnkappenbomber, oftmals unverfrorene Kopien ausspionierter Westprodukte. Im Bereich der Nullen und Einsen aber gelte die Volksrepublik heute sogar als dominierend:

O-Ton 7 - Bill Hagestad (Sprecher Overvoice):
Sie nutzen ihren innovativen Vorteil aus um den Kampf nach außen zu tragen, ohne dass wir es ihnen nachweisen könnten - das ist das Dilemma der Cyber-Kriegsführung.

Sprecher:
Das Ziel der chinesischen Führung sei dabei stets, die Souveränität des Reichs der Mitte zu erhalten. 2010, erklärt der Militärstratege, sei ein sehr bedeutsames Jahr in der Militärgeschichte gewesen, denn die USA haben in jenem Jahr den Cyberspace zum Kriegsschauplatz erklärt - Chinesen, Russen und die Iraner waren gleichermaßen alarmiert angesichts einer stets aggressiv auftretenden US-Weltmacht und haben ebenfalls militärische Cyberangriffsfähigkeiten aufgebaut. Aber die Motive der drei Staaten seien sehr verschieden, analysiert Bill Hagestad:

O-Ton 8 - Bill Hagestad (Sprecher Overvoice):
In China ist es der Nationalismus. In Russland dagegen mischt sich die Verbitterung über die Niederlage im Kalten Krieg mit krimineller Energie. Ganz anders im Iran, denn das Land wurde ja tatsächlich schon mit einer Cyberwaffe angegriffen: Stuxnet, aber auch mit Duqu, Flame, Shamoon und anderen Formen von Schadsoftware. Und sie wollen einfach ihre Kritische Infrastruktur schützen, gegenüber realen Feinden.

Sprecher:
Das Stichwort Stuxnet fehlt seit Mitte 2010 in keinem Buch, Artikel oder Vortrag über Cyberwar: Der mutmaßlich von amerikanischen Geheimdiensten entwickelte Computerwurm hatte in der iranischen Urananreicherungsanlage in Natanz Zerstörungen hervorgerufen, offenbar waren Zentrifugen mit gasförmigem Uran aus dem Gleichlauf geraten und zerplatzt. Er könne sich schon vorstellen, dass sich die Iraner bedroht fühlen, meint Bill Hagestad:

O-Ton 9 - Bill Hagestad (Sprecher Overvoice):
Der Iran ist heute von allen Seiten von Feinden eingeschlossen. Und ich frage regelmäßig die Leute, die meinen, mit einem Cyberangriff wie Stuxnet könnte man auch ohne kinetische Kriegsführung die politischen Ziele gegen den Iran erreichen: Waren sie schon einmal im Krieg? Machen sie sich wirklich klar, wie der Gegner, also der Iran, diese Aggression empfindet? Krieg ist grausam und auch wenn wir die USA verteidigen wollen, müssen wir genau aufpassen, wie wir vorgehen. Denn im Krieg gibt es kein Entkommen. Höchstens in einem Leichensack.

Sprecher:
Fast wird der Irak-Kriegsveteran Hagestad emotional: Die USA würden zu weit gehen, wenn sie jetzt der Diplomatie keine Chance mehr gäben und zum Angriff übergingen.

O-Ton 10 - Bill Hagestad (Sprecher Overvoice):
We all know that if policy fails and diplomacy goes by the wayside or we step over it, the next step is military action and I don't want to go back to war...I do not!

Wir wissen doch alle, wenn die Politik versagt und wir die Diplomatie übergehen, ist der nächste Schritt das militärische Eingreifen - und ich will nicht noch einmal in den Krieg ziehen!

Sprecher:
Der Stuxnet-Anschlag auf den Iran hat mutmaßlich nur Sachbeschädigung hervorgerufen, und keine Menschenopfer gefordert. Aber er könnte eines Tages als der eigentliche Beginn eines großen, echten Krieges im Nahen und Mittleren Osten gewertet werden. Wenn die Politik mit anderen Mitteln fortgesetzt wird, wie Carl von Clausewitz den Krieg seinerzeit beschrieb.

Regie: Thunderstruck refrain (Thunder! Thunder!)

Sprecher:
Mitte 2012 berichten Iranische Wissenschaftler von einem weiteren Virenangriff: Heavy Metal wird zur Waffe, schreiben amerikanische Magazine, denn der Virus enthält außer einem Schadprogramm auch eine Musikdatei: Mitten in der Nacht knallt aus den PC-Lautsprechern in Natanz der ACDC-Song Thunderstruck. Es ist eine Demonstration der Macht. Psychokrieg.

O-Ton 11 - David J. Smith

Sprecher:
Er werde nicht kommentieren, ob das intelligent war oder nicht - meint David J. Smith vom einflussreichen Potomac Institute, einem amerikanischen Think Tank für Sicherheitsfragen zu dem Stuxnet-Angriff.

O-Ton 12 - David J. Smith (Sprecher Overvoice):
Wenn sie ein Land wie den Iran haben, das an einer Atombombe arbeitet - und wir reden hier über eine sehr bedrohliche Entwicklung - was ist dann legitim und was nicht? Ich weiß es nicht! Aber die Realität ist: Wenn dieses Land weiter in diese Richtung geht, die es eingeschlagen hat, dann werden wir eine Menge Probleme haben. Also wenn es Mittel gibt außer dem physischen Krieg, damit umzugehen, dann sollten sie untersucht werden. Wird es die richtige Antwort für alle Situationen sein? Nein! Und ich weiß auch nicht, welche die richtige Antwort ist. Aber es ist doch der Iran, der sich unvernünftig verhält.

Sprecher:
Es schwingt eine heimliche Bewunderung für den geglückten Cyberwar-Angriff auf den Iran mit, auch wenn sich David J. Smith nicht hinreißen lässt, zu triumphieren. Im Kalten Krieg war er unter Ronald Reagan Unterhändler mit der Sowjetunion in Abrüstungsfragen. Diesen Krieg hat der Militärstratege und Realpolitiker gewonnen. Beeinflusst diese historische Erfahrung seinen Blick auf den Iran und die Möglichkeiten, den Konflikt zu entspannen?

O-Ton 13 - David J. Smith (Sprecher Overvoice):
Im Krieg sterben Menschen, das ist die hässliche Wahrheit. In Natanz ist übrigens niemand gestorben, das sollte man nicht vergessen. Legitim, nicht legitim, gefährlich, ungefährlich - die Realität ist: Krieg ist gefährlich. Wenn wir also einen Weg finden, eine Situation zu deeskalieren, dann sollte man sich das genau ansehen. Was sind denn die

Alternativen, ohne jetzt emotional zu werden: Wenn sie beklagen, dass im Krieg Menschen sterben, dann warten sie mal, was passiert, wenn der Iran erst einmal eine Atombombe hat!

Sprecher:
Offiziell hat die amerikanische Regierung nie die Urheberschaft für den Stuxnet-Angriff eingeräumt. Aber regierungsnahe Quellen ließen gegenüber der New York Times im vergangenen Jahr Informationen über Stuxnet und die Operation „Olympic Games“ durchsickern, die weltweit ernst genommen wurden. Und vor wenigen Wochen, im Februar verkündete das Verteidigungsministerium, erstmals seit 1944 eine neue militärische Auszeichnung einzuführen: Eine „Medaille für herausragende Kriegsführung“, die Soldaten für besondere Leistungen beim Kampf mit ferngesteuerten Drohnen, oder eben mit Cyberwaffen auszeichnen soll.

O-Ton 14 - Mike Stone (ohne Übersetzung)

Sprecher:
Brigadegeneral Mike Stone könnte ein Anwärter auf den neuen Orden sein, allerdings für Leistungen in der Abwehr: Der große kräftige Amerikaner gehört der Nationalgarde des Bundesstaates Michigan an. Im Kriegsfall wird diese ins Ausland verlagert - zuhause bekämpfen die 375.000 „Bürgersoldaten“ der National Guard Schneestürme und Flutkatastrophen. Sollte der Iran einmal mit den selben Waffen zurückschlagen, einem persischen Stuxnet, müsste Mike Stone die lebenserhaltenden Systeme, also die sogenannte Kritische Infrastruktur südlich der Großen Seen verteidigen:

O-Ton 15 - Mike Stone (Sprecher Overvoice):
Bei uns in Michigan sitzen die drei großen Autohersteller Ford, General Motors und Chrysler. Jetzt haben wir zum Beispiel in Detroit eine Brücke die gleichzeitig ein Grenzübergang nach Kanada ist, die Ambassador Bridge. Als am 11. September 2001 nach den Terrorangriffen alle Grenzübergänge geschlossen wurden, mussten wir feststellen: Wenn diese Brücke auch nur 30 Minuten geschlossen ist, werden die Autofabriken vom Nachschub abgeschnitten und müssen die Produktion einstellen.

Sprecher:
Angriffe auf die zivile Infrastruktur nehmen Strategen als die wahrscheinlichsten Szenarien an, in denen digitale Schadprogramme als Waffen eingesetzt würden. Allerdings nicht unbedingt plötzlich und flächendeckend, meint der deutsche IT-Sicherheitsforscher Sandro Gaycken:

O-Ton 16 - Sandro Gaycken:
Es gibt ja in der Militärtheorie diese „Strategies of Erosion“, also Erosionsstrategien, wo man dann sagt, wenn ich einem Feind sozusagen nicht in einer offenen Feldschlacht begegnen kann, dann kann ich den vielleicht so mit vielen tausend kleinen Stichen langsam ausbluten und schwächen, eigentlich eine klassische Guerillataktik. Und das kann man natürlich auch online machen, sozusagen und dann eine Wirtschaft systematisch schwächen.

Sprecher:
Das, so scheint es, kommt einer Beschreibung der Realität heute ziemlich nahe. Cyberwar als Wirtschaftskrieg. Aber wer ist dann für Angriff und Verteidigung zuständig? Geheimdienste sind auf dem Kongress in London kaum vertreten - dafür aber Militärs:

O-Ton 17 - Hans Folmer:
Hans Folmer, Kommandeur der Taskforce Cyber und ich mache das Cyberprogramm der niederländischen Streitkräfte.

Sprecher:
Hans Folmer, spricht offen über die Strategie der niederländischen Streitkräfte. Was er sagt, war aus dem deutschen Verteidigungsministerium oder aus der Bundeswehr so noch nie zu hören. Seit einem Jahr baut Folmer seine Task Force auf - zunächst noch vom Schreibtisch im Verteidigungsministerium aus:

O-Ton 18 - Hans Folmer:
Ich rekrutiere Menschen mit bestimmten Kenntnissen. Und das können Hacker sein, die können die Kenntnisse schon haben. Es kann aber auch sein, dass ich Soldaten, hier in Niederlande reduzieren wir 6000 Soldaten, Soldaten die ihren Job verlieren, die kann ich behalten und die kann ich als Hacker ausbilden.

Sprecher:
Die Niederlande setzen also unverhohlen auf kybernetische Offensivwaffen - vor allem aus Kostengründen. Allerdings weiß Kommandant Folmer, dass die Einsatzmöglichkeiten für Cyber-Angriffswaffen begrenzt sind:

O-Ton 19 - Hans Folmer:
Die niederländischen Streitkräfte müssen eine Milliarde Euro sparen aber gleichzeitig hat man entschieden, dass wir dieses Programm anlaufen, weil es wirklich sehr wichtig ist für uns. Ich glaube nicht, dass man mit „Cyber“ einen Krieg gewinnen kann, man hat Vorteile davon wenn man das nutzt, dass auf einmal alle Infrastrukturen angegriffen werden, glaube ich auch nicht. Dafür sind die verschiedenen Infrastrukturen zu unterschiedlich. Ich glaube nicht an Cyber-Pearl-Harbour.

Sprecher:
Der Überraschungsangriff der japanischen Luftwaffe auf die US-Marine in Pearl Harbour Ende 1941 ist eine historische Bezugsgröße in der Geschichte des Krieges. Noch gilt es zwar als unwahrscheinlich, dass Angriffe auf der Basis von Schadsoftware - zumal gegen militärische Netzwerke - jemals eine solche zerstörerische Wirkung erreichen könnten. Aber „Pearl Harbour“ war nicht nur eine desaströse militärische Niederlage: Es war auch der Auslöser für den Eintritt der USA in den Zweiten Weltkrieg, der im Pazifischen Raum erst mit dem Abwurf der zwei Atombomben beendet wurde. Der Kriegseintritt der USA war völkerrechtlich durch „Pearl Harbour“ legitimiert und - vielleicht wichtiger noch - auch gegenüber der eigenen, bis dahin eher pazifistisch gesinnten Bevölkerung zu rechtfertigen. Ist ein „Cyber-Pearl-Harbour“ in dieser *zweiten* Bedeutung tatsächlich ausgeschlossen?

O-Ton 20 - Bob Bigman (ohne Übersetzung):
Es wird nichts passieren, es sei denn, es gibt einen Cyber-Elften September.

Sprecher:
... hält Bob Bigman dagegen. 30 Jahre war er bei der CIA und berät nun Firmen in ihrer IT-Sicherheitsstrategie. Seine Argumentation zeigt nebenbei auf, wie nahe die Denkweise von Geheimdiensten und Militärs an der von Kriminellen liegen kann:

O-Ton 21 - Bob Bigman (Sprecher Overvoice):
Das letzte, was ein Cyberkrimineller will, ist ein echter Krieg. Denn so eine Auseinandersetzung könnte den Gegner dazu bringen, aufzurüsten, sich besser zu verteidigen. Heutzutage sind die Cyberkriminelle und die -Spione ganz happy mit dem Status Quo: Sie fahren ihre Angriffe, greifen Banken an, stehlen Geld und waschen es - warum sollten sie an dieser Situation etwas ändern wollen?

Sprecher:
Dieselbe Logik sieht Bigman auch bei der wirtschaftlichen oder politisch motivierten Spionage am Werk - in beiden Fällen könne der Täter nur profitieren, wenn er das Opfer nicht zerstört. Deshalb hält auch Bob Bigman das Wörtchen Cyberkrieg für irreführend. Aber auch er sieht eine Gefahr, dass mit Cyberangriffen die Schwelle zu einem physischen Krieg überschritten werden könnte:

O-Ton 22 - Bob Bigman (Sprecher Overvoice):
Ja, wir lieben das Wort „Krieg“! Aber von Cyberkrieg zu sprechen hat in meinen Augen nur eine Berechtigung, wenn es um anhaltende, tiefgehende Störungen der Infrastruktur geht: Das Verkehrssystem, das Gesundheitswesen, Kommunikation. Was ist nachhaltig: Nun, wenn die New Yorker U-Bahn, drei, vier Tage oder eine Woche den Betrieb einstellen müsste, das wäre schon eine Kriegserklärung gegen die Vereinigten Staaten. Wenn sie ähnlich gegen das Bankenwesen vorgehen, dann sieht das langsam aus wie 1914: Da ist gerade jemand in seinem Auto erschossen worden!

Sprecher:
Ausschließen will der Ex-Geheimdienstmann Bigman das Szenario eines „Cyber-Pearl-Harbour“ als Grund für einen Kriegseintritt offenbar nicht. Es komme auf die weltpolitischen Zusammenhänge an. Bigman sieht keinen Grund zur Panik - aber Panikmacher hatten in letzter Zeit Erfolg, beobachtet der investigative Journalist Misha Glenny. Der ehemalige BBC-Korrespondent beleuchtet in seinem Buch „Cybercrime - Kriminalität und Krieg im digitalen Zeitalter“ von 2012 die Ursprünge der organisierten Hackerkriminalität und ihre Übergänge zur digitalen Kriegsführung.

O-Ton 23 - Misha Glenny (Sprecher Overvoice):
Eine der bekanntesten hysterischen Stimmungsmacher in den USA ist Richard Clarke. In seinem Buch „Cyberwar“ hatte er 2010 in sehr dramatischen Bildern beschrieben, wie die gesamte amerikanische Infrastruktur nach einem Cyberangriff binnen Stunden zusammenbricht. Das ist Angstmacherei von Leuten, die - wie Richard Clarke - ihr Geld gleichzeitig als Sicherheitsberater in genau diesem Bereich verdienen.

Sprecher:
Und das sei ein zu leichtfertiger Umgang mit einem potentiell so gefährlichen Thema. Misha Glenny fühlt sich an das Wettrüsten im Kalten Krieg erinnert, und zwar an die Frühphase, als sich die Großmächte noch nicht auf Rüstungskontrollabkommen geeinigt hatten:

O-Ton 24 - Misha Glenny (Sprecher Overvoice):
Das Werkzeug ist hier nicht mehr ein Atomarer Sprengkopf und sein Trägersystem im Besitz eines Staates. Das Werkzeug ist die Verwundbarkeit des Gegners. Man kann Schadsoftware wie Stuxnet nicht einsetzen, wenn man nicht die Schwachstellen im gegnerischen Netzwerk genau kennt und ausnutzt. Das bedeutet, dass Cyberkrieg faktisch ein präemptiver Krieg ist.

Sprecher:
In einem „Präemptivkrieg“ wird dem Gegner eine aggressive Absicht unterstellt, die den eigenen Erstschlag legitimiert. Das moderne Kriegsvölkerrecht erlaubt ausschließlich Verteidigungskriege. Das umfasst zwar auch Präventiv- oder Präemptivschläge, allerdings nur, wenn ein Angriff unmittelbar bevorsteht. Und im Zusammenhang mit dem Stuxnet-Angriff auf die iranischen Uranzentrifugen diskutieren Experten, ob der Iran dadurch ein Recht auf Selbstverteidigung hatte.

O-Ton 25 - Robin Geiss:
Der Iran hat Stuxnet selbst nicht als bewaffneten Angriff bezeichnet.

Sprecher:
... stellt Robin Geiss fest, zur Zeit Juniorprofessor für Völker- und Europarecht an der Universität Potsdam:

O-Ton 26 - Robin Geiss:
Es gibt eigentlich zwei Wege wie Gewalt überhaupt noch im internationalen Verkehr legitimiert werden kann. Das eine sind Kapitel-Sieben-Resolutionen des Sicherheitsrates. Das würde dann eben der Sicherheitsrat beschließen. Der stellt eine Bedrohung des Weltfriedens fest. Aber es gibt eben auch noch die Möglichkeit, dass einzelne Staaten, wenn die sich angegriffen fühlen und wenn die Schwelle zum bewaffneten Angriff genommen ist - wo immer die genau liegt, das ist nicht so ganz klar - aber das ist jedenfalls die rechtliche Aussage: Der bewaffnete Angriff der löst das Recht auf Selbstverteidigung auch des einzelnen Staates dann aus.

Sprecher:
Wollte man den Stuxnet-Angriff als militärischen Angriff darstellen, wäre er also als Präemptivschlag nur unter der Annahme gerechtfertigt gewesen, dass der Iran unmittelbar davor stand, Atomwaffen gegen die USA einzusetzen. Das aber behauptet niemand. Umgekehrt hätte der Iran aus dieser Art Angriff kein Recht auf einen Angriff gegen die USA ableiten können.

Überhaupt sei es nicht im Interesse der Staaten, Cyberangriffe als kriegerische Angriffe zu werten, meint Robin Geiss. Denn im Krieg muss klar zwischen Militärs und Zivilisten unterschieden werden. Nur militärische Ziele und Soldaten dürfen angegriffen werden.

O-Ton 27 - Robin Geiss:
Die ganze Cyberinfrastruktur die zunächst mal zivil ist, die wird aber genauso von den Militärs benutzt. Der Cyberspace zeichnet sich ja gerade dadurch aus, dass alles mit allem vernetzt ist. Das heißt, wenn die Militärs beginnen, im großen Ausmaß in wirklichem bewaffneten Konflikt, in einer Auseinandersetzung zwischen großen hochtechnologisierten Staaten, wenn die also substanziell anfangen den Cyberspace für ihre Zwecke zu benutzen, dann wird auch quasi möglicherweise alles im Cyberspace durch diese militärische Nutzung zu einem militärischen Objekt. Das ist also eine ganz fatale Auswirkung. Weshalb ich auch glaube, dass da eines der größten Probleme liegt und wir uns auch da nicht der Illusion hingeben sollten, wir könnten diese Unterscheidung so noch aufrecht erhalten.

Sprecher:
Von „Cyberwar“ im Sinne von Krieg zu sprechen, ist also im völkerrechtlichen und historischen Sinn irreführend. Cyberwar will not take place. Aber Cyberwar wird in unserem Wortschatz bleiben, als Sammelbegriff für Sabotage, Spionage, Kriminalität und subversive Propaganda mittels Computertechnik.

O-Ton 28 - Sandro Gaycken:
Da haben wir dann tatsächlich auch die Situation, dass die großen Staaten, die sich ja natürlich nie kinetisch angreifen wollen und würden - glücklicherweise -, dass die aber auf diesem Level sich sehr wohl die ganze Zeit beharken.

Sprecher:
... fürchtet Sandro Gaycken, IT-Sicherheitsforscher an der Freien Universität Berlin und derzeit Berater des Auswärtigen Amtes für eine Cyberaußenstrategie. Er schließt sich einer aktuellen Forderung der Bundesregierung an, die auch die Europäische Kommission erhebt: Die Industrie und der Bankensektor als Hauptziele von Cyber-Spionage und -Kriminalität sollen verpflichtet werden, über Attacken auf ihre Netze zu informieren:

O-Ton 29 - Sandro Gaycken:
Wir brauchen natürlich noch mehr Informationen. Und was uns vor allen Dingen auch fehlt, ist der Link zwischen den Aktivitäten die laufen und staatlichen Interessen. China wird oft nachgesagt, dass die mit staatlichem Interesse die ganze Industriespionage betreiben. Aber wenn die sich nicht klar bekennen und sagen: „ja, das ist unsere Strategie, euch auszubeuten, damit wir uns aufbauen können und irgendwann mächtiger sind als ihr“ - und das werden sie natürlich so offen nicht sagen - und wenn sie das nicht sagen, dann haben wir keinen Beweis dafür. Von daher fehlt diese Verbindung, um das wirklich als strategisches Element zu bewerten.

Sprecher:
Der Berliner IT-Sicherheitsberater Felix Lindner weiß, wie schwierig solche Zuschreibungen sein können, hält sie aber grundsätzlich für möglich:

O-Ton 30 - Felix Lindner:
Ich tendiere zu der Schule, die sagt: „Die Handschrift gibt es sowieso und die wirst du nicht los." Aber es gibt andere Leute, die sagen: „Ja, das kann man alles faken und man kann so tun, als wäre das aus einem anderen Land, man kann einen Angriff bauen und so tun, als wäre das aus Russland oder China" - ich persönlich tendiere dazu zu sagen: „Ne, das ist nicht machbar."

Sprecher:
Und zwar weil der Aufbau eines sogenannten Exploits, also einer Schadsoftware, in vielen Schritten erfolgt, die den Experten Hinweise auf die verwendete Hard- und Software gibt. Aber die Handschrift zu erkennen, reicht noch nicht aus, auch tatsächlich den Täter zu benennen, meint Felix Lindner:

O-Ton 31 - Felix Lindner:
Was ist denn, wenn ich den Server hochnehme - also den Hauptrechner - von irgendeinem chinesischen Team? Dann hab ich ihre Angriffe und dann kann ich ihre Angriffe von ihrem Rechner aus starten.

Sprecher:
In der Digitalen Welt muss Identität ganz neu gedacht werden, weil es so viele Möglichkeiten gibt, Identitäten zu wechseln, zu verschleiern oder vorzutäuschen. Das ist der Hintergrund, vor dem auch die neuesten Meldungen über vermeintliche Hackerangriffe aus China bewertet werden müssen. Mag sein, dass Hackergruppen oder -Einheiten aus dem Reich der Mitte massive Wirtschaftsspionage in Europa und den USA betreiben - aber können die Europäer den USA wirklich trauen - und umgekehrt? In dieser unüberschaubaren Welt könnte eine wichtige Strategie darin liegen, Hard- und Software-Entwicklungen möglichst angriffssicher zu machen. Das ist das Geschäftsmodell von Felix Lindner und seiner Firma Recurity Labs. Allerdings weiß der erfahrene Hacker auch: Die größte Schwachstelle in jedem Netzwerk ist im Zweifelsfall der Mensch:

O-Ton 32 - Felix Lindner:
Das Problem, das ich mit der Idee habe, ist: Man nehme mal irgendjemandem seine gewohnten Computerfunktionalitäten weg und stelle was hin, was weniger macht. Das hat noch nie funktioniert!

Sprecher:
Tatsächlich gehe der Trend derzeit in die Gegenrichtung, beobachtet Thomas Tschersich, bei der Deutschen Telekom AG zuständig für technische Sicherheit. Die Telekom betreibt eigene Honeypots, also bewusst schlecht geschützte Computer. Sie sollen Viren einfangen, die dann analysiert werden. Sorgen bereiten aktuell die Nutzer

von Smartphones, die Sicherheitsbeschränkungen der Hersteller umgehen, um mehr Funktionen aus den Geräten herauszuholen:

O-Ton 33 - Thomas Tschersich:
Beispielsweise eines unserer Honeypotsysteme simuliert ein solches gejailbreaktes iPhone und es wurde innerhalb von einem Jahr mehr als 300.000 Mal versucht anzugreifen, aber fast 350 Mal erfolgreich, wo ein Angreifer wirklich bei einem realen Gerät in der Lage gewesen wäre, Software auf dieses Gerät einzubringen, Daten herunter zu kopieren, und dieses Gerät dann beispielsweise zum Teil eines mobilen Botnetzes zu machen.

Sprecher:
Die Telekom hat angekündigt, mit solchen Informationen in Zukunft noch transparenter umzugehen und alle Angriffe auf die eigenen Systeme oder die Geräte der Kunden öffentlich zu machen:

O-Ton 34 - Thomas Tschersich:
Zur CeBit diesen Jahres werden wir ein neues Informationsportal starten, wo eine tagesaktuelle Sicht auf die Angriffslage im Internet zu sehen ist. Wo wirklich statistische Informationen - Wo kommen Angriffe her! Was sind die Themen, die angegriffen werden, also welche Angriffsmuster werden hauptsächlich verwendet? Wie viel Angriffe sehen wir pro Tag gegen unsere Sensornetzwerke? - um damit ein Stück weit mehr für Transparenz zu sorgen. Und um - was wir für ganz wichtig halten - zu motivieren, einen branchenübergreifenden Dialog und Austausch zu dem Thema „Sicherheit“ hinzubekommen.

ATMO: Stimmengewirr, Wasser, Möwen

Sprecher:
Zurück nach London: Am Ende vieler verschlungener Gänge im King’s College, mit Blick auf die Themse, liegt das Arbeitszimmer von Thomas Rid, dem Skeptiker, der gerade sein Buch herausgebracht hat: Cyberwar will not happen. Diese Einsicht würde den bisher aggressivsten Angreifern allerdings noch fehlen:

O-Ton 35 - Thomas Rid:
Die Amerikaner sind ja in einer interessanten Situation hier, die man eigentlich nur mit dem Wort heuchlerisch beschreiben kann, oder doppelbödig vielleicht besser: Auf der einen Seite wollen die Amerikaner - immer wieder warnen sie vor einem Cyber-Pearl-Harbour, vor einem Angriff, der dem 11. September ähneln könnte, durch Computerangriffe - also sie machen Panik auf der einen Seite und wollen sich gut verteidigen gegen Cyberangriffe. Aber auf der anderen Seite sind die Amerikaner diejenigen, die am aggressivsten vorgehen.

Sprecher:
Wenn auch im strengen Sinne nicht von Krieg zu sprechen ist, wird diese neue Form der internationalen Auseinandersetzung ihren Namen wohl behalten: Cyberwar. Wir sind mitten drin.

****