[CYBERWAR & CYBER DEFENCE]

Europäische Sicherheit und Verteidigung: Bert Weingarten, CEO PAN AMP AG, Auszüge zum Vortrag, 09.12.2009

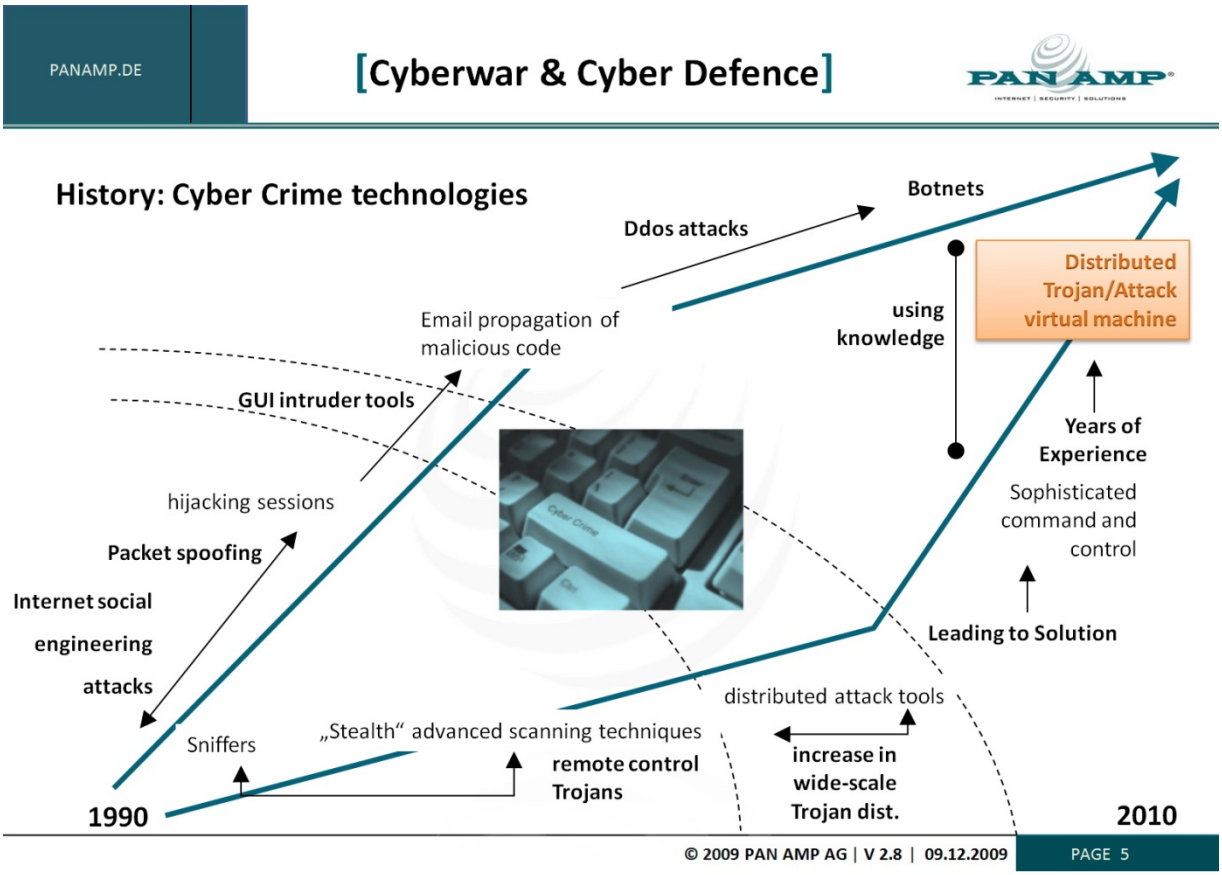
Berlin, den 9. Dezember 2009

Auf Anfrage von Dr. Karl von Wogau, im Europaparlament, Vorsitzender des Unterausschusses für Sicherheit und Verteidigung (2009), begann ich meinen Vortrag „Cyberwar & Defence“ für den 8. Kongress für Europäische Sicherheit & Verteidigung (Berlin, 08. und 09. Dezember 2009) auszuarbeiten. Beginnend mit der Begriffsdefinierung „Cyberwar“ recherchierte ich die in den USA, Asien und Europa bestehenden Informationen, um festzustellen, dass 840 unterschiedliche Meinungen, Einschätzungen und Inhalte, teilweise stark konträr, versuchten, den Begriff Cyberwar zu definieren. Die Informationen ordnete ich in Form von Ausdrucken auf einer Zimmerwand in drei gruppierte Informationslagen. Die erste Informationslage beinhaltete Cybercrime Elemente und die Auffassung, ein Cyberangriff wäre einem Cyberwar gleichzusetzen. Die zweite Informationslage beinhaltete die Meinung, einzelne Personen könnten einen Cyberwar führen und die dritte Informationslage vermischte virtuelle und physische Angriffsformen. Ich musste feststellen, dass die bestehenden Einschätzungen und Meinungen in allen drei Informationslagen nicht zielführend waren und eine Klassifizierung zur Schwere eines Cyberwars gänzlich fehlte.

Bert Weingarten, CEO PAN AMP AG, 8th Congress on European Security & Defence (09. Dez. 2009). [Foto: Klaus Dombrowsky]

Wie definiert man Cyberwar

Um den Begriff Cyberwar zu definieren, musste als erstes festgestellt werden, was ein Cyberwar definitiv nicht beinhaltet. Hierzu gehören Cybercrime Aktivitäten, die sich direkt gegen Privatnutzer oder Unternehmen richten. Die Historie der multiplen Cybercrime Technologien begann 1990 und erreicht 2010 eine weitere Evolutionsstufe mit der Verbreitung von virtuellen Systemen zur vereinfachten Teilnahme an Cybercrime Netzwerken. Materielle Angriffe, also das Zerstören und die Sabotage von Hardware (z. B. Kabel-, Antennen- und Satellitenverbindungen) sind ebenfalls keine Bestandteile eines Cyberwars solange die Zerstörung oder die Sabotage physisch ausgeführt wird, wie z.B. durch das physische Ausschalten einer Hardwareeinheit, einen Raketenangriff auf eine Vermittlungsstelle oder den Abschuss eines Kommunikationssatelliten. Davon ausgehend definieren eine Reihe von Wissenschaftlern den Kosovo-Krieg 1999 als den ersten Cyberwar zwischen Staaten, in dem beide Seiten entsprechende Kampfmittel einsetzten. Auch die umfassende Steuerung und Kontrolle des Kriegsgeschehens mittels weltraum-



Historie der multiplen Cybercrime-Technologien (1990 bis 2010). [Vortrag-SecDef-Seite 5_20091209]

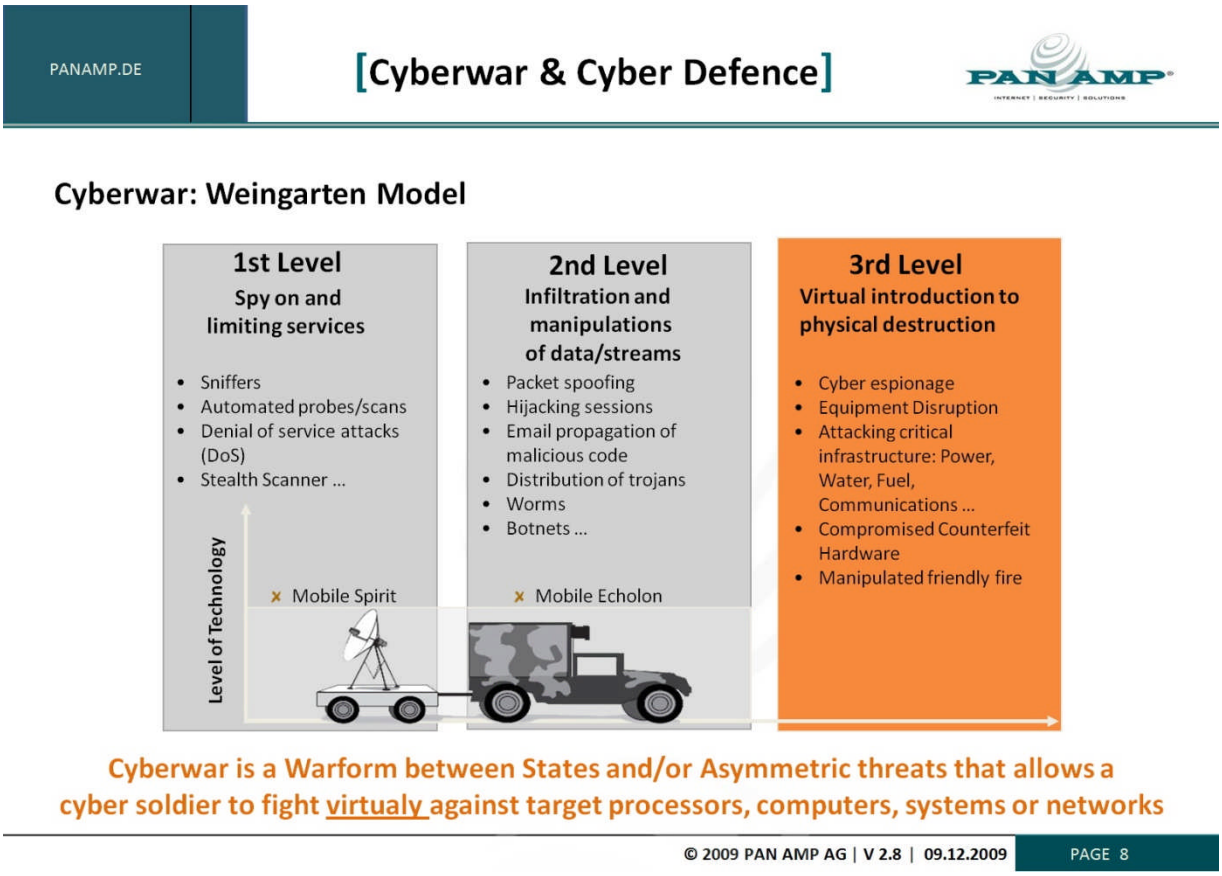
gestützter Systeme trat auf NATO-Seite bestimmend hervor, stellt jedoch keine Komponente eines Cyberwars da, da die eingesetzten Satelliten maßgeblich zur Aufklärung der Lage eingesetzt wurden und nicht zur Manipulation oder Übernahme feindlicher Waffensysteme.

Der Estland Vorfall

Nach intensiven Studium der Ereignisse in Estland im Jahre 2007, zu denen ich durch Vice Admiral Tarmo Kouts MoP, (Head of the Estonian Delegation to the ESDA/WEU Assembly), Tallinn, umfassende Informationen zu einzelnen Ereignissen und Auswertungen erhielt, ist beispielhaft für einen erfolgreichen Cyberangriff, dass durch konzertierte „Denial of Service“-Angriffe Regierungs- und Verwaltungsstellen, ebenso wie die größte Bank Estlands nicht mehr online zu erreichen waren. Obwohl sich der Angriff auf Krankenhäuser, Energie-versorgungssysteme und Notrufnummern in Estland auswirkte, ist der Angriff dem Cybercrime zuzuordnen, da kein Staat nachweislich den Angriff durchführte, sondern allenfalls die Tätigkeit einiger Hacker aus falsch verstandenem Patriotismus duldete.

Cyberwar

Cyberwar ist eine Kriegsform zwischen Staaten und/oder "Asymmetric threats", die Cybersoldaten ermöglicht, virtuelle Angriffe gegen Prozessoren, Computer, Systeme oder Netzwerke auszuüben.



Gefährdungsstufen

Die erste Stufe eines Cyberwars beinhaltet die Ausforschung und die Begrenzung von Zielressourcen. Hierzu gehören beispielsweise der Einsatz von automatisierten Sniffern, Scans und Denial of service Angriffe, um Zieldienste zu unterdrücken oder zu stören.

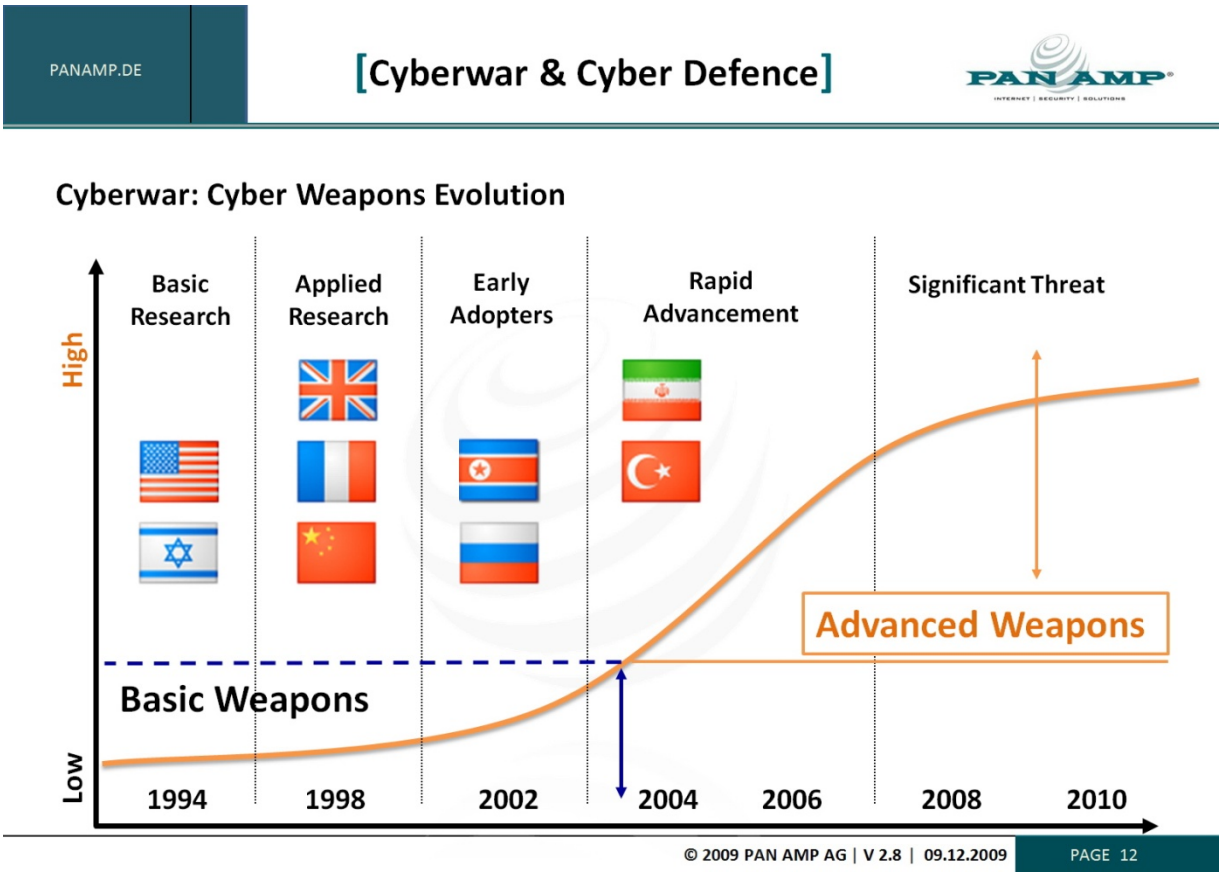
Die zweite Stufe beinhaltet die Infiltration und Manipulation von Daten und Datenverbindungen. Hierzu gehören Beispielsweise Hijacking sessions, der Einsatz von Trojans, Worms und Botnets, um zum Zwecke der Informations-gewinnung in fremde Computernetzwerke einzudringen.

Die dritte Stufe beinhaltet die virtuelle Manipulation zur physikalischen Zerstörung von Zielressourcen und Einheiten. Hierzu gehört Beispielsweise die Übernahme oder

Cyberwar: Weingarten Model mit Klassifizierung zur Schwere eines Cyberwars. [Vortrag-SecDef-Seite 8_20091209]

Zerstörung von zuvor manipulierter Hard- oder Software, von kritischen Infra-strukturanlagen der Energie, Wasser und Informationstechnologie sowie "Manipulated friendly fire" also die virtuelle Manipulation von Freund/Feind-Kennungen, bzw. die virtuelle Manipulation von Zieltechnologie oder Waffen zur Übernahme oder Vernichtung von Zieleinheiten.

Es bleibt festzustellen, dass sich bislang kein Cyberwar ereignet hat. Doch eine Vielzahl von Ereignissen der Jahre 2007 bis 2009 erlauben Rückschlüsse auf den Entwicklungsstand und die Weiter-entwicklung von Waffen hin zu "Advanced Cyberwar Weapons".



So begann die Evolution der Cyberwar Waffen mit der Grundlagenforschung im Jahre 1994 durch das Referat "Information Warfare and Strategy" in den USA. Schon seit den neunziger Jahren arbeiteten Staaten an digitaler Kriegsführung. So kann die erfolgte Aufrüstung und Weiterentwicklung von "Advanced Cyberwar Weapons" in China und den USA seit dem Jahr 2007 als Beginn des "Cold Cyberwar" bezeichnet werden.

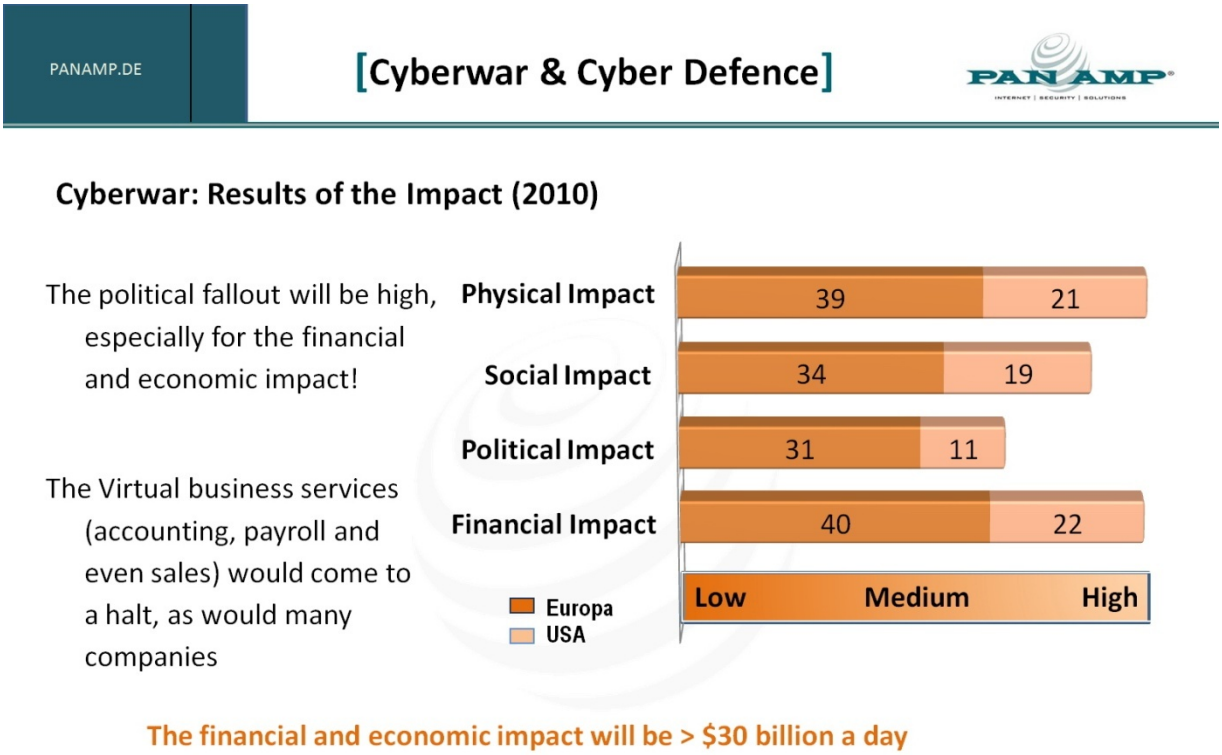
Es ist davon auszugehen, dass 60% aller Staaten bis 2014 zumindest eine "Basic-Level" Waffe für den Einsatz im Cyberwar besitzen. Hierdurch wird ein zukünftiger Cyberwar zu einer signifikanten Bedrohung Europas, da heutzutage Staaten und "Asymmetric threats" auch in kürzester Zeit in der Lage sind, Systeme zur Ausführung von Cyber-Attacken zu erwerben. Durch die geringen Entwicklungskosten für Basis-

Cyberwar: Evolution der Cyberwaffen. [Vortrag-SecDef-Seite 12_20091209]

Waffen zur Durchführung eines Online-Angriffes, die sich auf 50.000 bis 100.000 Euro beziffern lassen, sind insbesondere asymmetrische Auseinandersetzungen im Netz vorprogrammiert und finden zwischen der terroristischen Vereinigung Al-Qaida und westlichen Staaten bereits statt.

Ein großes Risiko: Das Internet

Insbesondere der Missbrauch des Internets für einen Cyber-Angriff stellt ein hohes Risiko da, da mit Lichtgeschwindigkeit jedes mit dem Internet verbundenen Zielsystems getroffen werden kann. Die hierzu berechnete Vorwarnzeit liegt bei < 2 Sekunden.



Konfliktfall: Cyberwar

In einer Zeit, in der die tägliche Onlineaktivität eine Selbstverständlichkeit darstellt und die Nutzung von eCommerce, online-banking und social networks zum Tagesablauf gehören, wird der tatsächliche Wert und der hohe Nutzen von Daten, Informationen und intakten Netzwerken aller Voraussicht nach erst durch einen Konfliktfall bewusst.

Kommt es zu einem Cyberwar, dass heißt zu einem Krieg zwischen Staaten über das Internet, würde dieser letztlich alle miteinander vernetzten Staaten treffen und gravierende politische sowie vor allem ökonomischen Schaden anrichten. Ein internationales Abkommen zur Begrenzung von Cyberwar Waffen ist bereits heute notwendig und sollte dringend von den Vereinten Nationen aufgenommen werden.

Ökonomische Schäden eines Cyberwars. [Vortrag-SecDef-Seite 15_20091209]

Schutzmaßnahmen

Insbesondere unter der Kenntnis der bestehenden Backbone-Netze, die insbesondere Europa und die USA datentechnisch verbinden, gleichen die Internetverbindungen in den USA und Europa "einer Burg mit mehr als 500 Toren". Wenn alle Tore attackiert werden, müssen auch alle verteidigt werden und je mehr Infrastruktur beschädigt wird, desto mehr werden sich die Angriffe auf die vorhandenen und intakten Ressourcen der Teilnetze verteilen und diese im Falle eines Cyberwars belasten. Wenn somit die USA per Cyberwar angegriffen werden, ist damit zu rechnen, dass auch Europäische Teilnetze des Internets tangiert werden.

Als Folge von immensen Überlastungen können auch verschlüsselte Verbindungen, die beispielsweise zwischen militärischen Einrichtungen im Internet bestehen, zusammen brechen. Was in militärischen Kreisen als eine gut zu verteidigende Anhöhe gilt, stellt die Netzstruktur Saudi Arabiens für den Fall eines Cyberwars da. Anders als in den meisten Staaten haben die Saudis die Möglichkeit, die Internet-Backbones in ihr Land direkt zu administrieren, in der Kapazität zu begrenzen oder abzuschalten. Gleiches gilt für verschiedene Teilnetze im Land. Damit hält die Regierung ein wirkungsvolles Instrument in der Hand, mit dem sich im Krisenfall eines Cyberwars Schaden begrenzen lässt und nationale Teilnetze nur geringfügig beeinflusst werden.

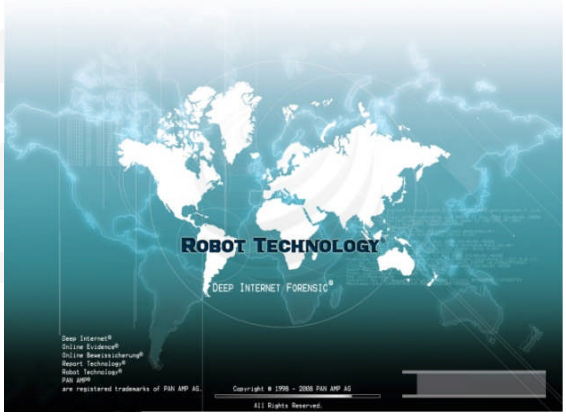
Cyber Defence

Als logische Konsequenz der Möglichkeit eines künftigen Cyberwars ist es daher dringend erforderlich, eine Europäische bzw. Nato-Strategie zur militärischen Verteidigung des virtuellen Raumes der Mitgliedsstaaten aufzubauen. Jeder Mitgliedsstaat sollte sich zudem in Form einer institutionalisierten staatlichen Verteidigung, die sich mit entsprechenden Mitteln auf die Möglichkeit eines Krieges per Internet vorbereitet, für einen kommenden Cyberwar rüsten. Der Ausbau von eigenständiger, militärischer Infrastruktur und die Absicherung nationaler Teilnetze sollten im Fall eines Cyberwars abgeschlossen sein, damit eine effektive Verteidigung erfolgen kann.

„Jeder Krieg wird zukünftig mit einem Angriff aus dem Cyberspace beginnen und effektive Gegenmaßnahmen im Cyberwar werden vorbereiteten Staaten vorbehalten sein“.

Weitergehende Informationen

Der Leistungsbereich „Cyber Defence“, der PAN AMP AG, entwickelt Technologien und Systeme zur militärischen Verteidigung des virtuellen Raumes.



Weitere Informationen und Berichte zum Thema Cyberwar & Cyber Defence stehen im Internet zur Verfügung: www.panamp.de

Kontakt

PAN AMP AG
Ausschläger Elbdeich 2
D-20539 Hamburg
Tel.: +49 (40) 55 30 02 – 0
Fax : +49 (40) 55 30 02 - 100
E-Mail: info@panamp.de
Internet: www.panamp.de