

Verwandte Meldungen

Indien: Eigenes Betriebssystem für mehr Sicherheit

Abwehr von Cyberattacken wird immer schwerer

Cyberkrieg: Banken erschüttern interne Angriffe

McAfee warnt vor "Kaltem Cyberkrieg"

Weitere Meldungen

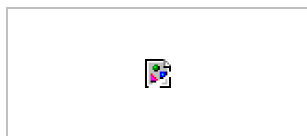
Handy "X-Ray" im transparenten Retro-Look

Österreich und China unterzeichnen Memorandum of Understanding

International anerkannt: Die Quantentechnologie des AIT

TeleNetfair: Netzwerk-Treffpunkt baut aus

Monster Jobcorner


 Suche:

 PLZ:

 Detailsuche 

Finden Sie uns auf Facebook



Werbung

pte101018025 Computer/Telekommunikation, Politik/Recht

Share |



"Genfer Konvention" für Cyberkonflikte gefordert Militärethiker: "Sind mit einem langen Kalten Cyberkrieg konfrontiert"

Buffalo/Wien (pte/18.10.2010/13:50) - Mit der zunehmenden Bedeutung von Computern wächst auch die Zahl an Cyberattacken auf Systeme von Datenbanken, über Stromversorgung bis hin zur Finanzindustrie. "Im Gegensatz zu konventioneller Kriegsführung gibt es für den Cyberkrieg nichts, was nur im Entferntesten einer Genfer Konvention gleichkommt", warnt der Militärethiker Randall R. Dipert, Philosophieprofessor an der University of Buffalo <http://www.buffalo.edu>. Dennoch

wird international fleißig aufgerüstet. "Ich würde sagen, wir sind mit einem langen Kalten Cyberkrieg konfrontiert", meint daher der Philosoph.

"Derzeit erfolgt ein Hochrüsten. Aber keiner weiß genau, was bei Attacken passieren und welche Kollateralschäden es geben kann", bestätigt der Sicherheitsexperte Joe Pichlmayr, Geschäftsführer von Ikarus Software <http://www.ikarus.at>, im Gespräch mit presetext. Er weist auf den Wurm Stuxnet als Beispiel, welche Cyberwaffen heute schon denkbar sind.

Ungeahnte Wirkung

Der Krieg im Cyberspace hat gewisse Parallelen zu realweltlichen Konflikten. "Eine Option bei Cyberattacken ist, möglich stark die Infrastruktur zu beeinträchtigen", erklärt Pichlmayr. Ein Beispiel dafür ist ein Angriff auf die Stromversorgung, dessen Auswirkungen schwer zu kontrollieren wären. Manchen Theorien zufolge war genau das der Zweck von Stuxnet. Sollte dieser Wurm tatsächlich speziell iranische Kraftwerke treffen, wären beispielsweise die aufgetretenen Infektionen deutscher Industrieanlagen letztendlich Kollateralschäden.

"Die willentliche Zerstörung oder Beeinträchtigung von Daten oder Algorithmen sowie Denial-of-Service-Angriffe könnte gewaltigen Schaden an Menschen, Maschinen, künstlichen Systemen oder der Umwelt anrichten", warnt Dipert. Dabei besteht unter anderem die Gefahr, dass wichtige zivile Systeme langfristig beeinträchtigt werden, beispielsweise in Krankenhäusern. Doch es existieren keinerlei Regeln gegen solche Attacken, während physische Angriffe auf Spitäler gegen die Genfer Konvention verstoßen.

Regeln im Wettrüsten

"Stuxnet hat uns vor Augen geführt was machbar ist. Umso verwunderlicher ist unsere nach wie vor gering entwickelte Wahrnehmung, wie sehr wir von unseren Infrastrukturen abhängen", meint Pichlmayr. Es sei daher sinnvoll, nach Regeln für die Cyberkriegsführung zu fragen. Für den Experten ist nicht verwunderlich, dass gerade Amerikaner wie auch der ehemalige CIA-Chef Michael Hayden dieses Thema ansprechen (presetext berichtete: <http://presetext.com/news/100730024/>). "Hoch industrialisierte Staaten könnten schließlich am stärksten getroffen werden", erklärt der Ikarus-Geschäftsführer.

Der Philosoph Dipert spricht sich jedenfalls für eine eingehende Beschäftigung auch mit den moralischen Aspekten der Cyberkriegsführung aus. Er betont, dass das Phänomen des Cyberkriegs längst Realität ist und ortet einen Kalten Cyberkrieg.

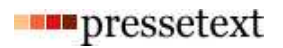


Computersysteme: Regelloses Schlachtfeld im Kalten Cyberkrieg (Foto: pixelio.de, Paul-Georg Meister)

21.10.2010

"Genfer Konvention" für Cyberkonflikte...

"Dieser wird durch begrenzte, aber häufige Schäden an Informationssystemen charakterisiert, während Nationen, Konzerne und andere Parteien die Waffen testen und sich auf eine Art Gleichgewicht hinbewegen." (Ende)



Aussender: [pressetext.redaktion](#)
Redakteur: Thomas Pichler
email: pichler@pressetext.com
Tel. +43-1-81140-303

Wie fanden Sie diese Meldung?



Weitersagen



[Startseite](#) | [Abo](#) | [Aussendung](#) | [Termine](#) | [Pressefotos](#) | [Adhoc-Dienst](#) | [Fotodienst](#) | [Toplocations](#) | [Archiv](#) | [Produkte](#) | [pressetext4Joomla](#)
© 1997-2010 [Pressetext](#) | [Nutzungsbedingungen](#) | [AGB](#) | [Impressum](#) | [Deutschland](#) | [Schweiz](#) | [Europa](#) | [Corporate](#) | [Kontakt](#)