

## Cyberwar 2.0 23.01.2012

**BERLIN** (Eigener Bericht) - Die Bundesakademie für Sicherheitspolitik bereitet die Kriegführung im virtuellen Raum vor. Der militärpolitische Think Tank lädt für Anfang Mai dieses Jahres zu einer Konferenz, die sich mit den Aufgaben und Kompetenzen des von der Bundesregierung eingerichteten "Nationalen Cyber-Abwehrzentrums" befassen soll. Gefordert wird, das Zentrum in die Lage zu versetzen, nicht nur zu reagieren, sondern auch "selbst zu agieren", also etwa Angriffe mit Computerviren durchzuführen. Die Bundesakademie für Sicherheitspolitik kooperiert dabei eng mit der Telekom-Tochtergesellschaft T-Systems, die bereits seit längerem an einer gemeinsamen "Sicherheitsrahmenarchitektur" für Bundeswehr, Polizei und Geheimdienste arbeitet. Erklärtes Ziel ist es, ein virtuelles Netzwerk zu schaffen, das den deutschen Repressionsbehörden ein gemeinsames Vorgehen etwa bei der Grenzüberwachung und der Personenfahndung ermöglicht. Speziell für das deutsche Militär entwickelt T-Systems sogenannte Führungs- und Waffeneinsatzsysteme, die sowohl die Treffgenauigkeit erhöhen als auch die Abstimmung der Truppen auf dem Schlachtfeld gewährleisten sollen.

### Cyber-Abwehrzentrum

Wie die Bundesakademie für Sicherheitspolitik (BAKS) mitteilt, wird sie am 7. und 8. Mai dieses Jahres eine Konferenz über die Aufgaben und Kompetenzen des von der Bundesregierung eingerichteten "Nationalen Cyber-Abwehrzentrums" veranstalten. Dem in der deutschen Verfassung verankerten Trennungsgebot zwischen Polizei, Militär und Geheimdiensten zum Trotz versammelt das "Cyber-Abwehrzentrum" Mitarbeiter aller Repressionsdienste. Vertreten sind neben dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) Bundespolizei, Bundeskriminalamt (BKA) und Zollkriminalamt, der für die Bekämpfung innenpolitischer Gegner zuständige Verfassungsschutz und der mit Auslandsspionage befasste Bundesnachrichtendienst (BND) sowie die Bundeswehr. Gemeinsames Ziel ist die Sicherung behördlicher und privatwirtschaftlicher Computernetzwerke gegen Hacker- und Virenangriffe, was der Bundesakademie für Sicherheitspolitik jedoch offenbar nicht weit genug geht. Rhetorisch wird gefragt, ob ein rein defensives Vorgehen bei "Sicherheitsvorfällen" in der Informationstechnik (IT) wirklich ausreiche: "Muss ein derartiges Abwehrzentrum nicht in der Lage sein, selbst zu agieren?"[1]

### Politische Umwälzungen kornern

Bei der Durchführung der Konferenz kooperiert die BAKS nach eigener Aussage eng mit T-Systems, einer Tochtergesellschaft der Deutschen Telekom.[2] T-Systems fordert seinerseits eine "umfassende, gesamtstaatliche Sicherheitsarchitektur, die alle notwendigen Kräfte miteinander verknüpft" und neben Polizeidienststellen und Rettungskräften auch Bundeswehr und Geheimdienste einbezieht. Die von T-Systems gelieferte Informationstechnik soll Firmenangaben zufolge in diesem Zusammenhang dazu beitragen, die Repressionsbehörden lückenlos zu vernetzen, und ihnen dadurch nicht nur die Generierung eines "gemeinsamen Lagebildes", sondern auch ein "gemeinsames Vorgehen" ermöglichen. Wie das Unternehmen weiter ausführt, könnten nur auf diese Weise "globale Herausforderungen und Bedrohungen" gekontert werden. Gemeint sind sowohl "Umweltgefahren" und "Seuchen" als auch "politische Umwälzungen und kulturelle Auseinandersetzungen mit unabsehbaren Folgen".[3]

### Grenzkontrollen und Verfolgung

Unter anderem bietet T-Systems laut einer Selbstdarstellung "Behörden und Organisationen mit Sicherheitsaufgaben" spezielle "software- und hardwaretechnische Systemlösungen" für Grenzkontrollen. Dabei wird beispielsweise ein Foto eines Reisenden aufgenommen, das dann, mit Personenangaben und biometrischen Daten verknüpft, an "allen weiteren Stationen im gesamten Abfertigungsprozess automatisch zur Verfügung" steht. Bestehen Zweifel an der "Rechtmäßigkeit" des Grenzübertretts, erhalten die jeweiligen Kontrolleure einen "Alarmhinweis". Auch für die "Verfolgung von Verdachtspersonen" liefert T-Systems nach eigenen Angaben die entsprechende Informations- und Kommunikationstechnik. Ermöglicht werde auf diese Weise die "globale Vernetzung der polizeilichen und erkennungsdienstlichen

Informationsdatenbanken", heißt es. Da das angebotene IT-System gleichzeitig die "vernetzte Operationsführung unterschiedlicher Einheiten und die zivilmilitärische Kooperation" unterstütze, könnten die Repressionsbehörden "gesuchte Personen über die eigene Dienststruktur hinaus unverzüglich identifizieren und sofort handeln".[4]

### **Idealer Partner der Streitkräfte**

Für Bundeswehr und Rüstungsindustrie entwickelt T-Systems nach eigenen Angaben neuartige "Führungs- und Waffeneinsatzsysteme", die sowohl die Treffgenauigkeit als auch das Zusammenwirken verschiedener Truppenteile auf dem Schlachtfeld verbessern sollen. So werden etwa Kriegsschiffe laut T-Systems "in Zukunft ebenso vernetzt sein wie Großunternehmen" und über ein "Gigabit-schnelle(s) Glasfasernetz" verfügen.[5] Im Angebot sind außerdem "satellitengestützte Kommunikationssysteme" samt "mobile(n) und ortsfeste(n) Bodenstationen" sowie "Führungs- und Kontrollsegmente(n)".[6] Bereits seit einigen Jahren verfügt das deutsche Militär über das von T-Systems vertriebene digitale Bündelfunksystem "Tetra", das es Interventionseinheiten ermöglicht, in einem beliebigen Einsatzland ein autarkes, mobiles Kommunikationsnetz zu betreiben (german-foreign-policy.com berichtete [7]). Wie das Unternehmen erklärt, sieht es sich selbst als "ideale(n) Partner für Streitkräfte und die Wehrtechnische Industrie" [8] bei der Wahrnehmung "friedenserzwingende(r) Aufgaben in der ganzen Welt" [9].

### **Tarnadressen**

Auch dem deutschen Auslandsgeheimdienst steht T-Systems als IT-Dienstleister zur Seite. So wurde 2008 publik, dass das Unternehmen den BND mit geheimen IP-Adressen ausgestattet hat, die die Verschleierung von Datenspuren im Internet ermöglichen. Medienberichten zufolge soll der BND die getarnten Adressen unter anderem dazu genutzt haben, unter falscher Identität Einträge in der Online-Enzyklopädie "Wikipedia" zu ändern.[10] Offenbar führt T-Systems den in Firmenpublikationen proklamierten "Cyberwar 2.0" also schon seit längerem.[11] Für Organisationen wie die Bundesakademie für Sicherheitspolitik und das "Nationale Cyber-Abwehrzentrum", die ebenfalls einen "proaktiven" Umgang mit Hacker- und Virenangriffen diskutieren, ist das Unternehmen damit unverzichtbar.

[1], [2] Die Deutsche Cyber-Sicherheitsstrategie - Neue Bedrohungen, neue Lösungen?  
www.baks.bund.de

[3], [4] T-Systems: Mit vereinten Kräften. Für innere und äußere Sicherheit. Frankfurt/Main  
(Broschüre des Unternehmensbereichs "Corporate Marketing and Communications")

[5] Führungs- und Waffeneinsatzsysteme; www.t-systems.de

[6] Satellitenkommunikation; www.t-systems.de

[7] s. dazu **Todesdrohung per Handy**

[8] Netzinfrastrukturen; www.t-systems.de

[9] Satellitenkommunikation; www.t-systems.de

[10] Geheime IP-Nummern des BND veröffentlicht; blog.ins.de 20.11.2008. IP-Adressbereiche des BND aufgetaucht; netzpolitik.org 13.11.2008

[11] René Reutter (T-Systems): Cyberwar 2.0 - Wie Datenspionage funktioniert. In: All About Security (Hg.): Information Security. Wielenbach (Security Advisor ePublication, T-Systems Special-Edition)

Copyright © 2005 Informationen zur Deutschen Außenpolitik

[info@german-foreign-policy.com](mailto:info@german-foreign-policy.com)