

# **Sifa-Post**

*Neues zu Sicherheit und Kriminalität*

15. April 2009

---

sifa - SICHERHEIT FÜR ALLE, Aktion gegen Kriminalität

Postfach 23  
CH-8416 Flaach  
Tel: 052 301 31 00  
Fax: 052 301 31 03  
PC-Konto: 87-370818-2

mail to: [info@sifa-schweiz.ch](mailto:info@sifa-schweiz.ch)

*Für den Inhalt ist verantwortlich:  
Ulrich Schliuer, Geschäftsführer sifa*

Wir sind Ihnen dankbar, wenn Sie uns Änderungen  
Ihrer E-Mail-Adresse mitteilen.

*Elektronischer Ernstfall*

## **Sind wir für den Cyber-War gerüstet?**

In der heutigen Zeit des Cyber-Wars wird die Sicherheit der eigenen Computernetze immer wichtiger; dies vor allem in sicherheitsrelevanten Bereichen wie der Armee.

Die Deutsche Bundeswehr wurde erst kürzlich Opfer eines Hacker-Angriffs, welcher zu massiven finanziellen Konsequenzen führte – ganz zu schweigen von den Sicherheitslücken. Diesen Entwicklungen muss schnellstmöglich entgegengewirkt werden.

### **«Hacker in Uniform»**

Die eingesetzten «Waffen» sind Werkzeuge aus dem Bereich der Informatik. Ziel ist es zum Beispiel, die Computersysteme des Gegners bzw. der Gegner so zu beeinträchtigen, dass sie nicht ihren Zweck erfüllen. Massive Hacker-Angriffe auf Netzwerke in Kanzleramt und Ministerien haben die deutsche Bundesregierung aufgeschreckt: Mit einer Bundeswehr-Sondereinheit will sie jetzt dem elektronischen Ernstfall begegnen. Die «Hacker in Uniform» sollen auch lernen, fremde Netze auszukundschaften und zu zerstören. Estland und Russland führten im Jahr 2007 Krieg gegeneinander. Im Internet legten Hacker gezielt offizielle Webseiten Estlands lahm. Und dieser Cyber-War blieb kein Einzelfall. Wie kann man sich als Land gegen solche Angriffe schützen?

### **Moderne Kriegführung**

An Amerikas berühmtester Militärakademie West Point lernen die angehenden Offiziere nicht nur den Umgang mit scharfen Waffen, sondern auch die modernen Mitteln der Cyber-Kriegführung. In einem separaten Trainingskurs müssen sie in vorgegebene Netze eindringen, Webseiten hacken oder diverse Server mit Attacken überschütten. Der Kurs endet mit einer Drei-Tages-Übung, in der die gegnerischen Netze «ausser Gefecht» gesetzt werden müssen. Der Internet-Einsatz, um den Gegner zu beeinflussen und zu zermürben wird immer bedeutsamer. Bereits im Februar 2007 erklärte das Pentagon, dass der Grossteil der Angriffe über das Internet aus China komme, vermutlich mit Unterstützung durch die Regierung. Dabei würden etwa technische Entwicklungen ausgespäht, aber auch versucht, die Aktivitäten des Pentagons zu beobachten und «Schläfer» in die Pentagon-Netzwerke für künftige Aktionen einzuschleusen. Verwiesen wurde auf ein Papier der chinesischen Regierung,

nachdem diese anstrebe, bis zur Mitte des Jahrhunderts einen «Informationskrieg» gewinnen zu können.

Zwar streiten sich weltweit die Experten, ob ein Begriff wie Cyber-War korrekt ist, weil es in solch einem Krieg keine Toten und Verletzten gibt, andererseits besteht aber anscheinend Einigkeit darüber, dass die Abwehr solcher Bedrohungen zu den Aufgaben der Streitkräfte eines Landes zählt. Das VBS hatte 2003 über den Start eines wissenschaftlichen Projekts mit dem Namen «Information Operations» orientiert. Vorgesehen war eine Truppe, die 500 bis 600 Mann umfasst. Sie soll bei Bedarf militärische Kommunikationssysteme schützen, Hackerangriffe abwehren und gegnerische Informationsstrukturen lahmlegen können. Das Projekt wurde jedoch nicht weiter konsequent verfolgt. Vom Cyber-War dauernd zu reden, genügt offensichtlich nicht. Hier muss die Armee jetzt Führung beweisen.

Computergestützte Kriegführung gibt es schon seit dem Ende des Zweiten Weltkriegs. Ein Krieg im Informationsraum funktioniert anders als ein Krieg mit Waffen. So sagt Ralf Bendrath, Politikwissenschaftler und Experte in Sachen Internet und Sicherheitspolitik:

*«Während man die Flugbahn und Detonationswirkung einer Granate recht präzise berechnen kann, geht das bei in die Welt gesetzten Informationen nicht. Jedenfalls nicht immer so leicht, und nicht so präzise. Die Regeln sind hier eben nicht die Gesetze der Physik, sondern die sich ständig wandelnde Kommunikation zwischen Menschen.»*

### **Parlamentarischer Vorstoss**

Nationalrat Ulrich Schlüer hat in der Frühjahrsession der Eidgenössischen Räte eine Interpellation zum Cyber-War eingereicht. Darin fragt er den Bundesrat:

1. Könnte ein solcher Hacker-Angriff gegen die Netze der Schweizer Armee verhindert werden? Wie zuverlässig sind unsere Netze im Allgemeinen gegen Cyber-War geschützt?
2. Was unternimmt die Schweiz für die Internet-Sicherheit? Sind zusätzliche Massnahmen geplant?
3. Verfügt die Schweiz sowohl über defensive wie über offensive Möglichkeiten zur Bekämpfung von Angriffen auf Netzwerke?
4. Zu welchen Gegenmassnahmen ist die Schweiz fähig?
5. Werden die privaten und beruflichen Hacker-Kenntnisse der Angehörigen der Armee für die Sicherung der Schweizer Armeenetzwerke eingesetzt? Wenn ja, in welchem Umfang? Wenn nein, warum werden diese Ressourcen nicht genutzt?

#### **Die sifa fordert**

Auf die Frage, wie die Schweiz auf Bedrohungen aus dem Cyber Space reagiert, fehlt weiterhin jede Antwort. Auch die Schweiz muss sich der vielfältigen Möglichkeiten der elektronischen Kriegführung endlich bewusst werden. Sie hat ihre Computernetze gegen Cyber-War zu schützen. Die sifa fordert deshalb: Zur Abwehr der Bedrohungen durch den so genannten Cyber-War und zum Schutz besonders gefährdeter Einrichtungen – wie Flughäfen, Kraftwerke etc. ist mit der Schaffung einer professionellen Spezialtruppe zu begegnen. Diese kann bei Bedarf durch Miliz-Spezialisten ausgebaut werden. Mit deren Ausbildung auf der Grundlage umgehend zu schaffender Abwehr- und Gegenschlags-Doktrinen ist sofort zu beginnen.

*Reinhard Wegelin/sifa*

***Wir bitten Sie: Verbreiten Sie diesen Kommentar an alle Ihnen zugänglichen Adressen.***

---

***Werden Sie sifa-Mitglied.***

Informationen erhalten Sie bei:

sifa - SICHERHEIT FÜR ALLE, Postfach 23, 8416 Flaach

Tel. 0041 (0)52 301 31 00

Fax 0041 (0)52 301 31 03

[info@sifa-schweiz.ch](mailto:info@sifa-schweiz.ch)

***Besuchen Sie die «sifa» im Internet:***

[www.sifa-schweiz.ch](http://www.sifa-schweiz.ch)