Bensberger Gespräche
24.-26. Januar 2011 in Bensberg

Tagungsdokumentation
Dokumentation: Christiane Toyka-Seid

Dienstag, 25. Januar

Arbeitsgruppe 2 „Virtuelle Sicherheit – Bedrohungen aus dem Internet“

Referenten: Peter Welchering, VoxMundi Medienanstalt GmbH, Kornwestheim, Sam May, Security Research Lab GmbH, Berlin
Moderation: Manfred Kloiber, Deutschlandradio, Köln

Diskutiert wurden unterschiedliche Fragen, die sich im Zusammenhang mit der virtuellen Sicherheit und den Entwicklungen im Internet auftun. Inwieweit ist der Kriegsbegriff tauglich im Zusammenhang mit Angriffen auf Datennetze, die für das Leben in Deutschland entscheidend sind (z.B. Energieunternehmen, Infrastrukturnetze)? Unklar ist hier, wer Täter ist, wer „Feind“ ist (beim Beispiel Stuxnet wurde das sehr deutlich). Auch Ort und Ziel der Handlung sowie Einsatz der Mittel sind nicht klar zu bezeichnen. Der Begriff „virtueller Krieg“ ist sehr diffus, weil oftmals mit denselben technischen (Angriffs)Mitteln wirtschaftliche wie auch sicherheitsrelevante Interessen verfolgt werden. Weder von den Methoden, noch von den Instrumenten oder den agierenden Personen aus kann man Schlüsse auf die Qualität eines Krieges schließen.

Ist aber, da Angriffe im virtuellen Netz zu enormen Störungen des öffentlichen Lebens führen können und dramatische Folgen für die Sicherheit des Landes haben können, der Staat dafür verantwortlich, hier für Sicherheit zu sorgen? Muss er in den Bereichen, wo wesentliche Interessen aller Bürger/innen betroffen sind – wie im Bereich der Infrastruktur, bei Energie und Bahn – Schutzmaßnahmen ergreifen?

Nach lebhafter und kontroverser Diskussion, bei der es u.a. um die Klärung des Kriegsbegriffs auch im internationalen Vergleich (USA: Deutschland) ging verständigte man sich darauf, die Verantwortung des Staates zu bejahen, weil die Wirtschaft den Schutz der Bürger (den diese zu Recht einfordern) nicht gewährleisten könne.

Doch wer ist für diesen Schutz zuständig? Das Militär, die Polizei? Handelt es sich bei Angriffen auf virtuelle Netze um kriminelle Handlungen oder sind es Angriffe, bei denen die Bundeswehr handeln muss? Müssen Strukturen aufgebaut werden, um bei solchen Angriffen zurückschlagen zu können oder geht es vor allem auch darum, präventiv zu handeln?

Was muss der Staat tun, wie handelt er aktuell? Derzeit stehen hinsichtlich Internetsicherheit Verbote im Mittelpunkt staatlichen Handelns, gefordert wird von vielen Fachleuten mehr Engagement des Staates bei der Prävention (D-Mail, Zertifizierung)

Diskussionsbedarf gibt es weiterhin zu vielen Fragen im Zusammenhang mit virtuellen Angriffen und virtueller Sicherheit:
Wie sind die neuen Angriffsoptionen zu bewerten? Könnte ein Cyberschlag humaner sein als der konventionelle oder nukleare Krieg, weil er möglicherweise (Stuxnet) unblutiger und günstiger ist? Greifen die völkerrechtlichen Bestimmungen zu Krieg, Kombattantenstatus etc. auch in diesem Bereich? Wie geht man damit um, dass es Handlungsmöglichkeiten gibt, für die es keine rechtlichen Vorgaben gibt?

Es wurde deutlich, dass die politische Bildung im Dialog mit der Bundeswehr hier einen wichtigen Beitrag zu Information und Aufklärung leisten kann.