AGA 8: Proliferation of Nuclear Technologies

Zeit: Donnerstag 17:00–18:30 Raum: HSZ-04

Hauptvortrag AGA 8.1 Do 17:00 HSZ-04

Laserisotopentrennung und Proliferation — •Werner Fuss — Garching

General Electric und Hitachi wollen in Wilmington/USA eine kommerzielle Anlage zur Anreicherung von 235U mit einem Laserverfahren der australischen Firma Silex Systems aufbauen. Die Genehmigung dafür liegt seit September 2012 vor. Aus den spärlichen Angaben (UF6, 16/mum, Isotopenselektivität 10 bis 20) kann man schließen, dass es sich um mehrstufige Vielfotonen-Dissoziation (selektive Anregung mit schwachen Lasern um 16 /mum, dann Dissoziation bei höherer Intensität und etwas längerer Wellenlänge) im kalten Molekülstrahl handelt. Die Laser sind gepulste CO2-Laser mit diskreter Frequenz, die in tiefkaltem para-H2 Raman-verschoben werden. Die hohe Isotopenselektivität lässt vermuten, dass eine solche Anlage (1) schnell arbeitet, so dass Überwachungszeiträume kurz sein müssen, (2) klein ist, so dass sie leicht versteckt werden kann, (3) schnell aufgebaut werden kann. Die Proliferationsüberwachung kann also Probleme bekommen. Mir scheint, Punkt 1 ist richtig, Punkt 2 nur begrenzt und Punkt 3 trifft nicht zu. Für Exportkontrolle bieten sich an u.a. CO2-Laser hoher Wiederholfrequenz (>500 Hz) und 16/mum-Optik.

AGA 8.2 Do 18:00 HSZ-04

Cyber meets Nuclear - Stuxnet and the Cyberattacks on Iranian Centrifuges — •Matthias Englert — IANUS, TU-Darmstadt

In 2010 the computer worm Stuxnet attacked the information hardware of the Iranian uranium enrichment program. Stuxnet spread by USB flash drives and attacked SCADA software installed on Windows systems via several zero-day exploits. SCADA configures programmable logic controllers which control in the case of the Iranian centrifuge cascades frequency converter drives to choose the frequency of centrifuge motors. Thus the attackers were able to either change the rotation frequency of the rotor and thereby the separative power of the centrifuge or even destroy the fast spinning centrifuges by stopping and restarting them. The designers of Stuxnet must have had intimate knowledge of the facility design as e.g. the cascade connection scheme was programmed into Stuxnet. Based on this information some calculations of the Iranian cascade regarding the potential to produce highly enriched uranium will be presented using cascade simulation tools.

The use of such highly sophisticated computer attacks to sabotage a nuclear program shed a new light on the debate about cyber attacks and the use of information technology for kinetic attacks in general. The talk will address problems the weaponization of information technology poses for international security and will highlight some more recent developments.