Ich bin Jürgen von den Datenschützern Rhein Main und ich freue mich, dass ich hier so viele Menschen begrüßen kann.

Wenn wir hier hierüber sehen, sehen wir ein ziemlich hässliches Gebäude, das Generalkonsulat der USA. Das Generalkonsulat der USA. Das ist nicht nur eines der größten Generalkonsulate weltweit sondern auch eines der wichtigsten Standorte der CIA.

Die USA stellt einen der größten Aggressoren dar, die wir weltweit haben und aktuell können wir sehen, dass wir eine eskalierende Spirale an Aggressionen auf allen Ebenen haben: politisch, wirtschaftlich und eben auch militärisch - vor allem gegen Russland, aber auch gegen China, Nordkorea, aber auch gegen Europa. Die USA kennt da keine Grenzen mehr. Da werden Erinnerungen an den „Kalten Krieg“ wach.

Dazu passt sehr gut, dass die bundesrepublikanischen Rüstungsausgaben drastisch erhöht werden sollen; die 2% vom BIP dürfte Jedem ein Begriff sein. Da reden wir zukünftig von nahezu einer Verdopplung. Wir reden hier also von 37 Milliarden Euro. Diese sind in der Friedenspolitik wesentlich besser aufgehoben.

Das Stockholmer Friedensforschungsinstitut SIPRIS sieht Deutschland weltweit mit 2,4% an neunter Stelle der Rüstungsausgaben von 1.686 Milliarden Dollar. Das bedeutet, dass jeder Mensch jedes Jahr 225 Dollar an Rüstung ausgibt; inklusive jedem Säugling. Dabei gibt die USA mit Abstand am meisten für Rüstung aus, nämlich 36%. Danach folgen China mit 13% und Russland mit 4,1%.

Nicht eingerechnet in diese Rüstungsausgaben ist jedoch eine neue Kategorie von Waffe. Nach den konventionellen und A-, B- und C-Waffen kommen nun die "D-Waffen": Die digitale Aufrüstung. Auch hier spielt dieser Standort eine erhebliche Rolle. Durch die Veröffentlichungen bei Wikileaks wissen wir vom "Center of Cyber Intelligence", welches ein wichtiges Zentrum für den Krieg im Netz darstellt.

Diese Waffen sollen nicht nur in die Hände der Militärs, sondern auch in die Hände der Geheimdienste und Polizeien.

Darauf komme ich gleich noch einmal zurück.

Die Kosten für die digitale Aufrüstung sind enorm. Allein in Deutschland haben wir eine Aufstockung beim Militär von 6.000 auf 13.000 Soldatinnen und Soldaten nur für den Bereich Cyberwar. Der BND bekommt 300 Millionen Euro für Aktivitäten im digitalen Raum, die ganz klar dem offensiven Bereich zuzuordnen sind. Die realen Kosten sind jedoch vollkommen unklar und intransparent.

Wir müssen uns eines klar machen: Cyberwar meint immer Angriffskrieg Es gibt keine "Cyberverteidigung". Die nennt sich IT-Sicherheit. Auch die sogenannte "Gegenschlagstrategie" ist nichts anderes als ein Angriffskrieg. Das berührt möglicherweise Artikel 26 unseres Grundgesetzes, der eben einen solchen Angriffskrieg verbietet.

Die Folgen können wir heute schon sehen durch die Kollateralschäden von Stuxnet und WannaCry. Wir können davon ausgehen, dass wir solche Schäden zukünftig sehr viel häufiger sehen werden und sie werden sehr viel umfangreicher sein. Das gefährdet die gesamte IT-Struktur, die komplette Sicherheit unserer Systeme. Vor allem zivile Infrastruktur ist gefährdet, also auch Krankenhäuser, Feuerwehr, Strom- und Wassernetze. Denn Alles was wir heute benutzen und benötigen, wird über IT gesteuert. Dabei sind Cyberwaffen nicht abrüstbar und nahezu unkontrollierbar. Es geht eben nicht darum, irgendetwas in der Abrüstung zu verschrotten, denn Wissen kann man nicht verschrotten.

WannaCry führt uns zurück zur NSA.

WannaCry nutzte eine Sicherheitslücke aus, die die NSA geheimgehalten hatte. Ob sie sie auch selbst genutzt hat, wissen wir nicht. Wer Sicherheitslücken nicht schließt, eröffnet Anderen,

Militärs, Kriminellen, oder Terroristen die Möglichkeit, diese ihrerseits zu finden und zu nutzen. Das dürfen wir nicht zulassen.

Deutlich wird, und das hatte ich bereits erwähnt, dass nicht nur die Militärs diese Waffen bekommen sollen, sondern auch die Geheimdienste und Polizeien - nicht nur in den Vereinigten Staaten sondern auch hier bei uns in Deutschland.

Wir in Hessen müssen uns ja aktuell mit der Novellierung des Verfassungsschutzgesetzes beschäftigen, was deutlich macht, dass es eine wirkliche Kontrolle der Geheimdienste nicht geben wird. Dabei sollen die Geheimdienste immer mehr Aufgaben erhalten mit immer weitreichenderen Befugnissen und können immer tiefer in unser Leben eindringen über unsere IT-Systeme. Das ist heute schon brandgefährlich, doch mit dem "Internet der Dinge" potenziert sich diese Gefahr. Jedes dieser Systeme ist angreifbar, ist ein Einfalltor in unseren Kernbereich der Lebensgestaltung, aber auch in Systeme, die für uns lebenswichtig sind.

Das ist nichts anderes, als die digitale Kriegsführung in die Zivilbevölkerung zu tragen.

Das ist nichts anderes als ein ein permanenter digitaler Häuserkampf.

**Dagegen müssen wir aufstehen !**

**Stoppt die Eskalation !**

**Setzt euch ein für Abrüstung und Entspannungspolitik !**

**Cyberpeace statt War !**

Legende :
SIPRIS: Stockholm International Peace Research Institute, deutsch : *Stockholmer internationales Friedensforschungsinstitut*)
Stuxnet u. WannaCry: Computerwurm (Schadsoftware)