REDE

Konrad-Adenauer-Stiftung e.V.

RECHTSSTAATSPROGRAMM SÜDOSTEUROPA
THORSTEN GEISSLER

Oktober 2013

www.kas.de/rspsoe
www.kas.de

Die „fünfte" Kriegsdimension, Cyberwar als Herausforderung für das Völkerrecht

X. VÖLKERRECHTKONFERENZ, BONN, 16. – 17. OKTOBER 2013

Neben den mehr oder weniger traditionellen Kriegsschauplätzen Boden, Wasser, Luft und All gibt es längst eine fünfte Kriegsdimension, den Cyberwar, kriegerische Auseinandersetzungen im virtuellen Raum, vorwiegend mit Mitteln aus dem Bereich der Informationstechnik.

Erinnert sei daran, dass bereits im Kosovo-Krieg 1999 beide Seiten entsprechende Kampfmittel einsetzen, die NATO steuerte und kontrollierte nicht nur das Kriegsgeschehen mittels weltraumgestützter Systeme, sondern griff das serbische Telefonnetz an, brach auf elektronischem Weg in russische, griechische und zypriotische Banken ein, um Konten des serbischen Präsidenten Slobodan Milosevic zu sabotieren und leerzuräumen, serbische Kräften störten ihrerseits NATO-Server. Nach der Bombardierung der chinesischen Botschaft in Belgrad schalteten sich chinesiche Hacker ein, versandten virenverseuchte E-Mails, griffen u.a. die Internetpräsenzen des US-Energieministeriums an, auch die Website des Weißen Hauses musste drei Tage geschlossen werden.

Im April 2007 kam es dann zum ersten schweren Hackerangriff auf einen ganzen Staat, nämlich auf Estland. Webserver wurden mit einer Flut unsinniger Datenabfragen überschwemmt, bis sie unter der Last der Spams zusammenbrachen. Fast die gesamte staatliche Infrastruktur im Netz wurde lahmgelegt: Die Internetseiten des Präsidenten, der Ministerien, der behörden, von Schulen, Banken und vielen Zeitungen waren vorübergehend nicht mehr zu erreichen. Vier Tage dauerten die Angriffe, Eine Aktion des Kreml- so lautete die Vermutung in Estland. Doch dies wurde von Russland vehement bestritten und konnte nie bewiesen werden.

Auf dem NATO-Gipfel in Bukarest im April 2008 unterstrich die Allianz, sie wolle die „Fähigkeit bieten, Bündnismitglieder auf Verlangen bei der Abwehr eines Cyberangriffs zu unterstützen" und am 28.10.2008 wurde in Tallinn das „Cooperative Cyber Defence Centre of Excellence" als eines von zehn Centres of Excellence der NATO offiziell akkreditiert

Allerdings stellte dies keine Reaktion auf den Cyberangriff 2007 dar, Estland hatte dieses Zentrum vielmehr bereits 2003 gefordert und die Vorbereitungen zu einer wirksamen Internetverteidigung bzw. zur Befähigung, operative Massnahmen durchführen zu können begannen viel früher. Bereits unter der Amtszeit von Bill

Konrad-Adenauer-Stiftung e. V.

RECHTSSTAATSPROGRAMM SÜDOSTEUROPA
THORSTEN GEISSLER

Oktober 2013

www.kas.de/rspsoe
www.kas.de

Clinton wurde unter dem Namen Federal Intrusion Detection Network mit der Planung einer wirksamen Internetverteidigung begonnen, 1999 begann der Aufbau eine Info-War Teams. Selbstverständlich wurden auch in anderen Staaten frühzeitig ähnliche Maßnahmen getroffen, allerdings gingen Länder wie Russland China oder Indien dabei nicht so transparent vor wie die USA.

Ein Wort noch zu Deutschland: Mitte 2012 teilte das Bundesverteidiungsministerium dem Bundestag mit, die Bundeswehr vefüge nunmehr über eine „Anfangsbefähigung" für Attacken in „gegnerische Netze".

Bereits im November 2010 hatte die NATO jedoch ein Strategisches Konzept für die Verteidigung und Sicherheit der Mitglieder der Nordatlantik-Vertragsorganisation beschlossen und darin konstatiert: „Cyber-Angriffe geschehen immer häufiger, sind besser organisiert und kostspieliger, was den Schaden angeht, den sie staatlichen Verwaltungen, Unternehmen, Volkswirtschaften und potenziell auch Transport- und Versorgungsnetzen und anderer kritischer Infrastruktur zufügen; sie können eine Schwelle erreichen, die den Wohlstand, die Sicherheit und die Stabilität von Staaten und des euro-atlantischen Raums bedroht." Dies ist nichts anderes als die Feststellung, dass Cyberkrieg mittlerweile zum „fünften Schlachtfeld" geworden ist.

Bevor wir uns den rechtlichen Fragen widmen, die mit diesser Entwicklung einhergehen, müssen wir klären, welche Verfahren im Cyberkrieg üblicherweise zur Anwendung gelangen. Es sind dies:

- Spionage: Das Eindringen in fremde Computersysteme zum Zwecke der Informationsgewinnung
- Defacement: Veränderungen am Inhalt einer Website
- Diverse Formen von Social Engineering
- Einschleusen von kompromittierender Hardware, die bewusst fehlerhaft arbeitet oder Fremdsteuerung erlaubt
- Denial-of-Service Attacken, um feindliche Dienste zu stören oder vollständig zu unterdrücken und
- Materielle Angriffe, d.h. Zerstören, Sabotage zum Ausschalten von Hardware.

Erlauben Sie mir nun, einige rechtliche Fragen in diesem Zusammenhang aufzuwerfen, doch zunächst muss ich feststellen, dass es eine völkerrechtliche Definition des Begriffs „Cyber War" nicht gibt, ist zunächst zu klären:

- Wann ist ein Cyber-Krieg eine Kriegshandlung, wann nur, wenn überhaupt, eine Strafftat?
  Konkreter: Kann eine Cyber Operation überhaupt und wenn ja unter welchen Bedingungen eine Bedrohung oder einen Bruch des Friedens oder eine Angriffshandlung i.S.d. Artikel 39 der Charta der Vereinten Nationen darstellen? Doch selbst wenn dies bejaht wird, wäre noch das Völkerrechtssubjekt zu identifizieren, von dem dieser Angriff ausgeht.

- Zwar sind Kriege nach der Charta der Vereinten Nationen grundsätzlich völkerrechtswidrig, ein „ius ad bellum" im herkömmlichen Sinn gibt es nicht mehr, wohl aber stellt Artikel 51 der Charta klar, dass das „naturgegebene Recht zur indidviduellen wie kollektiven Selbstverteidigung" durch die Charta nicht beeinträchtigt wird, dies gilt jedoch nur für den Fall eines „bewaffneten Angriffs". Stellt eine Cyber-Attacke einen solchen „bewaffneten Angriff" dar?

- Dürfen Staaten, die Cyber-Kriegshandlungen führen, die Netzstrukturen neutraler Drittstaaten nutzen und welche Verpflichtungen haben

Konrad-Adenauer-Stiftung e. V.

RECHTSSTAATSPROGRAMM SÜDOSTEUROPA
THORSTEN GEISSLER

Oktober 2013

www.kas.de/rspsoe
www.kas.de

in diesem Zusammenhang betroffenen neutrale Drittstaaten?

- Reicht unser humanitäres Völkerrecht („ius in bello") aus, um einen angemessenen Schutz der in den gegenwärtigen internationalen Konventionen gegenwärtig geschützten Personenkreise auch füe den Fall von Cyber-Kriegshandlungen weiterhin angemessen zu schützen?

Um diese und andere Fragen zu beantworten, haben wir drei renommierte Experten eingeladen, die ich Ihnen vorstellen darf:

- Herr Stefan Sohm, Referatsleiter Völkerrecht /Rechtsgrundlagen Auslandseinsätze im Bundesministerium der Verteidigung
- Frau Hila Adler, Dozentin an zahlreichen wissenschaftlichen Einrichtungen in Israel insbesondere zu Fragen des Völkerrechts
- Und Prof . Seong Woo-Ji von der Rechtswissenschaftlichen Fakultät der Sungkyunkwan Universität Seoul, Korea.