USA: Warum ein „Cyber-9/11" nur noch eine Frage der Zeit ist

27.07.2017 | Originalartikel

Mit al-Qaida und dem Daesh hat der Westen zwei Gruppierungen in Stellung gebracht, die es erlaubten ein Bedrohungsszenario für die Bevölkerungen aufzubauen, welches wiederum genutzt wurde, um dem terroristischen-industriellen Komplex und dessen „Geschäftsmodell" Abermilliarden an US-Dollar und Euro zukommen zu lassen. Doch dieses „Terrorparadigma" scheint in den Köpfen der Menschen immer „weniger zu ziehen", so dass sich der terroristische-industrielle Komplex auf die Suche machen muss, einen neuen Bösewicht zu installieren.

Da aber neue Gruppen, wie beispielsweise die Gruppierung Khorasan nicht so „gezündet" haben, wie von den Verantwortlichen gedacht, sehen wir seit Kurzem ein neues Paradigma, das gerade kunstvoll von Geheimdiensten, Politik und Hochleistungspresse aufgebaut wird: das Cyberterrorparadigma.

Genauso wie das alte Terrorparadigma des „globalen Krieges gegen den Terror" (im Folgenden TP abgekürzt), braucht auch das Cyberterrorparadigma (kurz CTP) einen stetigen Strom an Gefahren, um die aufgeblasenen Budgets der Geheimdienste und Sicherheitsapparate im Westen zu rechtfertigen. Ebenso benötigt das CTP einen steten Fluss an „Onlinegefahren", um neue Massnahmen wie Staatstrojaner oder das auch in Russland offenbar beliebte Netzwerkdurchsetzungsgesetz der Öffentlichkeit verkaufen zu können. Und genauso wie beim „althergebrachten TP" wird jede „ausgenutzte Schwachstelle" bei der Cybersicherheit und jede „unbeabsichtigte Vermehrung von Cyberwaffen" (Stichwort CIA Vault 7) als Begründung herangezogen, um noch weitere Gelder zu erhalten und noch umfassendere Massnahmen im „Kampf um das Netz" umsetzen zu können.

Das alte Terrorparadigma des „globalen Krieges gegen den Terror" stützte sich dabei auf das „katalytische Ereignis" eines „neuen Pearl Harbors", 9/11. Wäre es daher verwunderlich, wenn wir alsbald ein „Cyber-9/11" (im weiteren C-9/11) erleben werden, das von den Regierungen (bzw. den dahinterstehenden eigentlichen Strippenziehern) dazu genutzt werden wird, das Internet vollkommen unter Kontrolle zu bringen?

Im Grunde genommen wurde bereits kurz nach dem 11. September das Mem eines C-9/11 aufgebaut. Schon 2003, als das Pentagon seine Pläne bekannt gab gegen „bestimmte Aktivitäten im Netz" vorgehen zu wollen – fast so als wäre das Internet ein „feindliches Waffensystem" -, malte der ehemalige Direktor der NSA das Bild eines Cyberangriffs an die Wand, „der dem Angriff auf das World Trade Center entspricht (equivalent to the attack

on the World Trade Center)", wenn die USA nicht eine neue Behörde schafft, die die Cybersicherheit gewährleistet. Seitdem wurden zahlreiche Berichte und Reports veröffentlicht, die sich immer auf 9/11 beziehen, um die Angst in der Öffentlichkeit vor Cyberterrorismus peu à peu zu steigern.

Natürlich wissen diejenigen, die sich mit diesen Berichten befasst haben, dass die vorgeschobene Cyberterrorhysterie aus einem ganz anderen Grund geschürt wird: es gibt einen im Voraus ausgearbeiteten Plan, den man der Öffentlichkeit bekannt geben wird, wenn diese aufgrund eines (virtuellen) False Flag-Vorfalls nach noch mehr Kontrolle und Überwachung im Internet schreien wird. Dabei müssen wir überhaupt nicht spekulieren, wie dieser Plan aussieht. Denn 2008 sagte der Rechtsprofessor der Harvard University, Lawrence Lessing auf einer Technologiekonferenz, dass das Äquivalent des verfassungszerstörenden Patriot Acts bereits in der Schublade liegt. Fertig ausformuliert, um schnellstmöglichst in Gesetzesform gegossen zu werden. Analog zu den Tagen nach 9/11, als plötzlich ein über Tausend Seiten starkes Gesetz namens Patriot Act aus der Schublade eines gewissen John Kerry, Ex-US-Aussenminister, hervor gezaubert wurde. Und alles was man jetzt noch braucht, um das gleiche „Verfahren" anwenden zu können, wäre ein C-9/11.

Dazu ein kurzer Auszug aus dem Video mit Lawrence Lessing:

Es wird ein i-9/11 [C-9/11] Ereignis geben. Das bedeutet nicht unbedingt einen al-Qaida-Angriff, es bedeutet ein Ereignis, bei dem die Instabilität oder die Unsicherheit des Internets bei einem bösartigen Ereignis offensichtlich wird, das dann die Regierung zu einer Antwort inspiriert. Sie müssen sich daran erinnern, dass nach 9/11 die Regierung den Patriot Act innerhalb von 20 Tagen erstellt und durchgewunken hat.

[…]

Ich habe also mit dem [ehemaligen Counter-Terror-Zar] Richard Clarke zu Abend gegessen und ich fragte ihn, ob es ein Äquivalent gibt, gibt es einen i-Patriot-Act, der nur auf ein wichtiges Ereignis als Ausrede wartet, um die Art und Weise wie das Internet funktioniert zu verändern. Er sagte: „Natürlich gibt es diesen."

(There's going to be an i-9/11 event. Which doesn't necessarily mean an Al Qaeda attack, it means an event where the instability or the insecurity of the internet becomes manifest during a malicious event which then inspires the government into a response. You've got to remember that after 9/11 the government drew up the Patriot Act within 20 days and it was passed.

[…]

So I was having dinner with [former counter-terrorism czar] Richard Clarke and I asked him if there is an equivalent, is there an i-Patriot Act just sitting

waiting for some substantial event as an excuse to radically change the way the internet works. He said „of course there is.")

Letztlich wartet das Cybersicherheitsestablishment nur darauf, dass ein spektakulärer Cyberterrorangriff stattfindet, um dann ein Ende des Internets, wie wir es heute kennen, einläuten zu können. Und das wird Dinge beinhalten wie die Identifikation per Fingerabdruck, um ins Internet zu dürfen, und diverse Filter oder vollumfassende Deep Packet Inspection-Verfahren.

Wenn wir wissen, dass seitens der Regierungen (und ihrer Strippenzieher) ein C-9/11 „herbeigesehnt" wird, um ihren i-Patriot Act verwirklichen zu können, stellen sich für mich zwei offensichtliche Fragen: Würden die USA und dessen Vasallen wirklich ein solches Ereignis herbeiführen/inszenieren? Und wen würde man dann als Sündenbock präsentieren?

Die erste Frage ist schnell beantwortet: Ja, sie würden ein solches Eregnis herbeiführen. Weil sie es schon einmal getan haben. Stichwort Stuxnet.

Stuxnet war ein Computerwurm, den die USA und Israel gemeinsam entwickelt hatten, um die Anreicherungsanlage für Uran im iranischen Natanz anzugreifen. Wie wir heute wissen, war Stuxnet nur ein Teil einer viel grösser angelegten Cyberattacke gegen den Iran – gemeinsam durchgeführt von den USA und Israel unter dem Decknamen „Nitro Zeus". Obwohl Stuxnet das Cyberpendant einer Präzisionsbombe sein sollte, nur geschaffen um ganz spezielle Computersysteme in Natanz anzugreifen, wurde er zu einem richtig grossen Problem für das ganze Internet. Warum erinnert mich das jetzt schon wieder an Vault 7, WannaCry und Co.?

Im Jahre 2016 wurde bekannt, dass CIA und NSA nicht nur zahlreiche Schwachstellen in diversen Softwareprogrammen und bei Hardwareeinzelteilen gefunden hatten, sondern – ganz im Gegensatz zu ihren früheren Versicherungen – dass diese auch nicht an die entwickelnden Firmen gemeldet wurden, so dass diese die Probleme beheben konnten. Stattdessen haben die US-Geheimdienste diese sogenannten Exploits regelrecht gehortet, um damit Zugriff auf Computersysteme von anderen Regierungen und Privatpersonen zu erhalten. Cybersicherheitsexperten warnten bei Bekanntwerden dieses Skandals, dass die Wahrscheinlichkeit dramatisch steigt, dass diese Schwachstellen von Kriminellen, Hackern und Terroristen eingesetzt werden. Und mit WannaCry, ein NSA-Exploit, wurde diese Warnung bittere Realität.

Seltsamerweise kommen nur wenige Menschen auf den Gedanken, dass man mit solchen Exploits doch wunderbar ein „Cyber Pearl Harbor" durchführen kann. Wobei die Täter – nach dann offizieller Lesart – nur aufgrund von WikiLeaks und Co. an diese heran kommen konnten. Paradox oder?

Aber wer könnte nun genau ein solcher Täter sein? Natürlich die Russen. Wer denn auch sonst, möchte man fast hinzufügen. Schliesslich ist Russland in den letzten Monaten als Paradebeispiel eines Sündenbocks aufgebaut worden, der selbst dafür verantwortlich gemacht wird, wenn in einem Strassenzug in einer deutschen Stadt das Licht ausfällt. Und wie wir Dank unserer Hochleistungspresse wissen, haben ja auch die Russen den Server des Democratic National Committees (DNC) gehackt. Einfach mal bei Hillary Clinton nach Beweisen fragen. Sie hilft bestimmt gerne weiter. *Ironie aus*

Die bisherigen „Geheimdienstberichte", die bislang in der Causa „russisches Wahlhacking" veröffentlicht wurden, waren vollständig „beweisfrei". Nichts anderes als eine politische Verlogenheit in Reinkultur. Dabei darf nicht vergessen werden, dass die Informationen in diesen „Geheimdienstberichten" ja nicht von den Geheimdiensten selber stammen, sondern mehr oder weniger auf Angaben des DNC selbst beruhen. Denn das DNC hat es bis heute abgelehnt die betroffenen Server dem FBI zur Untersuchung zu überlassen.

Natürlich ist es vorstellbar, dass Moskau sich in die Computersysteme des DNC gehackt hat. Auch wenn es keinerlei Beweise dafür gibt, ist es aus rein geheimdienstlicher Sicht durchaus möglich, dass dies getan wurde. Aber selbst wenn Russland den DNC gehackt hat, hat Russland nicht die Wahlen gehackt, wie uns immer suggeriert wird.

Aber bei all dem geht es nicht allein um Russland, den DNC-Hack oder die Podesta Mails. Es geht vielmehr darum, dass unsere Hochleistungspresse jeden Hack, jeden Wurm und jede Cyberattacke sofort ungeprüft Russland in die Schuhe schiebt und Moskau in ihren Schlagzeilen als Täter präsentiert. Auch wenn dann auf Seite 27 unter ferner liefen der unvermeidliche Rückzug zu dieser Schlagzeile auf Seite 1 zu finden ist, weil es dafür keinerlei Belege gibt. Wer hier konkrete Beispiele sucht, findet diese in einem exzellenten Artikel auf Moon Of Alabama.

So lächerlich diese Neo-McCarthy-Hysterie in den letzten Monaten bereits geworden ist, so haben wir erst vor Kurzem dessen Spitze mit der Katar-Krise erlebt. Alles begann damit (und das werden die wenigsten wissen, weil es so nirgends in unserer Hochleistungspresse zu finden ist), dass Katar seine Nachbarn Bahrain, Saudi-Arabien, Ägypten und die Vereinigten Arabischen Emirate beschuldigte, eine Hetzkampagne gegen Katar, die Muslimbrüderschaft, Iran, Hamas und Hisbollah gestartet zu haben. Zumindestens wurde das in einem ganz kleinen Artikel der Qatari News Agency geschrieben, der nicht einmal eine halbe Stunde online stand, bevor er wieder von der Seite der katarsischen Nachrichtenagentur verschwand.

Die Begründung Katars für den kurzeitig veröffentlichten Artikel bzw. seine Löschung? Hacker hätten den Server gehackt und diese Geschichte auf die

Website gepackt. Sofort nahm das FBI dies auf und machte die Russen als verantwortliche Hacker aus, während unsere Hochleistungspresse diesen Knochen begierig aufnahm und weiterverbreitete – ohne jedweden Beweis oder dem Versuch diese Anschuldigungen gegenüber Russland zu prüfen.

Welchen Sinn sollte es aber für Moskau machen, eine solche Fake News auf die Website der Qatari News Agency zu stellen? Um die Saudis wütend auf die Kataris zu machen? Wie ernsthaft solche Anschuldigungen seitens des FBI zu nehmen sind, sieht man im Übrigen daran, dass das FBI inzwischen – in gleicher Vehemenz wie zuvor – mit dem Finger nicht mehr nach Russland zeigt, um den Hack der Qatari News Agency-Website zu erklären, sondern auf die Vereinigten Arabischen Emirate deutet. Wahrscheinlich liegen sie hier auch falsch, aber es zeigt sehr gut, wie ernst man solche Schuldzuweisungen des FBIs nehmen kann.

Gerade dieses „Wechselspiel" – heute Russland, morgen die Vereinigten Arabischen Emirate – zeigt sehr gut, dass die Cybersicherheitskräfte nicht in der Lage sind, den Täter bei einem Cyberangriff benennen zu können. Natürlich gibt es verschiedene „Methoden", um dies für die Öffentlichkeit doch tun zu können: vom lächerlichen Zirkelschluss („Wir haben schon in der Vergangenheit diesen Angriffstyp der Gruppe XY zugeordnet, daher muss es diesmal auch dieselbe Gruppe sein!") angefangen, bis zum Klassiker schlechthin („Russische Wörter im Code. Sie haben schlichtweg vergessen ihre Spuren besser zu verschleiern!"). Aber aufgrund der WikiLeaks-Dokumente wissen wir heute, dass die CIA Werkzeuge besitzt, eigene Hacks wie solche aussehen zu lassen, die von anderen Ländern durchgeführt wurden. Und dann landen wir wieder dort, wo wir immer landen. Wir müssen den Geheimdiensten einfach glauben. So wie es unsere Hochleistungspresse seit Jahr und Tag auch tut. Schliesslich würden die Geheimdienste solche Taktiken nie einsetzen. Doppelschwur!

Damit wird eines der fundamentalen Probleme bei der Zuordnung von Cyperterror offensichtlich. Es ist die eine Sache, einen „physikalischen Angriff" zuzuzordnen, da nach einem solchen Angriff immer wenigstens ein paar forensische Beweise vorliegen. Beispielweise Überweisungen von grossen Geldsummen, die man zwar auch – zugegebenermassen – fälschen kann. Aber bei einer Cyberattacke gibt es nichts, was man untersuchen, was man als Ermittler verfolgen kann. Die einzigen, die eine Chance haben herauszufinden, was wirklich bei einer Cyberattacke passiert ist, sind diejenigen, mit direktem Zugang zu den Serverlogs. Und selbst diese Logs können manipuliert sein. Letztlich läuft es daher immer darauf hinaus, dass wir hören werden: „Vertraut den Geheimdiensten. Sie wollen nur unser Bestes. Oder haben sie schon jemals gelogen?"

Wenn man weiss, dass die Geheimdienste uns tatsächlich in unzählbaren Fällen belogen haben; dass sie Cyberwaffen bereits in der Vergangenheit erschaffen und „freigesetzt" haben; dass sie False Flag-Angriffe dazu nutzen, um politischen Feinden die Schuld dafür in die Schuhe schieben zu können, und dass Russland als Sündenbock für das kommende grosse C-9/11-Ereignis auserkoren wurde, dann sollte man auch wissen, was wir über die Dinge denken sollten, die man uns nach dem neuen „Cyber Pearl Harbor" präsentieren wird.

Quellen:

- *Bracing for "Cyber 9/11"*
- *Worse Than ISIS? A Primer on the Khorasan Group*
- *TERROR INDUSTRIAL COMPLEX TIMELINE*
- *Ukraine Cyber Attack Spreads Globally*
- *WannaCry Ransomware: Microsoft Calls Out NSA For ‚Stockpiling' Vulnerabilities*
- *Confirmed: US and Israel created Stuxnet, lost control of it*
- *US to create independent military cyber command*
- *US plans to ‚fight the net' revealed*
- *Information Operations Roadmap*
- *‚Cyber 9/11' risk warning*
- *Michael Chertoff: Cyber Terror Threat On Par With 9/11*
- *Digital Pearl Harbor, Cyber 9/11, and E-Qaeda*
- *US Government has prepared a „Patriot Act" for the Internet*
- *Want to use the Web? Your fingerprint, please.*
- *Obama Order Sped Up Wave of Cyberattacks Against Iran*
- *Massive US-planned cyberattack against Iran went well beyond Stuxnet*
- *The NSA Is Hoarding Vulnerabilities*
- *HOW THE CIA'S HACKING HOARD MAKES EVERYONE LESS SECURE*
- *What I Learned From the Intelligence Report on "Russian Hacking"*
- *The FBI Relied on a Private Firm's Investigation of the DNC Hack—Which Makes the Agency Harder to Trust*
- *The Undeniable Pattern Of Russian Hacking (Updated)*
- *Donna Brazile Just Called Russians "The Communists", And It Wasn't An Accident*
- *Bombshell in the Gulf: The GCC/Qatar Crisis*
- *Uproar In The Gulf Following Alleged Statements By Qatari Emir Condemning Gulf States, Praising Iran, Hizbullah, Muslim Brotherhood And Hamas*
- *Russian hackers to blame for sparking Qatar crisis, FBI inquiry finds*
- *CNN Exclusive: US suspects Russian hackers planted fake news behind Qatar crisis*
- *UAE hacked Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials*
- *UAE rejects allegations of hacking Qatari news agency*
- *WikiLeaks Reveals „Marble": Proof CIA Disguises Their Hacks As Russian, Chinese, Arabic…*