Während in den Vereinigten Staaten die Hysterie über eine angebliche Einmischung Russlands in die US-Wahlen zunimmt, bleibt es ein völliges Rätsel, warum die US-Nachrichtendienste sich auf "Indizien" verlassen sollten, wo sie doch die Fähigkeit besitzen, handfeste Beweise zu erbringen, sagen die ehemaligen US-Geheimdienstler der „**Veteran Intelligence Professionals for Sanity**" in einer Denkschrift, die vor wenigen Tagen auf Consortium News veröffentlicht und nun von **Tim Slater** und **Stefanie Intveen** ins Deutsche übersetzt wurde.

Behauptungen über Hackerangriffe im US-Wahlkampf ohne Beweis

Ein Bericht in der *New York Times* vom Montag, den 12. Dezember 2016 darüber, dass die CIA aufgrund von „überwältigenden Indizienbeweisen" glaube, der russische Präsident Wladimir Putin habe "Computerhacker mit dem Ziel, die Wahl zugunsten Donald J. Trumps zu drehen, eingesetzt", ist leider frei von jedem Beweis. Das ist nicht überraschend, denn härtere technische Beweise legen ein Leak nahe, nicht einen Hackerangriff – von Russen oder wem auch immer.

In der *Washington Post* vom Montag wird berichtet, dass Senator James Lankford (Republikaner, Oklahoma), ein Mitglied des Geheimdienstausschusses des Senats, zusammen mit anderen Senatoren eine Untersuchung der vermuteten Cyber-Angriffe Russlands durch beide Kongressparteien fordere. Der Senat könnte sich den üblichen Parteienstreit, Kosten und unnötige Verzögerungen ersparen, wenn er unsere kurze Denkschrift lesen würde.

Im Folgenden bedienen wir uns unserer Erfahrung, die wir in hochrangigen Positionen mit einem Schwerpunkt in den Bereichen Cyber-Aufklärung und –Sicherheit in Jahrzehnten gesammelt haben, um den Nebel aus Unwissen und Parteilichkeit zu lichten. Anonymität liegt uns fern; wir melden uns mit fester Überzeugung zu Wort und hoffen, dass wir damit ein Publikum erreichen können, welches unseren Verdiensten aus unserer langjährigen Arbeit in der US-Regierung und anderen Technologie-Arbeitsbereichen entspricht. Und obwohl es heutzutage sentimental klingen mag, bleibt unser Berufsethos als Nachrichtendienstmitarbeiter darin bestehen, die Fakten so darzustellen wie sie sind – ohne Furcht oder Parteinahme.

Wir haben uns die verschiedenen Behauptungen über Hackerangriffe angesehen. Für uns ist es ein Kinderspiel, sie zu widerlegen. Die fraglichen E-Mail-Enthüllungen sind das

Ergebnis eines Leaks, nicht eines Hackerangriffs. Der Unterschied zwischen einem "Leak" und einem "Hackerangriff" ist wie folgt:

Leak: Wenn jemand physisch Daten einer Organisation entnimmt, und sie einer anderen Person oder Organisation übergibt, wie es Edward Snowden und Chelsea Manning getan haben.

Hackerangriff: Wenn jemand von außen Betriebssysteme, Firewalls, oder sonstige IT-Schutzsysteme elektronisch durchdringt und dann Daten herauszieht.

Alle Anzeichen weisen auf ein Leak, nicht auf Hackerangriffe hin. Wenn es sich um Hackerangriffe gehandelt hätte, dann wüsste das die National Security Agency (NSA) – und würde sowohl Absender als auch Empfänger kennen.

Kurz gesagt, ein Leak erfordert die Entnahme von Daten in physischer Form – zum Beispiel auf einem USB-Stick; es gibt nur einen Weg, solche Daten zu kopieren und zu entnehmen, ohne eine elektronische Spur davon auf dem Server zu hinterlassen: mithilfe eines physischen Speichermediums.

Überwältigende technische Fähigkeiten

Nochmals: die NSA kann sowohl Absender als auch Empfänger identifizieren, wenn es sich um Hackerangriffe handelt. Vor allem aufgrund des von Edward Snowden veröffentlichten Materials können wir ein vollständiges Abbild des ausgedehnten inländischen Datenerfassungsnetzwerks der NSA liefern, einschließlich der Upstream-Programme wie Fairview, Stormbrew und Blarney. Diese umfassen mindestens 30 Firmen in den USA, die die Glasfasernetze betreiben, über welche die Festnetztelephonie und das World Wide Web laufen. Dadurch erhält die NSA einen beispiellosen Zugang zu Daten, die innerhalb der USA fließen und in die übrige Welt hinausgehen, sowie zu Daten, welche die USA durchqueren.

Mit anderen Worten: alle Daten, die von den Servern des Democratic National Committee (DNC) [Parteivorstand der Demokratischen Partei] oder von Hillary Rodham Clinton (HRC) – oder von irgendeinem anderen Server in den USA – verschickt werden, werden von der NSA gesammelt. Diese Datenübertragungen enthalten Zieladressen in sogenannten Paketen, die es ermöglichen, die Übertragung durch das Netz aufzuspüren und ihr nachzufolgen.

Pakete: Emails, die über das Internet verschickt werden, werden in kleinere Segmente, die man Pakete nennt, zerlegt. Diese Pakete werden in das Netz eingespeist, um an einen Empfänger geliefert zu werden. Das bedeutet, dass die Pakete auf der Empfängerseite

wieder zusammengesetzt werden müssen.

Um das zu erreichen, wird allen Paketen, die zusammen eine Nachricht bilden, eine Kennziffer zugeteilt, die es der Empfängerseite ermöglicht, sie einzusammeln und wieder zusammenzusetzen. Außerdem enthält jedes Paket die Internetprotokollnummern (entweder IPV4 oder IPV6) sowohl des Erstellers als auch des Endempfängers, welche dem Netz die Weiterleitung der Daten ermöglichen.

Wenn E-Mail-Pakete die USA verlassen, würden die anderen "Fünf-Augen" [*Five Eyes*]-Länder (GB, Kanada, Australien und Neuseeland) und die sieben, acht weiteren Länder, die sich mit den USA an der Massenerfassung von allem auf dem Planeten beteiligen, ebenfalls Aufzeichnungen darüber besitzen, wohin diese Email-Pakete nach dem Verlassen der USA gegangen sind.

Die Erfassungsquellen sind umfangreich; dazu gehören hunderte von *Trace Route*-Programmen, welche den Weg von Paketen, die das Netz durchqueren, aufspüren, und zehntausende von Hardware- und Softwareeinbauten in Verteilern [*switches*] und Servern, welche das Netz verwalten. Alle Emails, die von einem Server gezogen und an einen anderen geschickt würden, könnten durch all diese Erfassungsquellen zumindest teilweise erkannt und aufgespürt werden.

Unter dem Strich heißt das, dass die NSA wüsste, wo und wie irgendwelche "gehackten" Emails von den Servern des DNC oder HRC oder von einem beliebigen anderen Server durch das Netz geleitet worden wären. Dieser Vorgang erfordert manchmal einen genaueren Blick auf die Weiterleitungsinfo, um Zwischenclients auszusondern, aber letzten Endes können Sender und Empfänger über das Netz hinweg aufgespürt werden.

Die verschiedenen Methoden, mit denen die üblicherweise anonymen Sprecher von US-Nachrichtendiensten ihre Aussagen relativieren – indem sie Formulierungen wie "unsere starke Vermutung" oder "unsere Meinung" oder "unsere Einschätzung" usw. gebrauchen – zeigen, dass die angeblich "gehackten" Emails nicht über das Netz aufgespürt werden können. Angesichts der umfassenden Fähigkeiten der NSA zur Rückverfolgung von Emails ziehen wir den Schluss, dass die angeblich gehackten Server von DNC und HRC in Wirklichkeit nicht gehackt wurden.

Die Nachweise, die vorhanden sein sollten, fehlen; sonst hätte man sie sicher vorgebracht, denn das ließe sich ohne Gefahr für Quellen und Methoden machen. Daher folgern wir, dass *ein Insider die Emails durchsickern ließ* – wie es der Fall bei Edward Snowden und Chelsea Manning war. Ein solcher Insider könnte jeder in einem Ministerium oder einer Behörde

sein, der Zugang zu NSA-Datenbanken hat, oder eventuell jemand innerhalb des DNC.

Was die an die Medien gerichteten Bemerkungen dazu, was die CIA glaube, betrifft, so ist die CIA im Bereich der grundlegenden Kommunikationsdaten tatsächlich fast vollständig von der NSA abhängig. Daher bleibt es rätselhaft, warum die Medien mit seltsamen Geschichten über Hackerangriffe versorgt werden, die überhaupt keine Grundlage haben. Mit einem Wort: angesichts dessen, was wir über die bestehenden Fähigkeiten der NSA wissen, ist es völlig unglaubwürdig, dass die NSA nicht in der Lage wäre, jeden – ob Russe oder nicht – zu identifizieren, der versuchen würde, durch Hacking in eine US-Wahl einzugreifen.

Für den Vorstand, Veteran Intelligence Professionals for Sanity (VIPS)

- William Binney, ehemaliger Technischer Direktor, World Geopolitical & Military Analysis, NSA; Mitbegründer des SIGINT Automation Research Center (i. R.)
- Mike Gravel, ehemaliger Adjutant, Aufsichtsbeamter für höchste Geheimhaltungsstufe, Communications Intelligence Service; Beamter [*special agent*] des Counter Intelligence Corps und ehemaliger US-Senator
- Larry Johnson, ehemaliger Nachrichtendienstmitarbeiter [*Intelligence Officer*] bei der CIA und ehemaliger Beamter des US-Außenministeriums im Bereich Terrorismus-bekämpfung [*Counter Terrorism Official*]
- Ray McGovern, ehemaliger Infanterie- und Nachrichtendienstoffizier der US-Armee und Auswerter bei der CIA (i.R.)
- Elizabeth Murray, Deputy National Intelligence Officer für den Mittleren Osten, CIA (i.R.)
- Kirk Wiebe, ehemaliger Leitender Auswerter [*Senior Analyst*], SIGINT Automation Research Center, NSA (i.R.)