Ehemalige US-Geheimdienstexperten erläutern, warum der Vorwurf, Russland habe die Wahl des US-Präsidenten mit Hilfe von Hackern zugunsten Trumps beeinflusst, nicht zutrifft.

LUFTPOST

Friedenspolitische Mitteilungen aus der US-Militärregion Kaiserslautern/Ramstein
LP 177/16 – 15.12.16

Ehemalige US-Geheimdienstler äußern sich zu der Behauptung, russische Hacker hätten die US-Präsidentenwahl manipuliert

Veteran Intelligence Professionals for Sanity
(Ehemalige Geheimdienstmitarbeiter für Vernunft)
Consortium.news, 12.12.16
(https://consortiumnews.com/2016/12/12/us-intel-vets-dispute-russia-hacking-claims/)

Ehemaligen US-Geheimdienstlern ist es ein Rätsel, warum die US-Geheimdienste in der hysterischen Diskussion über die angebliche Beeinflussung der US-Präsidentenwahl durch Russland mit "Indizien" arbeiten; wenn die Hackerangriffe tatsächlich erfolgt wären, hätten sie doch unwiderlegbare Beweise dafür vorlegen können.

Memorandum

Die Behauptung, russische Hacker hätten die US-Wahl beeinflusst, ist nicht haltbar

Ein am Montag in der *New York Times* veröffentlichter Bericht, in dem behauptet wurde, die CIA könne mit "eindeutigen Indizien" nachweisen, "dass der russische Präsident Wladimir Putin Hacker eingesetzt hat, um die Wahl zugunsten Donald J. Trumps zu beeinflussen", führt keinen einzigen Beleg an, der diese Anschuldigung stützen könnte. Das hat uns nicht überrascht, weil alle bisher bekannt gewordenen technischen Angaben (über angeblich gehackte E-Mails, weitere Infos dazu unter http://www.n-tv.de/politik/Obama-will-Wahl-Cyberattacken-aufklaeren-article19295266.html) darauf schließen lassen, dass die besagten E-Mails weder von Russen noch von Experten anderer Staaten "gehackt" wurden, sondern durch interne "Leaks" in die Öffentlichkeit gelangten.

Ebenfalls am Montag hat die *Washington Post* berichtet, der republikanische Senator James Lankford aus Oklahoma, der dem Geheimdienst-Ausschuss des Senates angehört, habe gemeinsam mit anderen Senatoren gefordert, die vermuteten russischen Cyber-Angriffe von einer überparteilichen Kommission untersuchen zu lassen. Die Lektüre dieses kurzen Memorandums könnte den Senat vor ergebnisloser Zeitverschwendung und unnötigen Ausgaben bewahren.

Unsere nachfolgenden Ausführungen beruhen auf jahrzehntelangen geheimdienstlichen Erfahrungen – auch im Bereich Internet-Sicherheit – und sollen helfen, die aus durchsichtigen Motiven betriebene Vernebelung von Tatsachen zu durchschauen. Wir wollen nicht anonym bleiben, denn wir sind stolz darauf, uns nach langjähriger, meist verdeckt ausgeübter geheimdienstlicher Tätigkeit nun auch aufklärend an die Öffentlichkeit wenden zu können. Unser Ethos als Geheimdienstexperten verpflichtet uns immer noch dazu, furchtlos und ohne jede Begünstigung einfach die Wahrheit zu sagen – auch wenn das heute nicht mehr üblich ist.

Wir haben die Behauptungen über angebliche Hacker-Angriffe geprüft, und wegen unserer profunden Kenntnisse war es für uns ein Kinderspiel, sie alle zu widerlegen. Die enthüllten E-Mails wurden nicht gehackt, sie sind durch ein oder mehrere interne Leaks in die Öffentlichkeit gelangt. Wir erklären jetzt den Unterschied zwischen einem "Leak" und einem "Hack".

> Um ein **Leak** handelt es sich, wenn Personen wie Edward Snowden oder Chelsea Manning Daten einer Organisation aus deren Computersystem auf einen Datenträger kopieren und diesen Datenträger einer anderen Person oder Organisation übergeben.
>
> Ein **Hack** findet statt, wenn eine Person, die sich in einem weit entfernten Gebäude oder Land befindet, auf elektronischem Weg alle Firewalls und anderen Schutzeinrichtungen eines fremden Computersystems überwindet und auf elektronischem Weg Daten aus diesem System abzweigt.

Bei allen von uns untersuchten Fällen kann es sich nicht um Hackerangriffe gehandelt haben, denn die National Security Agency / NSA kann alle Hackerangriffe verfolgen und sowohl den Angreifer als auch den Angegriffen problemlos identifizieren.

Nur wenn der Datenklau von einer realen Person mit Hilfe eines transportablen Datenträgers (Speicherkarte, Stick oder CD) vor Ort vorgenommen wird, entstehen keine elektronischen Spuren, über die der Täter jederzeit zu identifizieren wäre.

Erstaunliche technische Fähigkeiten

Wir wiederholen noch einmal: Die NSA kann bei jedem über das Internet abgewickelten Datenaustausch (also auch bei jedem Hackerangriff) den Absender und den Empfänger, (bzw. den Angreifer und den Angegriffenen) ermitteln. Dank des von Edward Snowden veröffentlichten Materials wissen wir, dass die NSA – u. a. mit Hilfe ihrer Programme Fairview [s. https://consortiumnews.com/wp-content/uploads/2016/12/fairview.jpg], Stormbrew [s. https://consortiumnews.com/wp-content/uploads/2016/12/stormbrew-01.jpg] und Blamery [s. https://consortiumnews.com/wp-content/uploads/2016/12/Blarney.gif] – den Datenfluss in den Glasfasernetzen von mindestens 30 US-Kabelgesellschaften, das komplette öffentliche Telefonnetz und das gesamte World Wide Web überwacht. Die NSA kann also auf alle Daten zugreifen, die innerhalb der USA und in der ganzen Welt kursieren – auch auf die, welche die USA nur durchqueren.

Mit anderen Worten, alle Daten, die jemand aus Servern des Democratic National Committee / DNC (s. dazu auch https://en.wikipedia.org/wiki/2016_Democratic_National_Committee_email_leak), aus einem Server Hillarys Rodham Clintons / HRC oder aus irgendeinem anderen Server in den USA abgreift, werden auch von der NSA eingesammelt. Jeder Datentransfer enthält in einem sogenannten "Packet" (Paket) auch die Adresse des Empfängers und kann deshalb durch das gesamte Internet bis zu ihm verfolgt werden.

E-Mails werden vor dem Transport durch das Internet in kleinere Segmente, die so genannten "Packets" aufgeteilt, vor der Ankunft beim Empfänger aber wieder zusammengefügt.

Damit das geschehen kann, erhalten alle Packets, die zu einem Datentransfer gehören, die gleiche Identifikationsnummer. Außerdem trägt jedes Packet eine IPV4- oder IPV6-Nummer (s. https://de.wikipedia.org/wiki/IPv4), die seine Verfolgung im Netz ermöglicht.

Wenn die E-Mail-Packets die USA verlassen, kann auch in den anderen "Five-Eyes"-Staaten (s. https://de.wikipedia.org/wiki/UKUSA-Vereinbarung) Großbritannien, Kanada, Aus-

tralien und Neuseeland und in sieben oder acht weiteren ausgewählten Staaten, die eng mit den USA kooperieren, der Weg einer E-Mail bis zum Empfänger verfolgt werden.

Die Möglichkeiten der NSA, den weltweiten Datenverkehr zu kontrollieren, sind sehr vielfältig (s. dazu auch https://consortiumnews.com/wp-content/uploads/2016/12/Picture1.jpg , https://consortiumnews.com/wp-content/uploads/2016/12/Picture2.jpg , https://consortiumnews.com/wp-content/uploads/2016/12/Picture3.jpg , https://consortiumnews.com/wp-content/uploads/2016/12/Picture4.png und zu guter Letzt https://consortiumnews.com/wp-content/uploads/2016/12/Picture5.jpg]; mit Hunderten von Spürprogrammen können die Packets durch das gesamte Internet und in ganz unterschiedlichen Software- und Hardware-Produkten verfolgt oder immer wieder aufgefunden werden. Auch E-Mails, die in einem Server abgegriffen und zu einem anderen geleitet werden, sind mit den genannten Mitteln wenigstens teilweise zu verfolgen oder zu orten.

Daraus ergibt sich, dass die NSA auch alle in den Servern des DNC oder der Frau HRC "gehackten" E-Mails auf ihrem gesamten Weg durchs Internet – auch über Zwischenstationen – bis zum Hacker verfolgen könnte.

Wenn die meist anonym bleibenden Sprecher von US-Geheimdiensten verschwommene Formulierungen wie "vermutlich" oder "unserer Meinung bzw. Schätzung nach" verwenden, heißt dass im Klartext, dass die E-Mails in Wirklichkeit nicht "gehackt" wurden, weil sie dann auch den oder die Hacker benennen könnten. Da sie das nicht konnten, sind wir sicher, das die Server des DNC und der Frau HRC nicht gehackt wurden. .

Wenn es tatsächlich Hackerangriffe gegeben hätte, wären die Hacker auch gefunden und benannt worden, denn dazu hätte man weder die Quellen noch die Methoden preisgeben müssen. Daraus schließen wir, dass die E-Mails von einem Insider auf ein Speichermedium übertragen und weitergegeben wurden, wie das auch bei Edward Snowden und Chelsea Manning der Fall war. Dieser Insider könnte aus jedem Ministerium kommen, das Zugriff auf die NSA-Daten hat, oder auch im DNC bzw. in Frau Clintons Umgebung zu finden sein.

Warum sich die Medien auf die CIA berufen, bleibt uns ein Rätsel, denn die CIA könnte ihre Informationen nur von der NSA haben. Wir können uns auch nicht erklären, warum die Medien mit seltsamen Storys über russische Hacker gefüttert werden, die Trump zum Wahlsieg verholfen haben sollen, obwohl die NSA trotz ihrer vielfältigen Möglichkeiten keinerlei Beweise dafür vorlegen kann.

Für den Vorstand der Veteran Intelligence Professionals for Sanity / VIPS

William Binney, former Technical Director, World Geopolitical & Military Analysis, NSA; co-founder, SIGINT Automation Research Center (ret.)

Mike Gravel, former Adjutant, top secret control officer, Communications Intelligence Service; special agent of the Counter Intelligence Corps and former United States Senator

Larry Johnson, former CIA Intelligence Officer & former State Department Counter-Terrorism Official

Ray McGovern, former US Army infantry/intelligence officer & CIA analyst (ret.)

Elizabeth Murray, Deputy National Intelligence Officer for Middle East, CIA (ret.)

Kirk Wiebe, former Senior Analyst, SIGINT Automation Research Center, NSA (ret.)

Consortiumnews.com

US Intel Vets Dispute Russia Hacking Claims

December 12, 2016

As the hysteria about Russia's alleged interference in the U.S. election grows, a key mystery is why U.S. intelligence would rely on "circumstantial evidence" when it has the capability for hard evidence, say U.S. intelligence veterans.

Veteran Intelligence Professionals for Sanity

MEMORANDUM

Allegations of Hacking Election Are Baseless

A New York Times report on Monday alluding to "overwhelming circumstantial evidence" leading the CIA to believe that Russian President Vladimir Putin "deployed computer hackers with the goal of tipping the election to Donald J. Trump" is, sadly, evidence-free. This is no surprise, because harder evidence of a technical nature points to an inside leak, not hacking – by Russians or anyone else.
Seal of the National Security Agency

Monday's Washington Post reports that Sen. James Lankford, R-Oklahoma, a member of the Senate Intelligence Committee, has joined other senators in calling for a bipartisan investigation of suspected cyber-intrusion by Russia. Reading our short memo could save the Senate from endemic partisanship, expense and unnecessary delay.

In what follows, we draw on decades of senior-level experience – with emphasis on cyber-intelligence and security – to cut through uninformed, largely partisan fog. Far from hiding behind anonymity, we are proud to speak out with the hope of gaining an audience appropriate to what we merit – given our long labors in government and other areas of technology. And corny though it may sound these days, our ethos as intelligence professionals remains, simply, to tell it like it is – without fear or favor.

We have gone through the various claims about hacking. For us, it is child's play to dismiss them. The email disclosures in question are the result of a leak, not a hack. Here's the difference between leaking and hacking:

> **Leak:** When someone physically takes data out of an organization and gives it to some other person or organization, as Edward Snowden and Chelsea Manning did.
>
> **Hack:** When someone in a remote location electronically penetrates operating systems, firewalls or any other cyber-protection system and then extracts data.

All signs point to leaking, not hacking. If hacking were involved, the National Security Agency would know it – and know both sender and recipient.

In short, since leaking requires physically removing data – on a thumb drive, for example – the only way such data can be copied and removed, with no electronic trace of what has left the server, is via a physical storage device.

Awesome Technical Capabilities

Again, NSA is able to identify both the sender and recipient when hacking is involved. Thanks largely to the material released by Edward Snowden, we can provide a full picture of NSA's extensive domestic data-collection network including Upstream programs like Fairview, Stormbrew and Blarney. These include at least 30 companies in the U.S. operating the fiber networks that carry the Public Switched Telephone Network as well as the World Wide Web. This gives NSA unparalleled access to data flowing within the U.S. and data going out to the rest of the world, as well as data transiting the U.S.

In other words, any data that is passed from the servers of the Democratic National Committee (DNC) or of Hillary Rodham Clinton (HRC) – or any other server in the U.S. – is collected by the NSA. These data transfers carry destination addresses in what are called packets, which enable the transfer to be traced and followed through the network.

Packets: Emails being passed across the World Wide Web are broken down into smaller segments called packets. These packets are passed into the network to be delivered to a recipient. This means the packets need to be reassembled at the receiving end.

To accomplish this, all the packets that form a message are assigned an identifying number that enables the receiving end to collect them for reassembly. Moreover, each packet carries the originator and ultimate receiver Internet protocol number (either IPV4 or IPV6) that enables the network to route data.

When email packets leave the U.S., the other "Five Eyes" countries (the U.K., Canada, Australia, and New Zealand) and the seven or eight additional countries participating with the U.S. in bulk-collection of everything on the planet would also have a record of where those email packets went after leaving the U.S.

These collection resources are extensive [see attached NSA slides 1, 2, 3, 4, 5]; they include hundreds of trace route programs that trace the path of packets going across the network and tens of thousands of hardware and software implants in switches and servers that manage the network. Any emails being extracted from one server going to another would be, at least in part, recognizable and traceable by all these resources.

The bottom line is that the NSA would know where and how any "hacked" emails from the DNC, HRC or any other servers were routed through the network. This process can sometimes require a closer look into the routing to sort out intermediate clients, but in the end sender and recipient can be traced across the network.

The various ways in which usually anonymous spokespeople for U.S. intelligence agencies are equivocating – saying things like "our best guess" or "our opinion" or "our estimate" etc. – shows that the emails alleged to have been "hacked" cannot be traced across the network. Given NSA's extensive trace capability, we conclude that DNC and HRC servers alleged to have been hacked were, in fact, not hacked.

The evidence that should be there is absent; otherwise, it would surely be brought forward, since this could be done without any danger to sources and methods. Thus, we conclude that the emails were leaked by an insider – as was the case with Edward Snowden and

Chelsea Manning. Such an insider could be anyone in a government department or agency with access to NSA databases, or perhaps someone within the DNC.

As for the comments to the media as to what the CIA believes, the reality is that CIA is almost totally dependent on NSA for ground truth in the communications arena. Thus, it remains something of a mystery why the media is being fed strange stories about hacking that have no basis in fact. In sum, given what we know of NSA's existing capabilities, it beggars belief that NSA would be unable to identify anyone – Russian or not – attempting to interfere in a U.S. election by hacking.

For the Steering Group, Veteran Intelligence Professionals for Sanity (VIPS)

Signers see end of translation

www.luftpost-kl.de
VISDP: Wolfgang Jung, Assenmacherstr. 28, 67659 Kaiserslautern