Dieser Text wurde zuerst am 31.03.2023 auf www.craigmurray.org.uk unter der URL ‹https://www.craigmurray.org.uk/archives/2023/03/the-so-far-non-existent-vulkan-leaks/› veröffentlicht. Lizenz: Craig Murray, CC BY-NC-ND 4.0

Symbolbild (Bild: Gerd Altmann, Pixabay, CC0)

Die bislang nicht existierenden **Vulkan-Enthüllungen**

Der Guardian [1], die Washington Post [2] und Der Spiegel [3] haben heute (30.03.2023, Anm. d. Red.) „sensationelle", auf durchgesickerten Dokumenten basierende Enthüllungen über russische Cyber-Kriegsführung veröffentlicht. Dabei haben sie aber nur ein einziges, eher harmloses Dokument (in der Washington Post) hervorgebracht, das keinerlei Verbindungen zu anderen Dokumenten aufweist.

Autor: Craig Murray

ist Autor und Menschenrechtsaktivist. Von 1984 bis 2004 war er britischer Diplomat, zuletzt Botschafter in Usbekistan, sowie von 2007 bis 2010 Rektor der schottischen Universität Dundee. Falls Sie die Arbeit von Craig Murray unterstützen möchten, finden Sie hier die Details: ‹https://www.craigmurray.org.uk/support-this-website/›

(Anm. d. Red.: Wikipedia: Bei den Vulkan Files (...) handelt es sich um durchgesickerte E-Mails und andere Dokumente, die die Entwicklung von Sabotage-Software des russischen Unternehmens NTC Vulkan bezeugen.)

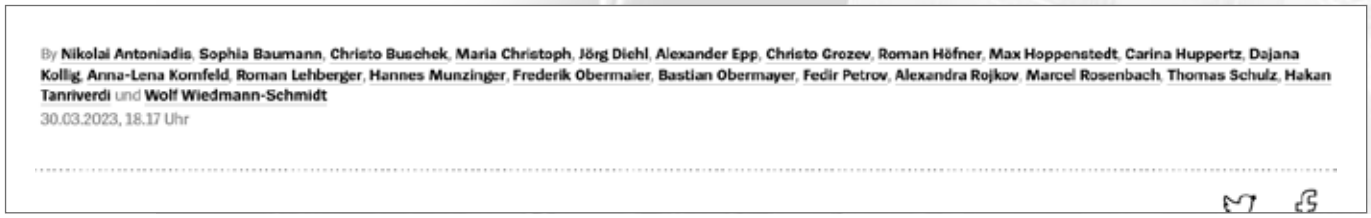
Wo sind diese Dokumente und was sagen sie eigentlich aus? Der Spiegel erzählt es uns:

> „Dies alles ist in 1.000 geheimen Dokumenten festgehalten, die 5.299 Seiten voller Projektpläne, Anweisungen und interner E-Mails von Vulkan aus den Jahren 2016 bis 2021 umfassen. Obwohl sie alle auf Russisch verfasst und extrem technisch sind, bieten sie einen einzigartigen Einblick in die Tiefen der russischen Cyberkriegspläne."

Okay … wo sind sie also?

Zehn verschiedene Medienhäuser haben bei den Leaks zusammengearbeitet, und die Artikel wurden von großen Journalistenteams in jeder einzelnen Publikation verfasst.

Der Artikel im „Guardian“ stammt von Luke Harding, Stilyana Simeonova, Manisha Ganguly und Dan Sabbagh, jener der „Washington Post“ von Craig Timberg, Ellen Nakashima, Hannes Munzinga und Hakan Tanriverdi. Und der „Spiegel“ nennt die Namen von 22 Journalisten!


By Nikolai Antoniadis, Sophia Baumann, Christo Buschek, Maria Christoph, Jörg Diehl, Alexander Epp, Christo Grozev, Roman Höfner, Max Hoppenstedt, Carina Huppertz, Dajana Kollig, Anna-Lena Kornfeld, Roman Lehberger, Hannes Munzinger, Frederik Obermaier, Bastian Obermayer, Fedir Petrov, Alexandra Rojkov, Marcel Rosenbach, Thomas Schulz, Hakan Tanriverdi und Wolf Wiedmann-Schmidt
30.03.2023, 18.17 Uhr

Das sind also 30 namentlich genannte Journalisten, womit jede Publikation ein großes Team für die Erstellung ihres eigenen Artikels eingesetzt hat.

Und doch kommt man beim Lesen dieser drei Artikel nicht um die Feststellung herum, dass sie sich … ähm ... bemerkenswert ähnlich sind.

Aus dem „Spiegel“:

„‚Diese Dokumente deuten darauf hin, dass Russland Angriffe auf zivile kritische Infrastrukturen und die Manipulation sozialer Medien als ein und dieselbe Aufgabe ansieht, die im Wesentlichen ein Angriff auf den Kampfeswillen des Gegners ist´, sagt John Hultquist, ein führender Experte für russische Cyberkriegsführung und Vizepräsident für nachrichtendienstliche Analysen bei Mandiant, einem IT-Sicherheitsunternehmen.“

Die „Washington Post“ schreibt:

„‚Diese Dokumente deuten darauf hin, dass Russland Angriffe auf zivile kritische Infrastrukturen und die Manipulation sozialer Medien als ein und dieselbe Mission ansieht, die im Wesentlichen ein Angriff auf den Kampfeswillen des Gegners ist´, so John Hultquist, Vizepräsident für nachrichtendienstliche Analysen bei der Cybersicherheitsfirma Mandiant.“

Und beim „Guardian“ liest man:

„John Hultquist, Vizepräsident für nachrichtendienstliche Analysen bei der Cybersicherheitsfirma Mandiant, die im Auftrag des Konsortiums eine Auswahl des Materials geprüft hat, sagte: ‚Diese Dokumente legen nahe, dass Russland Angriffe auf zivile kritische Infrastrukturen und die Manipulation sozialer Medien als ein und dieselbe Mission ansieht, die im Wesentlichen ein Angriff auf den Kampfeswillen des Feindes ist.´"

Beachten Sie, dass nicht nur das zentrale Hultquist-Zitat identisch ist.

Die Teams aus insgesamt dreißig Journalisten haben offenbar einen kompletten, mittels Copy-and-Paste erstellten Absatz nur minimal verändert. Der bemerkenswerte Gleichklang aller drei Artikel mit denselben Zitaten, Quellen und denselben Gedanken lässt jeden Leser erkennen, dass alle diese Artikel aus ein und derselben Quelle übernommen wurden. Die Frage ist, wer dieses zentrale Dokument erstellt hat. Ich vermute, dass es sich um einen der „fünf Sicherheitsdienste” handelt, die laut allen Artikeln konsultiert wurden.

Es ist aufschlussreich, dass alle drei Artikel die vollständig widerlegte Behauptung enthalten, Russland habe die Clinton- oder DNC-E-Mails gehackt. Und das, obwohl in keinem der drei Artikel auch nur der geringste Versuch unternommen wird, diese Behauptung mit einem der durchgesickerten Vulkan-Dokumente in Verbindung zu bringen oder gar Beweise dafür zu liefern.

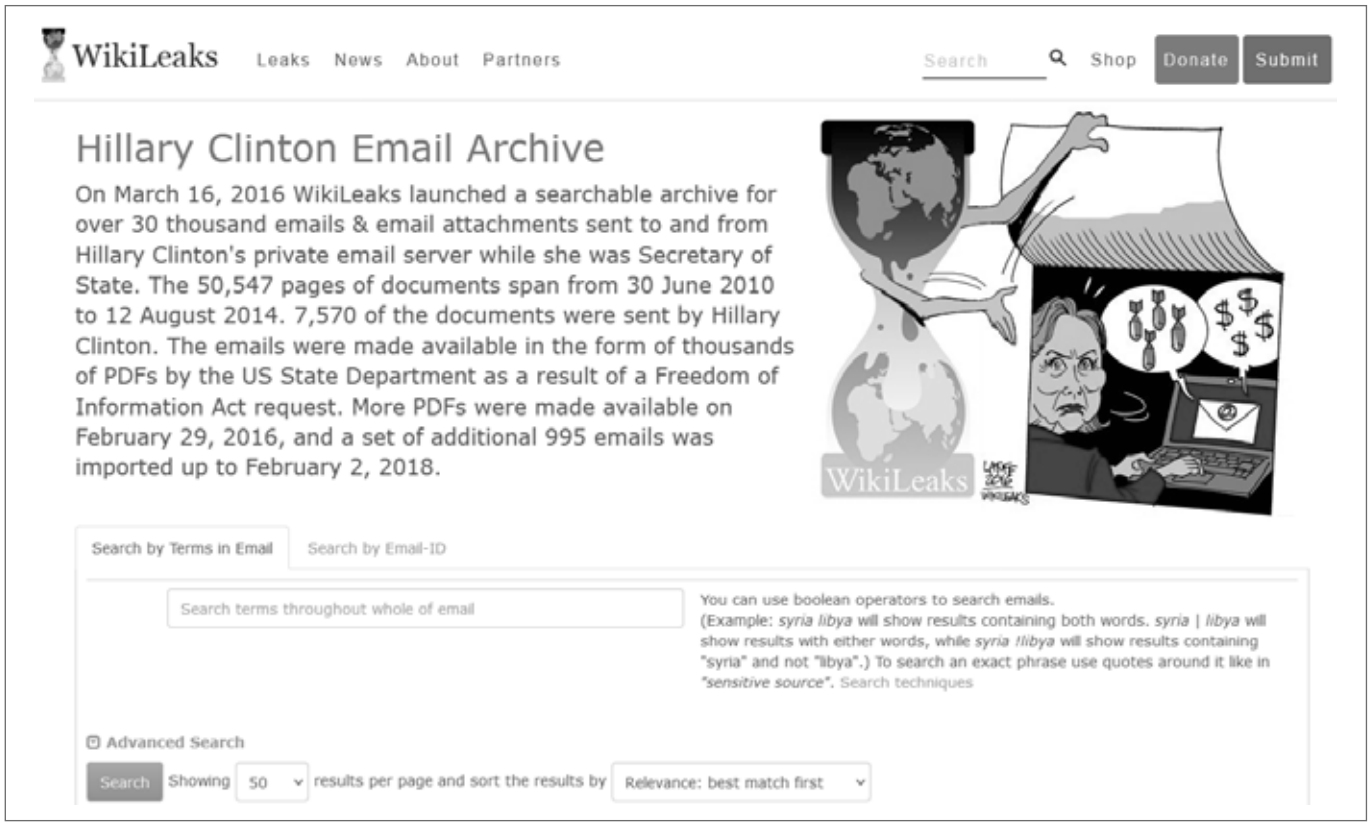
Der Gelegenheitsleser wird zu der Schlussfolgerung verleitet, das Vulkan-Leak enthalte irgendeinen Beweis für den Clinton-Hack, und zwar trotz der Tatsache, dass keine Beweise angeführt werden. Bei genauerer Lektüre wird auch in keinem der Artikel tatsächlich behauptet, die Vulkan-Dokumente enthielten auch nur einen Hinweis auf den Clinton-Hack oder irgendeine andere Art von Beleg, der diese Behauptung stützt.

Dass alle drei Journalistenteams unabhängig voneinander eine widerlegte Behauptung einstreuen, die nichts mit dem geleakten Material zu tun hat, das sie angeblich diskutieren, ist nicht sehr wahrscheinlich.

Auch hier ist wohl eindeutig von einer zentralen Quelle auszugehen, die den Unsinn der Clinton-Mails bekräftigt.

Die „Washington Post“ hat sich tatsächlich erdreistet, uns eine Seite Faksimile der durchgesickerten E-Mails zur Verfügung zu stellen, wo in der Tat auf die Möglichkeiten der Cyberkriegsführung zur Kontrolle oder Deaktivierung lebenswichtiger Infrastrukturen hingewiesen wird.

Publiziert auf Free21 am 19.06.2023, 6:00 Uhr



Das Problem ist jedoch, dass sie uns Seite 4 eines Dokuments ohne jeglichen Kontext zeigen. Warum gibt es keinen Link zum gesamten Dokument? Wir können sehen, dass es um die Erforschung solcher Fähigkeiten geht, aber vermutlich könnte das gesamte Dokument etwas über den Zweck dieser Forschung verraten – zum Beispiel, ob es sich um eine Offensive handelt oder um die Entwicklung einer Verteidigung gegen solche Angriffe.

Ich bin immer misstrauisch gegenüber Leaks, bei denen die eigentlichen Dokumente verborgen bleiben und wir nur das erfahren, was uns – wie in diesem Fall – von einer Propagandaorganisation mitgeteilt wird. Erst recht, wenn daran – selbst bei oberflächlicher Betrachtung – westliche Sicherheitsdienste, regierungs-finanzierte „Cybersicherheitsfirmen„ sowie Microsoft und Google beteiligt sind.

Wenn Wikileaks Dokumente veröffentlicht, geben sie die gesamten Dokumente frei, so dass die Leser sie ansehen und sich selbst ein Bild davon machen können, was sie wirklich beinhalten oder bedeuten, wie zum Beispiel die Veröffentlichung von Vault 7 über CIA-Hacking-Tools [4]. (Anm. d. Red.: Vault 7 bezeichnet eine Reihe von Dokumenten, die WikiLeaks ab März 2017 veröffentlichte. Darin werden detailliert Aktivitäten und Fähigkeiten der Central Intelligence Agency (CIA) der Vereinigten Staaten zur Cyber-Kriegsführung und zur Durchführung von elektronischer Überwachung beschrieben. Wikipedia)

Meine Lieblingsenthüllung in Vault 7 war, dass die CIA-Hacker gefälschte „Fingerabdrücke" hinterlassen, darunter auch Befehle in kyrillischer Schrift, um den Eindruck zu erwecken, dass die Russen die Täter waren. Wie gesagt, Sie können die aktuellen Dokumente auf Wikileaks einsehen [5].

Ich habe keinen Grund, daran zu zweifeln, dass Russland Techniken der Cyber-Kriegsführung einsetzt, aber ich habe absolut keinen Grund zu glauben, dass Russland dies mehr tut als westliche Sicherheitsdienste.

Diese Vulkan-Informationen deuten sogar darauf hin, dass die russische Cyber-Kriegsführung weniger fortgeschritten ist als die westliche. Ohne sich der Tragweite ihrer Aussagen bewusst zu sein, erzählen uns Luke Harding und sein Team vom „Guardian":

> In einem Dokument empfehlen Ingenieure Russland, seine eigenen Fähigkeiten durch die Verwendung von Hacking-Tools zu erweitern, die 2016 von der Nationalen Sicherheitsagentur der USA gestohlen und ins Internet gestellt wurden."

Das ist natürlich nur dann schlecht, wenn die Russen es tun.

Die Tatsache, dass es in keiner der Veröffentlichungen einen Querverweis auf die Snowden- oder Vault-7-Leaks gibt, zeigt, dass es sich um eine koordinierte Propagandaübung der Sicherheitsdienste handelt.

Es werden jedoch zahlreiche Beispiele für verschiedene Hackerangriffe angeführt, die angeblich von russischen Sicherheitsdiensten begangen wurden, ohne dass es irgendeine Verbindung zu einem Dokument in den Vulkan-Leaks gibt. Und es werden auch keine sonstigen Beweise angeführt – außer mehreren Verweisen auf Behauptungen von US-Behörden.

Der Artikel in der „Washington Post“ entspricht noch am besten vernünftigen journalistischen Standards. Er enthält diese wichtigen Sätze, die in Luke Hardings Leitartikel im „Guardian“ nicht zu finden sind:

„Diese Beamten und Experten konnten keine eindeutigen Beweise dafür finden, dass die Systeme von Russland eingesetzt oder für bestimmte Cyberangriffe verwendet wurden. Die Dokumente enthalten weder verifizierte Ziellisten noch bösartigen Softwarecode oder Beweise, die die Projekte mit bekannten Cyberangriffen in Verbindung bringen. Dennoch bieten sie Einblicke in die Ziele eines russischen Staates, der – wie andere Großmächte, einschließlich der Vereinigten Staaten – bestrebt ist, seine Fähigkeit zur Durchführung von Cyberangriffen mit größerer Geschwindigkeit, größerem Umfang und größerer Effizienz auszubauen und zu systematisieren.“

Das letzte Zitat ist natürlich der springende Punkt, und die „Washington Post“ verdient zumindest ein gewisses Lob dafür, dass sie ihn anerkennt. Und das kann man vom „Guardian“ oder dem „Spiegel“ nicht sagen. Aber selbst die „Washington Post“, die diesen Punkt anerkennt, lässt in keiner Weise zu, dass dadurch Ton oder Tenor ihres Berichts beeinflusst wird.

Natürlich gibt es überhaupt keinen Grund zu bezweifeln, dass der russische Staat seine Fähigkeiten zur Cyberkriegsführung entwickelt, ebenso wenig wie daran, dass kommerzielle Firmen wie Vulkan als Subunternehmer an diesen Arbeiten beteiligt sind.

Genau das gleiche gilt aber für die Vereinigten Staaten, das Vereinigte Königreich und jede andere große westliche Nation. Dutzende von Milliarden werden in die Cyberkriegsführung gesteckt, und die von den NATO-Staaten dafür eingesetzten Ressourcen übersteigen bei weitem die für Russland verfügbaren Mittel.

Und damit rückt diese große Übung antirussischer Propaganda ins richtige Licht. Hier sind einige wichtige Fakten dazu.

Betrachtet man die Artikel des „Guardian“, der „Washington Post“ und des „Spiegel“ zusammen, so ergibt sich folgendes Bild:

- Weniger als 2% des Textes sind direkte Zitate aus den angeblich durchgesickerten Dokumenten.
- Weniger als 10% der Artikel-Texte enthalten eine angebliche Beschreibung des Inhalts der Dokumente.
- Mehr als 15% der Artikel-Texte geben Kommentare westlicher Sicherheitsdienste und der Cyberkriegs-Industrie wieder.
- Über 40% des Textes besteht aus Beschreibungen behaupteter russischer Hacking-Aktivitäten, von denen in den eigentlichen Vulkan-Leaks nichts erwähnt wird.

Wir bekommen eine Seite von angeblich 5.000 durchgesickerten Informationen zu sehen, dazu einige Karten und Grafiken.

30 MSM-Journalisten waren also nötig, um diese plumpe Propaganda zu produzieren. Ich hätte Ihnen das allein in einer Nacht liefern können. Aus dem, was die Sicherheitsdienste direkt und indirekt geliefert haben, hätte ich lediglich drei geringfügig unterschiedliche Texte erstellen müssen. Aber ich verstehe die Verlockung, ein journalistischer Büttel der Macht zu sein, denn für diese dreckigen Dreißig war es leicht verdientes Geld.

Verzeihen Sie mir, wenn ich darauf hinweise: Diese Berichterstattung hängt ausschließlich von Ihren freiwilligen Abonnements ab, die diesen Blog am Leben erhalten. Jedermann kann diesen Beitrag frei reproduzieren oder neu veröffentlicht, auch in Übersetzungen. Ebenso können Sie ihn auch gern ohne Abonnement lesen.

Im Unterschied zu unseren Gegnern wie der „Integrity Initiative“, der 77th Brigade, Bellingcat, dem Atlantic Council und Hunderten anderer kriegstreiberischer Propagandaorganisationen, wird dieser Blog in keiner Weise von Staaten, Unternehmen oder Institutionen finanziert. Er wird ausschließlich durch freiwillige Abonnements seiner Leser betrieben, von denen viele nicht unbedingt mit jedem Artikel einverstanden sind, aber die alternative Stimme, die Insiderinformationen und die Debatte begrüßen.

Abonnements zur Aufrechterhaltung dieses Blogs werden dankbar angenommen:

<https://www.craigmurray.org.uk/support-this-website/>

Quellen:

[1] The Guardian, Luke Harding u. A. „`Vulkan-files`leak reveals Putins global and domestic cyberwarfare tactics", am 30.3.2023: *<https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics>*

[2] Washingtonpost, Craig Timberg u. A. „The "Vulkan Files" - Secret trove offers rare look into Russian cyberwar ambitions", am 30.3.2023: *<https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/>*

[3] Spiegel International, Nikolai Antoniadis „The "Vulkan Files" - A Look Inside Putin's Secret Plans for Cyber-Warfare", am 30.3.2023: *<https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236>*

[4] Wikileaks „Vault 7: CIA Hacking Tools Revealed", Leak-Serie, begonnen am 17.3.2017: *<https://wikileaks.org/ciav7p1/>*

[5] Wikileaks „Vault 7: CIA Hacking Tools Revealed", Dokument: *<https://wikileaks.org/ciav7p1/cms/page_2621751.html>*