

Warren Buffett warnt: „Es gibt Schlimmeres als COVID-19“

Autor: Andreas Hoose | 14. Juli 2021



US-Multimilliardär und Investment-Legende Warren Buffett glaubt, dass die nächste Pandemie schwerer ausfallen könnte als die aktuelle COVID-19-Krise. Microsoft-Gründer Bill Gates kommt zu ähnlichen Schlussfolgerungen.

In einem Interview mit dem US-Nachrichtensender CNBC sagte Buffett:

„Es wird eine weitere Pandemie geben. Wir wissen, dass es eine nukleare, chemische, biologische und nun auch eine Cyber-Bedrohung gibt. Diese Bedrohungen haben alle schreckliche Möglichkeiten. Es sieht nicht so aus, als wäre die Gesellschaft vollständig darauf vorbereitet, damit umzugehen.“

Und weiter:

„Ich habe gelernt, dass die Menschen nicht so viel wissen, wie sie zu wissen glauben. Aber am meisten habe ich gelernt, dass man die Pandemie kommen sehen konnte und dass dies nicht das Schlimmste ist, was man sich vorstellen kann. Die Gesellschaft kann sich nur schwer auf ferne Situationen vorbereiten, die aber möglich sind und früher oder später eintreten werden.“

[Hier der vollständige Artikel...](#)

Was könnte Buffett mit seiner verklausulierten Warnung meinen? Spontan fällt einem da die jüngste „Übung“ des World Economic Forum ein:

Erst vor wenigen Tagen hatten die Milliardäre um Klaus Schwab mit ihrem vor Jahresfrist schon einmal veranstalteten **„Cyber Polygon“**, einen Hacker-Angriff mit [schwerwiegenden globalen Folgen](#) simuliert. Nach den Vorstellungen der selbsternannten „Eliten“ stehen globale Cyber-Attacken ganz oben auf der Liste möglicher Bedrohungsszenarien. Von einer möglichen „Cyber-Pandemie“ ist da die Rede. Auffällig ist in diesem Jahr außerdem die Einbindung Russlands in das Planspiel.

In einem bemerkenswerten Beitrag schreibt Stefan Korinth dazu unter dem Titel **„Angriff mit Ansage“** für das Multipolar-Magazin:

Konferenzen und Übungen internationaler Organisationen gibt es häufiger – warum also sollte gerade diese Veranstaltung besondere Aufmerksamkeit erfahren? Die Antwort basiert auf einem gewissen Lerneffekt aus vorangegangenen Entwicklungen. Die US-Journalisten Johnny Vedmore und Whitney Webb von *Unlimited Hangout* [schreiben](#):

„Wenn die mächtigsten Menschen der Welt, wie zum Beispiel die Mitglieder des WEF, radikale Veränderungen vornehmen wollen, tauchen bequemerweise Krisen auf – sei es ein Krieg, eine Seuche oder ein wirtschaftlicher Zusammenbruch –, die einen „Reset“ des Systems ermöglichen, der häufig von einem massiven Transfer von Wohlstand nach oben begleitet wird. In den letzten Jahrzehnten sind solchen Ereignissen oft Simulationen vorausgegangen, die sich häufen, bevor genau das Ereignis eintritt, das sie „verhindern“ sollten. Jüngste Beispiele sind die US-Wahl 2020 und COVID-19. (...) Die aktuelle Agenda des Forums und seine bisherige Erfolgsbilanz bei der Ausrichtung

prophetischer Simulationen verlangen, dass die Übung [Cyber Polygon 2021] genau unter die Lupe genommen wird.“

Die WEF-Warnungen vor den Folgen einer weltweiten Cyber-Attacke klingen fast genau wie die WEF-Warnungen (beim Planspiel *Event 201* im Oktober 2019) vor einer weltweiten Pandemie, schreiben Vedmore und Webb. Auch die Lösungsvorschläge des WEF klingen identisch. Vor allem der Ruf nach einer verstärkten „public-private partnership“ sticht immer wieder hervor. Letztlich ein wohlklingender Begriff für die zunehmende Verschmelzung von staatlichen Einrichtungen und privaten Konzernen – also einer Monopolisierung von Macht, Kapital und Durchgriffsrechten.

Pandemie-Framing

Auch das Vokabular, das Klaus Schwab und andere an Cyber Polygon beteiligte Akteure, im Zusammenhang mit einem großen Cyberangriff benutzen, erinnert an Corona und zeigt geradezu penetrant, wie das WEF das ganze Thema interpretiert sehen will. Seit 2020 sprechen die Organisatoren wortwörtlich von einer bevorstehenden „Cyber-Pandemie“. Das mittlerweile erfolgreich in die Umgangssprache integrierte Corona-Vokabular wird von den Übungsveranstaltern gezielt verwendet, beide Ereignisse („Corona-Pandemie“ und „Cyber-Pandemie“) immer wieder gleichgesetzt.

Ein gezielt eingesetztes „Virus“ oder andere Schadprogramme könnten immer mehr Rechner „infizieren“. WEF-Business-Chef Jeremy Jurgens spricht in dem Zusammenhang von „exponentiellem Wachstum“. Das WEF [wirbt](#) bei Unternehmen dafür, ihre Firmen gegen eine Cyber-Pandemie zu „impfen“ und für „Cyber-Hygiene“ zu sorgen. Auch von „Wellen“ ist die Rede. [In einem Video](#) von Anfang 2021 spricht das WEF von einer „Cyberattacke mit covid-ähnlichen Eigenschaften“.

Das Framing trägt Früchte: Im Dezember 2020 bezeichneten mehrere Medien – [so etwa die Süddeutsche Zeitung](#) – den Lieferkettenangriff auf die US-Firma Solarwinds als „Angriff mit dem Superspreader“.

Ermöglicht das Planspiel späteres Hacking der Teilnehmer?

Beide Stränge von Cyber Polygon – das Hacking-Manöver und die Eliten-Statements – geben Anlass zur Sorge. Wie eine militärische Übung könnte auch

Cyber Polygon 2021 als Tarnung oder Sprungbrett für einen echten Angriff verwendet werden. Tatsächlich sind Teile der IT-Sicherheitsteams zahlreicher Unternehmen an diesem Tag in der Abwehrübung gebunden und geben für informierte Fachleute erkennbar ihre Fähigkeiten und Verteidigungsstrategien preis. Interessierte Akteure können hieraus Rückschlüsse auf deren Kompetenzen und Verhaltensweisen bei realen Cyber-Angriffen ziehen. Johnny Vedmore und Whitney Webb merken an,

„dass das Wissen, das BI.ZONE durch Cyberdefense-Training über die Schwachstellen globaler Institutionen erlangt hat, eine nützliche Information für die Muttergesellschaft, die Sberbank, und damit für den größten Aktionär der Sberbank, die russische Regierung, sein könnte.“

Die Leistungen der einzelnen Teams werden anhand eines festgelegten Punktekatalogs bewertet und anschließend verglichen. Cyber Polygon bietet demnach einen Spiel- und Wettbewerbscharakter für die teilnehmenden IT-Profis. Diese „Gamification“ der Übung sollte kritische Beobachter aufhorchen lassen. Dienen solche Wettbewerbsanreize in der modernen Informationstechnologie doch vor allem als Köder, um bei Betroffenen bestimmte Verhaltensweisen und Informationen zum Vorschein zu bringen.

Agenda-Setting der Superreichen

Auf eine andere Art bedrohlich ist die politische Themensetzung, die das WEF mit der Veranstaltung inhaltlich betreibt. Nach der großen Pandemie wird von Klaus Schwab und Co. hier die nächste globale Bedrohung öffentlich als solche definiert, präsentiert und mental verankert. Dazu wird auch immer wieder der aus Sicht des WEF richtige politische Umgang mit einem großen Hacker-Angriff erklärt. Die hunderten hochrangigen Teilnehmer von Cyber Polygon sind damit nicht nur Sender, sondern auch Empfänger der WEF-Botschaften.

Sobald die angekündigte globale Cyber-Attacke tatsächlich kommt, wissen alle schon, was nun zu tun ist. Ähnlich funktionierte dies mit der vor 2020 in Planspielen immer wiederholten Botschaft, dass nur die Impfung eine Pandemie beenden könne. Seit die Corona-Krise Anfang 2020 ihren Lauf nahm, werden gar keine anderen Lösungsansätze mehr diskutiert als die „Impfung“ der Weltbevölkerung.

Klaus Schwab [bezeichnete](#) die Corona-„Pandemie“ als Ereignis mit „katalytischem

Effekt“, weil es die Digitalisierung so dermaßen beschleunigt habe. „In ein paar Monaten haben wir solche Fortschritte in der digitalen Transformation gemacht, die sonst zwei, drei oder noch mehr Jahre gedauert hätten“, [sagte](#) er bei Cyber Polygon 2020.

Damit entsteht die interessante Situation, dass das WEF genau die katastrophalen Ereignisse, vor denen es im Vorhinein „warnt“, tatsächlich sehr befürworten müsste, da seine politisch-ökonomischen Vorstellungen dadurch umso schneller und nahezu widerstandslos umgesetzt werden können. Umso besser, wenn die Umbaupläne schon in der Schublade liegen. Vedmore und Webb schreiben:

„Sollten die bei Cyber Polygon simulierten destabilisierenden Ereignisse tatsächlich eintreten, wird dies vom WEF wahrscheinlich ähnlich begrüßt werden, da ein kritisches Versagen des derzeitigen globalen Finanzsystems die Einführung neuer öffentlich-privater „digitaler Ökosystem“-Monopole ermöglichen würde, wie sie in Russland von der Sberbank aufgebaut werden.“

(...)

Der erwartete Zusammenbruch des internationalen Finanzsystems und die Einführung digitaler Währungen könnten mit einem anonymen Hackerangriff ideal begründet werden, vermuten Vedmore und Webb. Wahrscheinlich werde der Kollaps kontrolliert durchgeführt, damit die Machteliten ihre Macht auch behalten. Anonyme Hacker seien hierbei ideale Täter, nicht nur weil die Superreichen, die unter anderem im WEF organisiert sind, so ihre Verantwortung für den Zusammenbruch des Finanzsystems weit von sich weisen könnten. Sondern auch, weil jedes mögliche Feindbild damit bedient werden könnte: von Nordkorea über Iran bis hin zu sogenannten inländischen Terroristen, schreiben die beiden Autoren von *Unlimited Hangout*.

(...)

Letztlich bauen die Botschaften des WEF aufeinander auf. Erstens: Corona erzwingt global-einheitliche Reaktionsweisen und die umfassende Digitalisierung des Lebens. Zweitens: Drohende Cyber-Angriffe erforderten die Einrichtung einer gemeinsamen globalen Sicherheitsarchitektur von Staaten und Konzernen. Und da in der digitalen Welt prinzipiell alles hackbar ist, wie die Firma BI.Zone [in diesem Video](#) selbst darlegt, müssten die Zugriffsrechte der Sicherheitsdienste maximal,

umfassend und tiefgehend sein.

Die gesamte Krise könnte nicht nur dazu benutzt werden, Zugriffsrechte von Staaten und Unternehmen [auszuweiten](#) sowie digitale Zentralbankwährungen einzuführen, sondern auch die verpflichtende digitale biometrische Identität (ID) durchzusetzen, für die der britische Ex-Premier Tony Blair bei Cyber Polygon 2020 geworben hat. Auch digitale Impfpässe könnten integriert werden. Tony Blair sagte, die Einführung einer digitalen ID sei unvermeidbar. [„Absolut unvermeidbar!“](#)

Unvermeidbar war bei Cyber Polygon 2020 eines der entscheidenden Wörter, das immer wieder fiel. Die ständig voranschreitende Digitalisierung sei unvermeidbar, die globale Krise sei unvermeidbar, ein großer Cyberangriff sei unvermeidbar. Die Verwendung des Begriffs gehört zu den verschleiernenden Hauptstrategien der Einpeitscher des modernen Überwachungskapitalismus, stellte die Ökonomin Shoshana Zuboff in ihrem [aktuellen Buch zum Thema](#) (Seite 260) fest:

„Das Bild von Technologie als autonomer Kraft, deren Handlungen und Folgen unvermeidbar seien, wird seit Jahrhunderten dazu eingesetzt, die Fingerabdrücke der Macht zu verwischen und sie von jeder Verantwortung zu befreien. Das Monster war's, nicht Victor Frankenstein.“

Den äußerst lesenswerten Artikel von Stefan Korinth [finden Sie hier...](#)

Aus Anlegersicht ist an dieser Stelle noch der folgende Aspekt von Interesse: Das WEF-Planspiel 201 vom Herbst 2019, das auf geheimnisvolle Weise eine Art „Blaupause“ für die aktuelle Corona-Krise geliefert hatte, fand sich ziemlich genau **drei Monate später** in der Realität wieder.

Würde dieser „Zeitplan“ auch bei Cyber Polygon vom Sommer 2021 eingehalten, könnte es drei Monate nach dem Veranstaltungstermin 9. und 10. Juli in den Börsensälen ungemütlich werden. Womöglich nach einem „Cyber-Angriff“ auf die globale Finanzarchitektur?

Das wäre ganz grob der Zeitraum um Mitte Oktober. Da war doch mal was? Richtig: Das wäre ziemlich genau jene angstbesetzte Periode im Verlauf eines Börsenjahres, die in der Finanzgeschichte mit historischen Turbulenzen zu zweifelhaftem Ruhm gekommen ist:

Der Jahrhundertcrash von 1929 mit der darauffolgenden

Weltwirtschaftskrise begann am Donnerstag, 24. Oktober - und der größte Tagesverlust aller Zeiten beim Dow Jones wurde am 19. Oktober 1987 verzeichnet...

Passt doch irgendwie wie die Faust aufs Auge...

Mehr dazu in der kommenden Ausgabe des Antizyklischen Börsenbriefs...