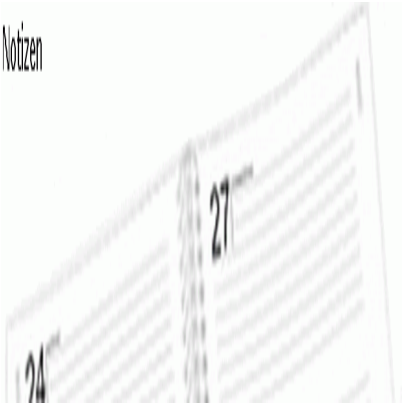

Cyber-Attacke auf Finanzsystem?

Description

Vor einigen Tagen hat die größte Organisation für den Informationsaustausch in der Finanzindustrie, das Financial Services Information Sharing and Analysis Center (FS-ISAC), erneut gewarnt, dass nationalstaatliche Hacker und Cyberkriminelle zusammenarbeiten, um das globale Finanzsystem in Kürze anzugreifen. Zu den bekannten Mitgliedern der Organisation gehören die Bank of America, Wells Fargo und die CitiGroup.

Die Cyber Policy Initiative von WEF (World Economic Forum) und Carnegie Endowment for International Peace warnte im November 2020, das globale Finanzsystem sei zunehmend anfällig für Cyberangriffe. Sie fordert in ihrem Bericht „International Strategy to Better Protect the Financial System" den engen Zusammenschluss von Wall-Street-Banken, ihren Regulierungsbehörden und Geheimdiensten. Ein angeblich drohender Cyberangriff könnte das bestehende Finanzsystem zum Einsturz bringen. Eines sei klar, heißt es: „Es ist nicht die Frage, ob ein größerer Vorfall passieren wird, sondern wann."

Der Bericht fordert außerdem, dass Social-Media-Unternehmen mit den Zentralbanken zusammenarbeiten, um „Eskalationspfade zu entwickeln, die denen ähnlich sind, die im Zuge der vergangenen Wahlbeeinflussung entwickelt wurden, wie sie in den USA und Europa zu beobachten waren." Diese „Eskalationspfade" bedeuten eine weitreichende Zensur der sozialen Medien, es heißt, dass „eine schnelle Koordination mit Social-Media-Plattformen notwendig ist, um die Löschung von Inhalten zu organisieren." In diesem Zusammenhang schließt der Bericht auch ein die Verbreitung „falscher Informationen, die sich nicht direkt auf die Finanzmärkte beziehen, aber die Finanzmärkte zu Reaktionen veranlassen." Solche sei besonders während einer größeren Finanzkrise wahrscheinlich, um schädliche Narrative zu verstärken. Mit dieser Handhabung kann jede wahre Nachricht unterdrückt werden, wenn sie als destabilisierend eingestuft wird.

Der beunruhigendste Teil des Berichts ist die Aufforderung, die Zusammenarbeit des nationalen Sicherheitsapparats mit der Finanzindustrie als Modell zu nutzen, um das Gleiche in anderen Sektoren der Wirtschaft zu tun. Wird das umgesetzt, würde es keinen Teil des täglichen menschlichen Lebens mehr geben, der unkontrolliert bliebe – ein klares Rezept für Techno-Faschismus in globalem Maßstab.

Zu den Beratern des WEF-Carnegie-Projekts gehören Vertreter der Fed, der EZB, der Bank of England, des IWF, SWIFT, Wall-Street-Giganten wie Bank of America und JP Morgan Chase und Unternehmensgiganten wie Amazon und Accenture, Strafverfolgungs-Behörden wie INTERPOL und der US-Geheimdienst, aber eben auch der CEO des Financial Services Information Sharing and Analysis

Center (FS-ISAC), Steve Silberstein.

Die Carnegie Endowment for International Peace, ist eine der einflussreichsten außenpolitischen Denkfabriken in den Vereinigten Staaten. Er verfügt über enge und anhaltende Verbindungen zum US-Außenministerium, ehemaligen Präsidenten, Corporate America und amerikanischen Oligarchenclans. Zu den aktuellen Kuratoren der Stiftung gehören Führungskräfte der Bank of America und der CitiGroup sowie anderer einflussreicher Finanzinstitute.

Einige Monate vor Herausgabe des Berichts hatte das WEF eine Simulation genau zu einem Cyberangriff durchgeführt, der das globale Finanzsystem in die Knie zwingt – interessanterweise in Zusammenarbeit mit Russlands größter Bank, der Sberbank. Diese soll die wirtschaftliche „digitale Transformation" des Landes mit der Einführung einer eigenen, Zentralbank-gestützten Kryptowährung ankurbeln.

Solche koordinierten Simulationen und Warnungen von denjenigen, die das derzeitige, kränkelnde Finanzsystem beherrschen, machen hellhörig. Schließlich ist das WEF für seine Simulation Event 201 hinsichtlich einer globalen Coronavirus-Pandemie bekannt, die nur wenige Monate, im Oktober 2019, vor Ausbruch von COVID-19 stattfand.

Seitdem dient COVID-19 als Hauptbegründung für die Beschleunigung der „digitalen Transformation" des Finanz-Sektors. Experten warnen seit der Finanzkrise 2008 vor einem Zusammenbruch des Finanzsystems, das durch die Misswirtschaft der Geldflut der Zentralbanken und der zügellosen Kasinomentalität an Wall Street und anderswo extrem instabil ist. Ein Cyberangriff, der den Zusammenbruch des derzeitigen, fragilen Finanzsystem herbeiführt, böte das perfekte Szenario für die Demontage des aktuellen, nicht überlebensfähigen Geldsystems, da es die Zentralbanken und Finanzinstitutionen von jeglicher Verantwortung freisprechen würde.

Hier drängen sich weitere Parallelen zur Corona-„Pandemie“ auf. „Corona“ lieferte den perfekten Anlass für die Zentralbanken, ihre Geldschleusen aufzureißen, ohne dass der Verdacht aufkam, dass das Finanzsystem erneut am Abgrund stand. Dabei gab es spätestens seit Herbst 2019 entsprechende Anzeichen (link). Genauso verhielt es sich mit der Realwirtschaft, die am Ende ihrer Expansion angekommen war. Seinerzeit, im Februar 2020 stand fest: „Die Großspekulation braucht frisches Geld, die Realwirtschaft braucht ein Konjunkturprogramm.“

WEF und Big Tech unterstützen die Vaccine-Credential-Initiative mit biometrischen IDs und so genannten „Impfpässen" (ID2020). ID2020, eine öffentlich-private Partnerschaft, ist ein elektronisches ID-Programm, das Impfungen als Plattform für die digitale Identität nutzt. Es ist eine breit angelegte Allianz, UN-Organisationen sind dabei, auch die Impforganisation des Gates-Stiftung, die Global Alliance for Vaccines and Immunization. GAVI wird von der WHO unterstützt, und damit von ihren Sponsoren aus der Pharmaindustrie. Mit dabei, natürlich, auch das WEF. Der Feldtest findet momentan in Bangladesch statt.

Ein Cyberangriff auf den Finanzsektor mit der Reaktion der Einführung eines neuen Geldsystems könnte in einem Zuge auch die Zusammenführung mit Credential-Systemen befördern und das Ergebnis dadurch Akzeptanz verschaffen, dass es als „Ausweg" aus allen COVID-19-bezogenen Beschränkungen propagiert wird. Gesundheits- und Finanzdaten über eine Quelle erreich- und vermarktbar? Traumhaft!

[Unter Verwendung von Material aus dieser Quelle]

Ergänzung:
Der deutsche Bundestag hat am 29. Januar die Implementation der Agenda ID2020 ratifiziert.

Nachtrag:
Das WEF hat für den 9. Juli 2021 eine weitere Trainingsübung hinsichtlich einer weltweiten Cyber-Attacke angesetzt, das Event trägt den Namen „Cyber Polygon 2021“. Dabei soll ein Cyberangriff auf die

Lieferkette eines Unternehmens simuliert werden, die Teilnehmer sollen darauf in Echtzeit reagieren.