https://unlimitedhangout.com/2021/04/investigative-reports/wef-warns-of-cyber-attack-leading-to-systemic-collapse-of-the-global-financial-system/

18- CYBER ATTACK WILL COLLAPSE GLOBAL FINANCIAL SYSTEM

Whitney Webb
April 9, 2021

A report published last year by the WEF-Carnegie Cyber Policy Initiative calls for the merging of Wall Street banks, their regulators and intelligence agencies as necessary to confront an allegedly imminent cyber attack that will collapse the existing financial system.

Originally published at The Last American Vagabond.

In November 2020, the World Economic Forum and Carnegie Endowment for International Peace coproduced a report that warned that the global financial system was increasingly vulnerable to cyberattacks. Advisers to the group that produced the report included representatives from the Federal Reserve, the Bank of England, the International Monetary Fund, Wall Street giants such as JPMorgan Chase, and Silicon Valley behemoths such as Amazon.

The ominous report was published just months after the World Economic Forum had conducted a simulation of just such an event—a cyberattack that brings the global financial system to its knees—in partnership with Russia's largest bank, which is due to jumpstart that country's economic transformation by launching its own central bank–backed digital currency.

As recently as last Tuesday, the largest information-sharing organization of the financial industry, the Financial Services Information Sharing and Analysis Center (FS-ISAC), whose known members include the Bank of America, Wells Fargo, and Citigroup, warned that nation-state hackers and cybercriminals are poised to jointly attack the global financial system. The CEO of this organization had previously given the same warning, which was published in the World Economic Forum-Carnegie Endowment (WEF-Carnegie) report.

Such coordinated simulations and warnings from those who dominate the current ailing financial system are obviously a cause for concern, particularly given that the World Economic Forum is well-known for its Event 201 simulation about a global coronavirus pandemic that took place just months prior to the COVID-19 crisis.

The COVID-19 crisis has since been cited as the main justification for accelerating what is termed the digital transformation of the financial sector and other sectors, which that the World Economic Forum and its partners have promoted for years. Their latest prediction of a doomsday event, a cyberattack that stops the current financial system in its tracks and initiates its systemic collapse, if it came to pass, would be the final, necessary step required to bring about the Forum's desired outcome of a widespread shift to digital currency and increased global governance of the international economy.

Given that experts have been warning since the last global financial crisis that the collapse of the entire system was inevitable due to central bank mismanagement and rampant Wall Street corruption, a cyberattack would also provide the perfect scenario for dismantling the current failing system, as it would absolve central banks and corrupt financial institutions of any responsibility. It would also provide a justification for incredibly troubling policies promoted in the WEF-Carnegie report, such as a greater fusion of intelligence agencies and banks in order to better "protect" critical financial infrastructure.

Considering the precedent of the WEF's past simulations and reports with the COVID-19 crisis, it is well worth examining all their simulations, warnings, and desired policies. The remainder of this article will examine the November 2020 WEF-Carnegie report from. A follow-up article will focus on the FS-ISAC report published last week. The World Economic Forum's simulation of a cyberattack on the global financial system, Cyber Polygon 2020, was covered in detail by Unlimited Hangout in a previous article.

The WEF-Carnegie Cyber Policy Initiative

The Carnegie Endowment for International Peace is one of the most influential foreign policy think tanks in the United States, with close and persistent ties to the US State Department, former US presidents, corporate America, and American oligarch clans suchas the Pritzkers of Hyatt hotels. Current trustees of the endowment include executives from Bank of America and Citigroup as well as other influential financial institutions.

In 2019, the same year as Event 201, the Carnegie Endowment launched its Cyber Policy Initiative with the goal of producing an "international strategy for cybersecurity and the global financial system 2021–2024." That strategy was released just months ago, in November 2020, and, according to the Carnegie Endowment, it was authored by "leading experts in governments, central banks, industry and the technical community" in order to provide a "longer-term international cybersecurity strategy" specifically for the financial system.

The initiative is an outgrowth of past efforts of the Carnegie Endowment to promote the fusion of financial authorities, the financial industry, law enforcement, and national security agencies, which is both a major recommendation of the November 2020 report and a conclusion of a 2019 "high-level roundtable" between the endowment, the IMF, and central bank governors. The endowment had also partnered with the IMF, SWIFT, Standard Chartered, and the FS-ISAC to create a "cyber resilience capacity-building tool box" for financial institutions in 2019. That same year, the endowment also began tracking "the evolution of the cyber threat landscape and incidents involving financial institutions" in collaboration with BAE Systems, the UK's largest weapons manufacturer. Per the Carnegie Endowment, this collaboration continues into the present.

In January 2020, representatives of the Carnegie Endowment presented their Cyber Policy Initiative at the annual meeting of the World Economic Forum, after which the Forum officially partnered with the endowment on the initiative.

Advisers to the now-joint WEF-Carnegie project include representatives of central banks including the US Federal Reserve and the European Central Bank; some of Wall Street's most infamous banks such as Bank of America and JPMorgan Chase; law enforcement organizations such as INTERPOL and the US Secret Service; corporate giants such as Amazon and Accenture; and global financial institutions including the International Monetary Fund and SWIFT (the Society for Worldwide Interbank Financial Telecommunication). Other notable advisers include the managing director and head of the WEF's Centre for Cybersecurity, Jeremy Jurgens, who was also a key player in the Cyber Polygon simulation, and Steve Silberstein, the CEO of the Financial Services Information Sharing and Analysis Center.

Not a Question of If but When

The Cyber Policy Initiative's November 2020 report is officially titled International Strategy to Better Protect the Financial System. It begins by noting that the global financial system, like many other systems, is "going through unprecedented digital transformation, which is being accelerated by the coronavirus pandemic."

It then warns:

"Malicious actors are taking advantage of this digital transformation and pose a growing threat to the global financial system, financial stability, and confidence in the integrity of the financial system. Malign actors are using cyber capabilities to steal from, disrupt, or otherwise threaten financial institutions, investors and the public. These actors include not only increasingly daring criminals, but also states and state-sponsored attackers."

Following this warning of "malign actors," the report adds that "increasingly concerned, key voices are sounding the alarm." It notes that Christine Lagarde of the European Central Bank and formerly of the IMF warned in February 2020 that "a cyber attack could trigger a serious financial crisis." A year prior, at the WEF's annual meeting, the head of Japan's central bank predicted that "cybersecurity could become the financial system's most serious risk in the near future." It also notes that in 2019, Jamie Dimon chairman and CEO of JPMorgan Chase similarly labeled cyberattacks as possibly "the biggest threat to the US financial system."

Not long after Lagarde's warning in April 2020, the Bank for International Settlements' Financial Stability Board asserted that "cyber incidents pose a threat to the stability of the global financial system" and that "a major cyber incident, if not properly contained, could seriously disrupt financial systems, including critical financial infrastructure, leading to broader financial stability implications."

The WEF-Carnegie report authors add to these concerns that "the exploitation of cyber vulnerabilities could cause losses to investors and the general public" and lead to significant damage to public trust and confidence in the current financial system. It also notes, aside from affecting the general public in a significant way, this threat would impact both high-income countries and low to lower-middle income countries, meaning the impact on the masses would be global in scope.

The report then ominously concludes that "one thing is clear: it is not a question of if a major incident will happen, but when."

Ensuring Control of the Narrative

Another section of the report details recommendations for controlling the narrative in the event such a crippling cyberattack takes place. The report specifically recommends that "financial authorities and industry should ensure they are properly prepared for influence operations and hybrid attacks that combine influence operations with malicious hacking activity" and that they "apply lessons learned from influence operations targeting electoral processes to potential attacks on financial institutions."

It goes on to recommend that "major financial services firms, central banks and other financial supervisory authorities," representatives of which provided advice for the WEF-Carnegie report, "identify a single point of contact within each organisation to engage social media platforms for crisis management."

The report's authors argue that, "in the event of a crisis," such as a devastating cyberattack on the global banking system, "social media companies should swiftly amplify communications by central banks" so that central banks may "debunk fake information" and "calm the markets." It also states that "financial authorities, financial services firms and tech companies [presumably including social media companies] should develop a clear communications and response plan focused on being able to react swiftly." Notably, both Facebook and Twitter are listed in the report's appendix as "industry stakeholders" that have "engaged" with the WEF-Carnegie initiative.

The report also asserts that premeditated coordination for such a crisis between banks and social media companies needs to take place so that both stakeholders may "determine what severity of crisis would necessitate amplified communication." The report also calls for social media companies to work with central banks to "develop escalation paths similar to those developed in the wake of the past election interference, as seen in the United States and Europe."

Of course, those "escalation paths" involved wide-ranging social media censorship. The report seems to acknowledge this when it adds that "quick coordination with social media platforms is necessary to organize content takedowns." Thus, the report is calling for central banks to collude with social media platforms to plan out censorship efforts that would be enacted if a sufficiently severe crisis occurs in financial markets.

As for "influence operations," the report divides these into two categories: those that target individual firms and those that target markets overall. Regarding the first category, the report states that "organized actors will spread fraudulent rumors to manipulate stock prices and generate profit based on how much the price of the stock was artificially moved." It adds that, in these influence operations, "firms and lobbyists use astroturfing campaigns, which create a false appearance of grassroots support, to tarnish the value of a competing brand or attempt to sway policymaking decisions by abusing calls for online public comments." The similarities between this latter statement and the WallStreetBets phenomenon of

January 2021 are obvious.

Regarding the second category of "influence operations," the report defines these operations as "likely to be carried out by a politically motivated actor like a terrorist group or even a nation-state." It adds that "this type of influence operation may directly target the financial system to manipulate markets, for example, by spreading rumors about market-moving decisions by central banks" as well as spreading "false information that does not directly reference financial markets but that causes financial markets to react."

Given that the report states that the first category of influence operation poses little systemic risk while the second "may pose systemic risk," it seems likely that the event being predicted by the WEF-Carnegie report would involve claims of the latter by a "terrorist group" or "nation-state." Notably, the report on several occasions mentions North Korea as a likely nation-state offender. It also dwells on the likelihood that synthetic media or deepfakes would be part of this system-devastating event in emerging economies and/or in high-income countries experiencing a financial crisis.

A separate June 2020 report from the WEF-Carnegie initiative was published specifically on the subject of deepfakes and the financial system, noting that such attacks would likely transpire during a larger financial crisis to "amplify" damaging narratives or "simulate grassroots consumer backlash against a targeted brand." It adds that "companies, financial institutions and government regulators facing public relations crises are especially vulnerable to deepfakes and synthetic media."

In light of these statements, it is worth pointing out that bad actors within the current system could exploit these scenarios and theories to paint genuine grassroots backlash against a bank or corporation as being a synthetic "influence operation" perpetrated by "cybercriminals" or a nation-state. Considering that the WEF-Carnegie report references a scenario analogous to the WallStreetBets situation in January 2021, a banker-led effort to falsely label a future grassroots backlash as being synthetic and the fault of a "terrorist group" or nation-state should not be ruled out.

"Reducing Fragmentation": Merging Banks with Their Regulators and Intelligence Agencies

Given the inevitability of this destructive event, as predicted by the WEF-Carnegie report's authors, it is important to focus in on the solutions proposed in the report, as they will become immediately relevant when this event does come to pass.

Some of the solutions proposed are to be expected from a WEF-linked policy document, such as increased public-private partnerships and greater coordination among regional and international organizations as well as increased coordination among national governments.

However, the main "solution" at the heart of this report, and also at the heart of the WEF-Carnegie initiative's other endeavors, is the fusing of corporate banks, the financial authorities that oversee them, tech companies, and the national-security state.

The report's authors argue that the main vulnerability of the global financial system at present is "the current fragmentation among stakeholders and initiatives" and that mitigating this threat to the global system lies in reducing that "fragmentation." The authors argue that the way to resolve the issue requires the massive reorganization of all "stakeholders" via increased global coordination. The report notes that the "disconnect between the finance, the national security and the diplomatic communities is particularly pronounced" and calls for much closer interaction between the three.

It then states:

"This requires countries not only to better organize themselves domestically but also to strengthen international cooperation to defend against, investigate, prosecute and ideally prevent future attacks. This implies that the financial sector and financial authorities must regularly interact with law enforcement and other national security agencies in unprecedented ways, both domestically and internationally."

Some examples of these needed "unprecedented" interactions between banks and the national-security state are included in the report's recommendations. For instance, the report states that "governments should use the unique capabilities of their national security communities to help protect FMIs [financial market infrastructures] and critical trading systems." It also calls for "national security agencies [to] consult critical cloud service providers [like WEF-Carnegie Cyber Policy Initiative partner Amazon Web Services] to determine how intelligence collection could be used to help identify and monitor potential significant threat actors and develop a mechanism to share information about imminent threats" with tech companies.

The report also states that "the financial industry should throw its weight behind efforts to tackle cyber crime more effectively, for example by increasing its participation in law enforcement efforts."

On this last point, there are indications that this has already begun. For instance, Bank of America, the second largest bank in the US and part of the WEF-Carnegie Cyber Policy Initiative and FS-ISAC, was reported to have "actively but secretly engaged" with US law enforcement agencies in the hunt for "political extremists" following the January 6th events at Capitol Hill. In doing so, Bank of America shared private information with the federal government without the knowledge or consent of its customers, leading critics to accuse the bank of "effectively acting as an intelligence agency."

Arguably the most troubling part of the report, however, is its call to unite the national-security apparatus and the finance industry and then use that as a model to do the same with other sectors of the economy. It states that "protecting the international financial system can be a model for other sectors," adding that "focusing on the financial sector provides a starting point and could pave the way to better protect other sectors in the future."

Were all sectors of the economy to fuse with the national-security state, it would create a reality in which no part of daily human life is not controlled

by these two already very powerful entities. This is a clear plan for creating techno-fascism on a global scale. As this WEF-Carnegie report makes clear, the recipe regarding how to cook up such a nightmare has already been charted out in coordination with the very institutions, banks, and governments that currently control the global financial system.

Not only is global corporate control a goal, but—as pointed out in Unlimited Hangout's article on Cyber Polygon—the World Economic Forum and many of its partners actually have a vested interest in the systemic collapse of the current financial system. In addition, many central banks have recently proposed digital currency systems that can only achieve rapid mass adoption if the existing system collapses.

Given that these systems are set to be integrated with biometric IDs and so-called vaccine passports through the WEF and the Big Tech–backed Vaccine Credential Initiative, it is worth considering the timing of the expected launch of such systems in determining when this predicted and allegedly inevitable event is likely to occur.

With this new financial system so deeply interconnected with so-called credential efforts, the envisioned cyberattack on the financial sector would likely take place at a time when it would best facilitate the adoption of the new economic system and its integration into credential systems currently being promoted as a way out of COVID-19–related restrictions.