GlobalResearch
Center for Research on Globalization

World Economic Forum (WEF) Warns of Cyberattack Leading to Systemic Collapse of the Global Financial System

By Whitney Webb

Theme: Global Economy, Intelligence

Global Research, September 03, 2021
The Last American Vagabond 7 April 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.

In November 2020, the World Economic Forum (WEF) and Carnegie Endowment for International Peace co-produced a report that warned that the global financial system was increasingly vulnerable to cyber attacks. Advisors to the group that produced the report included representatives from the Federal Reserve, the Bank of England, the International Monetary Fund, Wall Street giants likes JP Morgan Chase and Silicon Valley behemoths like Amazon.

The ominous report was published just months after the World Economic Forum had conducted a simulation of that very event – a cyber attack 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 "digital transformation" with the launch of its own central bank-backed digital currency.

More recently, last Tuesday, the largest information sharing organization of the financial industry, whose known members include Bank of America, Wells Fargo and CitiGroup, have again warned that nation-state hackers and cybercriminals were poised to work together to attack the global financial system in the short term. The CEO of this organization, known as the Financial Services Information Sharing and Analysis Center (FS-ISAC), had previously advised the WEF-Carnegie report that had warned much the same.

Such coordinated simulations and warnings from those who dominate the current, ailing financial system are obvious 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 the "digital transformation" of the financial and other sectors that the Forum and its partners have promoted for years. Their latest prediction of a doomsday event, a cyber attack that stops the current financial system in its tracks and instigates its systemic collapse, would offer the final yet necessary step for the Forum's desired outcome of this 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 cyber attack 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 by 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 the simulations, warnings and the policies promoted by these powerful organizations. The remainder of this report will examine the WEF-Carnegie report from November 2020, while a follow-up report will focus on the more recent FS-ISAC report published last week. The WEF simulation of a cyber attack on the global financial system, Cyber Polygon 2020, was covered in detail by Unlimited Hangout in a previous report.

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 Presidents, corporate America and American oligarch clans like 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 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 Endowment, 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 fo 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 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 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.

Advisors to the now joint WEF-Carnegie project include representatives of central banks like the US Federal Reserve and the European Central Bank; some of Wall Street's most infamous banks like Bank of America and JP Morgan Chase; law enforcement organizations such as INTERPOL and the US Secret Service; corporate giants like Amazon and Accenture; and global financial institutions like the International Monetary Fund (IMF) and SWIFT. Other notable advisors 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 (FS-ISAC).

"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, are "going through unprecedented digital transformation, which is being accelerated by the coronavirus pandemic."

It then warns that:

> "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."

Followed by this warning of "malign actors", the report notes 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 of JP Morgan Chase similarly labeled cyber attacks as possibly "the biggest threat to the US financial system."

Not long after Lagarde's warning, in April 2020, the 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 its impact on the masses will 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 cyber attack 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 advised 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 cyber attack 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 parties 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 organise 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 far as "influence operations" go, 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 "organised actors will spread fraudulent rumours to manipulate stock prices and generate profit based on how much the price of the stock was artificially moved." It then 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 Wall Street Bets 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 rumours 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 more likely that the event being predicted by the WEF-Carnegie report would involve claims of the latter by a "terrorist group" or potentially a nation-state. Notably, the report mentions North Korea as a likely nation-state offender on several occasions. It also dwells on the likelihood that synthetic media or "deep fakes" 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 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 actual 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 Wall Street Bets situation in January 2021, a banker-led effort to falsely label a future grassroots backlash as instead 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 predicted by the report's authors, it is important to focus in on the solutions proposed in the WEF-Carnegie report as they will become immediately relevant if this event, as predicted by the WEF and Carnegie Endowment, does come to pass.

Some of the solutions proposed are to be expected from a WEF-linked policy document, such as the calls for increased public-private partnerships and greater coordination among regional and international organizations as well as increased coordination between 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 a call to fuse corporate banks, the financial authorities that essentially oversee them, tech companies and the national security state.

The report's authors first 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 global system lies in reducing that "fragmentation." The report argues that the way to resolve the issue requires massive re-organization 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 that:

> "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 "unprecedented interactions" between banks and the national security state are included in the report's recommendations. For instance, it argues 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 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 that last point, there are indications this has already begun. For instance, Bank of America, the second largest bank in the US and part of the WEF-Carnegie 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."

Yet, arguably the most troubling part of the report is its call to unite the national security apparatus and the finance industry first, 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 the sectors of the economy to also fuse with the national security state, it would inevitably create a reality where there is no part of daily human life that is not ultimately controlled by these two already very powerful entities. This is a clear recipe for techno-fascism on a global scale. As this WEF-Carnegie report makes clear, the roadmap 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 that, but – as pointed out in *Unlimited Hangout*'s article on Cyber Polygon – the World Economic Forum and many of its partners have a vested interest in the systemic collapse of the current financial system. In addition, many central banks have recently backed new 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 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 inter-connected to these “credential” efforts, this cyber attack 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.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, @crg_globalresearch. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Whitney Webb has been a professional writer, researcher and journalist since 2016. She has written for several websites and, from 2017 to 2020, was a staff writer and senior investigative reporter for Mint Press News. She currently writes for The Last American Vagabond.

Featured image is from The Last American Vagabond
