MERCOLA
Take Control of Your Health

What's the End Game for Cybercrimes and Ransomware Attacks?

Analysis by Dr. Joseph Mercola ✔ Fact Checked | August 16, 2023

STORY AT-A-GLANCE

- Over the past few years, a number of organizations have warned that the world is facing growing danger from hackers and cybercriminals, and could be facing a cyberattack large enough to take down our society as a whole
- In June 2020, the World Economic Forum (WEF) warned that the world must prepare for an "inevitable global cyberattack," a "COVID-like global cyber pandemic that will spread faster and further than a biological virus, with an equal or greater economic impact"
- In December 2021, a 10-nation exercise simulated a scenario in which a cyberattack brought down the financial system worldwide. Responses and solutions included emergency liquidity assistance to banks, a globally coordinated bank holiday (bank closure), debt repayment grace periods, and a "coordinated delinking from major currencies," meaning bank balances in USD, GBP and EUR were eliminated and replaced with a central bank digital currency (CBDC). In case of a real cyberattack on the financial system, we can therefore expect this to happen
- At the end of 2020, hackers accessed the SolarWinds supply chain by delivering a backdoor malware through an infected SolarWind Orion software update. The malware infected the networks, systems and data of more than 30,000 public and private organizations, including local, state and federal agencies. It's thought to be the largest and most devastating cyber breach to date
- The end game of all these organized cyberthreats is to eliminate anonymity on the web under the auspices of "preventing cybercrime," and to impose extreme centralization of the internet for the purpose of information control

Over the past few years, several organizations have warned that the world is facing growing danger from hackers and cybercriminals and could be facing a cyberattack large enough to take down our society as a whole. An effective cyberattack could compromise any device and system connected to the internet, including but not limited to:

Life-saving medical devices	The internet of things (IoT) ecosystem (i.e., devices that run smart homes)
The internet of bodies (IoB) ecosystem	Global financial systems
Energy grids	Water treatment facilities
Government IT systems	Military and defense infrastructure

Warnings and Predictions of Internet Doom

In June 2020, the World Economic Forum warned[1] that the world must prepare for an "inevitable global cyberattack," a "COVID-like global cyber pandemic that will spread faster and further than a biological virus, with an equal or greater economic impact."

"Our 'new normal' isn't COVID-19 itself — it's COVID-like incidents. And a cyber pandemic is probably as inevitable as a future disease pandemic," the WEF said.

In November 2020, the WEF followed up with a report co-created with the Carnegie Endowment for International Peace, which warned that the global financial system is failing to keep up with the ever-growing list of cyberthreats and is ill-equipped to defend against large-scale cyberattacks.[2]

To address this problem, the report called for greater coordination between government and industry, and for nations to cooperate more directly and intimately, rather than drafting a new treaty on international cybercrime.

Similarly, in March 2021, the Financial Services Information Sharing and Analysis Center (FS-ISAC) predicted that a cyberattack on the global financial system is practically inevitable, with ransomware and other extortion attacks topping the list of hazards.[3,4]

Another major target for cybercriminals and ransomware hackers is the health care industry, which has seen the largest increase in attacks — about double that of other industries.[5]

What Simulations and Exercises Tell Us About the Plan

As in the biosecurity arena, a number of tabletop exercises have been held to simulate a massive cyberattack. One such exercise took place in early December 2021 in Israel.[6] The simulation was based on a scenario in which a cyberattack brought down the financial system worldwide.

Participants included treasury officials from Israel, the U.S., the U.K., United Arab Emirates, Austria, Switzerland, Germany, Italy, The Netherlands and Thailand, as well as representatives from the International Monetary Fund, the World Bank and the Bank of International Settlements (BIS).

Emergency responses presented during that exercise included emergency liquidity assistance to banks, a globally coordinated bank holiday (bank closure), debt repayment grace periods and SWAP/REPO agreements.

The response also included a "coordinated delinking from major currencies," meaning bank balances in USD, GBP and EUR were eliminated and replaced with a central bank digital currency (CBDC).[7]

So, in the case of a real cyberattack on the financial system, we can probably expect this swap to happen. It's also possible that if the rollout of CBDCs fails, a catastrophic systemic attack on the banking system could be used to force the issue.

At the time, former Pfizer executive Mike Yeadon, Ph.D., said he believed the simulation was a front for a planned financial reset in which most people will lose all their financial

assets, thereby bringing about the WEF's promise that you will "own nothing" by 2030.[8]

Preparing for a cyber pandemic more destructive than COVID also took place during the Cyber Polygon exercises of 2020 and 2021. This is yet another annual event staged by the WEF.

In 2020, the simulation involved a cyberattack against the global financial system.[9] The following year, participants simulated a targeted supply chain attack on a corporate ecosystem resulting in industry collapses, mass unemployment, widespread rioting and global lockdowns.[10,11] Solution trends that emerged from those exercises include:[12]

- A movement toward digital identity schemes, which the WEF has previously stated will determine "what products, services and information we can access — or, conversely, what is closed off to us"[13]
- "Fake news" being recognized as a "digital pandemic" that people must be protected from
- A recommendation to strengthen public-private partnerships and collaboration
- A recommendation to increase consolidation of corporate and state resources
- A recommendation to target cryptocurrencies, especially those offering transactional anonymity, and the infrastructure used by them.[14] This, even though only 0.34% of cryptocurrency transactions in 2020 were tied to criminal activity, down from 2% in 2019[15]

As you can see, the solutions presented by these unelected globalists always require more surveillance and greater public-private collaboration that blurs the line between elected and unelected decision-makers. In the end, unelected globalists are demanding — and getting — more and more power to make decisions for humanity.

Recent Cyberattacks Reveal the Scope of the Problem

Cyberattacks are clearly increasing and getting larger in scope. This should come as no surprise, as the world is becoming increasingly digitized — and connected digitally.

Hacking health records, for example, was near-impossible in years past when paper records were kept, but with the introduction of digital health records and the sharing of those records across institutions, hacking has become a relatively simple, and profitable, affair.

> **“The end game of all these organized cyberthreats is to eliminate anonymity on the web under the auspice of 'preventing cybercrime,' and impose extreme centralization of the internet for the purpose of information control.”**

Recent cyberattacks demonstrating the scope of the problem include:

- The 2016 Bangladesh Bank heist, where hackers absconded with $81 million in a matter of hours by targeting the bank's SWIFT accounts (the international money transfer system banks use to transfer money between themselves). Hackers used the SWIFT credentials of employees at the Bangladesh Central Bank to request money transfers to bank accounts in the Philippines and other Asian banks.[16]
- In 2020, a ransomware attack resulted in BancoEstado, one of the biggest banks in Chile, to temporarily shut down all branches. In this case, the bank's internal IT network was infected with the REvil ransomware originating from an infected Office file opened by an employee. The file installed a back door to the bank's network, which the hackers then used to install the ransomware.[17]
- At the end of 2020, hackers accessed the SolarWinds supply chain by delivering a backdoor malware through an infected SolarWind Orion software update. The malware infected the networks, systems and data of more than 30,000 public and private organizations, including local, state and federal agencies. It's thought to be the largest and most devastating cyber breach to date.[18]

- In early August 2023, California-based Prospect Medical Holdings Inc. had to shut down certain services, including outpatient medical imaging and blood draw services, after a cyber breach was detected. Some of its hospitals and clinics also had to revert to paper records as IT systems were shuttered.
- That same week, Pennsylvania-based Crozer Health also had to shut down its computer systems and close emergency rooms due to a system-wide ransomware attack.[19,20]

  It experienced a similar attack in 2020,[21] and apparently didn't figure out how to prevent a repeat. According to cybersecurity experts, Crozer data was auctioned off in that 2020 attack after Crozer refused to pay the ransom.

Eliminating Online Anonymity Is the Endgame

So, where is all of this taking us? As explained by investigative journalist Whitney Webb in the short video at the top of this article, the end game is a) to eliminate anonymity on the web under the auspice of "preventing cybercrime" and b) to impose extreme centralization of the internet for the purpose of information control. She also wrote about this in a July 2021 article for The Last American Vagabond:[22]

> *"... there is a ... push by WEF partners to 'tackle cybercrime' that seeks to end privacy and the potential for anonymity on the internet in general, by linking government-issued IDs to internet access.*
>
> *Such a policy would allow governments to surveil every piece of online content accessed as well as every post or comment authored by each citizen, supposedly to ensure that no citizen can engage in 'criminal' activity online.*
>
> *Notably, the WEF Partnership against Cybercrime employs a very broad definition of what constitutes a 'cybercriminal' as they apply this label readily to those who post or host content deemed to be 'disinformation' that represents a threat to 'democratic' governments.*

The WEF's interest in criminalizing and censoring online content has been made evident by its recent creation of a new Global Coalition for Digital Safety to facilitate the increased regulation of online speech by both the public and private sectors."

Global Cyber Utility Will Usher in Unprecedented Surveillance

In her article,[23] Webb goes on to review the roles of the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the WEF Partnership Against Cybercrime (WEF-PAC). Both are currently being positioned as a "main solution" to the catastrophic cyber pandemic predicted, by being set up as centers of global coordination of financial services and the protection thereof, with a "shared narrative" against cybercrime.

This new global "cyber utility" seeks to unite law enforcement agencies, cybersecurity firms, banks and other large corporations and "stakeholders" around the world under one umbrella to prevent cybercrime. For that to be feasible, WEF-PAC has noted that legislation may need to be revised to allow law enforcement agencies and government regulators to fuse their operations with the private sector, including entities they're meant to oversee, regulate and prosecute for wrongdoing.

We're already seeing this plan take shape, with the rapid consolidation of banks. The next step will be to merge the remaining banks with regulators and intelligence agencies, forming this new "cyber utility" entity.[24] Webb continues:[25]

"Many organizations that are related to or are formally part of WEF-PAC are deeply invested in Central Bank Digital Currencies (CBDCs) as well as efforts to digitalize and thus more easily control nearly every sector of the global economy and to regulate the internet.

Therefore, it is reasonable to conclude that many of these groups may look to justify regulations and other measures that will advance these agendas in which they have long-term 'strategic interests' through the promotion of a

'shared narrative' that is deemed most palatable to the general public, but not necessarily based in fact ...

The considerable involvement of some of the most powerful corporations in the world from some of the most critical sectors that underpin the current economy, as well as non-profits that manage key internet, government and utility infrastructure in these organizations that comprise WEF-PAC is highly significant and also concerning for more than a few reasons.

Indeed, if all were to follow the call to form a 'shared narrative,' whether it is true or not, in pursuit of long-term 'strategic interests,' which the WEF and many of its partners directly relate to the rapid implementation of the 4th Industrial Revolution via the 'Great Reset,' the WEF-PAC global cyber utility could emerge sooner rather than later.

As evidenced by the architecture put forth by WEF-PAC, the power that organization would have over the public and private sectors is considerable.

Such an organization, once established, could usher in long-standing efforts to both require a digital ID to access and use the internet as well as eliminate the ability to conduct anonymous financial transactions. Both policies would advance the overarching goal of both the WEF and many corporations and governments to usher in a new age of unprecedented surveillance of ordinary citizens."

Sources and References

- [1] Weforum June 1, 2020
- [2] Cyberscoop November 18, 2020
- [3] FSISAC.com Navigating Cyber 2021
- [4] Cyberscoop March 30, 2021
- [5] Weforum February 12, 2021
- [6] Reuters December 9, 2021
- [7, 8] Daily Telegraph NZ December 16, 2021
- [9, 14, 15, 22, 23, 25] The Last American Vagabond July 8, 2021
- [10, 12] Global Research May 7, 2021

- [11] Unlimited Hangout February 5, 2021
- [13] WEF Identity in a Digital World September 2018
- [16] Wired May 17, 2016
- [17] ZDnet September 7, 2020
- [18] Tech Target June 27, 2023
- [19] Inquirer August 3, 2023
- [20] CBS News August 4, 2023
- [21] Cyberscoop June 19, 2020
- [24] The Last American Vagabond April 7, 2021