Prepping for a Cyber Pandemic: Cyber Polygon 2021 to Stage Supply Chain Attack Simulation

Will Cyber Polygon 2021 be as prophetic as Event 201 in simulating a pandemic response? The implications for the country are frightening to think about!

We have had a few warnings already, in the recent shut down of the Colonial Pipeline serving an area from Houston to New Jersey and most of the southeast; then there was the shutdown of the world's largest beef processor JBS was shut down last month. There have been a few smaller warnings as well, frequent outages of Internet and bank card operations over the past year. All were hints, but likely meant to get our attention. Colonial Pipeline and JBS were acts of cyber-attacks demanding ransom money!

JBS produces beef, pork and poultry, and is headquartered in Greeley, Colorado. The company's website says it has 84 locations in the United States and Australia, as well as nearly two dozen sites in the United Kingdom. The company also has locations in Mexico, Canada, and New Zealand, as well as other locations throughout Europe. My interest in Cyber Polygon 2021 was peaked when I reported on Bill Gates buying up farm land across the country.

We were told the Colonial Pipe Line and the JBS meat processor was both computer ransomware attacks, hackers steal an organization's data and lock its computers. Victims must pay to regain access to their network and prevent the release of sensitive

information. Two weeks ago another pipe line service operation was also shut down, and I did not read all the news details. I can only do so much in a day.

Similar to JBS, Colonial Pipeline's systems were hit with ransomware. Once a company has been hit by ransomware, its first course of action is usually to take much or all of its systems offline to isolate the hackers' access and make sure they can't move into other parts of the network.

That may be among the reasons why JBS shut down its operations and Colonial shut down its pipeline — to disconnect the companies' operations from the IT systems that hackers breached. People briefed on the Colonial attack told media that the company halted operations because its billing system was also compromised and feared they wouldn't be able to determine how much to bill customers for fuel they received.

The most recent indicator that has been on my radar has been the shortage of microchips used in cars, trucks, farm equipment. Up the road from me a couple hours a way is the Kentucky Speedway which is overflowing with Ford pickup trucks, stored production from their Louisville, KY plant, but lacking microchips needed for the vehicles to become operational and marketable. John Deere suspended production for lack of microchips about a month ago.

The World Economic Forum (WEF) will stage another cyber-attack exercise as it continues to prep for a potential cyber pandemic that founder Klaus Schwab says will be worse than the current global crisis caused by Covid. From that we can only conclude it will impact millions of people. The major thing that comes to mind would be the collapse of the SWIFT global inter-banking system and the financial network in some way that undermines cash and credit transactions. We have to consider this as the onslaught of the "cashless" society and the transition to computer units or a global unit of value continues to unfold.

I follow a web site Biometrics.com and there was big news this week relative to finger-print biometrics. Since the Bible has made it clear that the world will be tied in with a global system of identity, it provides a pulse overview on the entire realm of global ID. With Bill Gates new Quantum Dot/Hydrogel ID2020 and his ties to the WEF, it is quite likely that it has the lead in this entire issue of digital identity.

The markets for fingerprint biometrics in cards, facial recognition for physical access control systems, and both in mobile devices are gaining momentum. Fingerprint Cards leads the week with a U.S. patent and a rollout related to biometric payment cards, while Thales is in the news for payment and national ID cards and Idemia for the latter plus a smartphone-based identity verification service. The widely-read stories below contain a dozen new customer wins and partnerships, plus more than half a dozen new biometrics and digital identity technology launches.

Top biometrics news of the week indicates the frenzy to market ID technology world-wide:

Fingerprint Cards continues to build out its intellectual property for biometric payment cards, patenting a method for integrating its fingerprint module with standard card production techniques in the U.S. Instead of soldering the module to an inlay and then laminating that in, the new method involves electric wire-bonds and connecting pads.

Consumers in the Philippines prefer using their fingerprints for authentication, then face and iris biometrics, according to a new survey from Visa. As the country's PhilID biometric cards continue to roll out, meanwhile, the national press is pointing out the regulatory requirements for using it in authentication, including user consent.

Contactless biometric payment cards from Thales with Fingerprint Cards' technology are coming to market from BBVA Mexico in the form of the Smart Key Visa. The card is being launched for two groups of BBVA customers to start, but is expected to be offered to all 23.7 million clients eventually.

Selfie biometrics for remote onboarding and authentication continues to be a rapid growth area, and Stripe wants in. As the new Stripe Identity launches, Idemia, TruNarrative and Yoti each signed up new customers, while Accura Scan and Pass unveiled new solutions. ID.me's use of biometrics, meanwhile, is being targeted by a petition campaign arguing too many people are waiting too long for unemployment benefits.

A new report on face biometrics and digital commerce shows three-quarters of millennials are happy using selfie biometrics for authentication, mainly because it is convenient. Trunarrative, Veriff, Sumsub and iDenfy have each signed up fintech service providers to help them meet their regulatory obligations and prevent fraud, while a mystery provider won a Malaysian social media customer.

Jumio VP of APAC Frederic Ho joins BFM's Tech Talk podcast to discuss how Malaysia's digital identity program will impact inclusivity, online service access, and the country's economy. Ho emphasizes the importance of liveness, talks about what makes a good identity verification solution, and praises the Philippines' rapid embrace of digital technologies.

iPhones are taking another step towards going passwordless, with Apple testing a new WebAuthn-based feature as part of iCloud Keychains that allows users to associate their Face ID or Touch ID biometrics with the login for a particular account across different devices. While the feature only works with other Apple products at the moment, the company is in talks to add support for cross-platform authentication.

South Korean biometric authentication startup Octatco, SK Telecom and one of the latter's subsidiaries are developing a keycard utilizing fingerprints with a quantum random number generator for FIDO passwordless authentication. The EzQuant security keys has been through FIDO Alliance interoperability testing, and can be integrated with various enterprise software systems.

Call volumes during the pandemic spiked by 800 percent prompting more than three-quarters of fraud detection and security managers to change their protocols and policies, according to Pindrop data. CTO Collin Davis maps the altered fraud landscape, including tough terrain for fintechs, in a Biometric Update guest post.

Nepal is currently deciding between Thales and Idemia's competing bids for its national biometric ID card contract after a delay caused by the COVID-19 pandemic. Each bid is for between $14 million and $15 million to issue an expected 12 million cards, but Idemia ran the pilot, and was previously awarded a contract without a competitive process.

SITA, NEC and Star Alliance have formed a partnership to make flight boarding with face biometrics work across the Alliance's member airlines with only one enrollment, and advance deployments of the technology throughout the world. NIC I:Delight and SITA Smart Path will be connected for combined use at up to 460 airports.

Biometric touchless access control deployments have been announced by Biosite for a construction site and Invixium for an industrial facility and data centers. Amid this booming market, new hardware products in the space have been developed by HID Global and Anviz, and ZKTeco has launched video access management software.

Olympic venues spread around Tokyo will be using NEC's face biometrics to authenticate participating athletes, as well staff, media and volunteers during the 2021 games, putting the technology to the test in one of the year's most intensely-covered events, E&T Magazine. The article considers the data collection implications, and says a strong performance at the games by the technology could inspire more extensive deployments, but the reverse may also be true.

In a pair of interesting webinars over the past week, BixeLab explained the concept and value of Red Teaming for testing biometric systems and the EAB went in-depth on the TELEFI facial recognition forensic data sharing system.

The Los Angeles Review of Books carries a review of Susan Liautaud's 'The Power of Ethics: How to Make Good Choices in a Complicated World' by Rochester Institute of Technology Philosophy Professor Evan Selinger, who co-wrote an editorial recently for Wired arguing against identity verification with face biometrics. Selinger is not impressed with the arguments made by Liautaud, and takes umbrage at her dismissal of proposals to ban hazardous technologies.

Submissions have closed in the International Identity Day Design Competition, organized by ID4Africa and sponsored by Integrated Biometrics. An official design for ID-Day 2021 will be selected from among the submissions by African digital artists, and offered for re-use by the identity community, with the winner receiving a cash prize of $3,000.

Whether you are taking a helicopter ride over the mountains, or just racing your sports car from one shootout to another, you can bring your belongings comfortably with Kabuto Luggage featuring a biometric sensor from Fingerprint Cards. The company's latest high-production video promotes the new, larger entry in its fingerprint-secured luggage line, The Trunk.

My wife and I have experienced what everyone dreads and fears. She was in a Walmart in Lebanon, KY a week ago when she was the target of a team that stole her wallet from her purse. The perps stole her wallet inside her purse, containing her credit card, driver's license, DQ gift card, and my debit card. As she went to check out, in less than fifteen minutes she realized her wallet was missing. She quickly called the bank to report the wallet and bank cards stolen, she called me, and had me call about my debit card being stolen. Between calling the bank and me, she then called the local police. All accounts were frozen, but within a half hour, the thieves had racked up purchases at a local Walgreens. The police said the same perps hit three Walmart's in 3 contiguous counties in just a matter of a few hours. My wife has spent more time on the phone with the bank, getting new PIN numbers, answering police and bank security personnel questions, and getting back to what is normal personal affairs.

I have not had the time to do all the research about Klaus Schwab's plan to pull off his **Cyber Polygon 2021,** a global, regional, computer attack, or to pull down the Internet for an undefined period of time. All are possible when you consider the people behind this Global Reset being brought to our door steps. We are so interconnected in such a way as to be vulnerable at every turn. Our national supply chain is built upon a "just-in-time" delivery system. At the bottom of this article, I will include some of Clif High's remarks from last evening's podcast.

Years ago I worked in logistics as a traveling expediter traveling the country, babysitting valuable high-n-wide oversized power equipment moved by railroad cars. It was my job to ride herd with the shipments movement safely and as quickly as possible. I often became the equivalent of a third-party when it came to insurance claims and damages in transit as to the circumstances as to what happened and how. I'm not talking a few thousand dollars here as such equipment cost millions of dollars and often required months to replace. As an example of this "just-in-time" concept, I once was in the Union Pacific Railroad's huge freight train yard in North Platte, Nebraska, and called the customer in Gillette, Wyoming just before departure so they could schedule heavy lift cranes for my railroad cars for unloading on my destination arrival. The rental on the equipment required to unload the heavy duty railroad cars was metering at $500 an hour. As our freight train was slowing down on the outskirts of Gillette, Wyoming, I could see two large lift cranes and their equipment on several low-boy trailers rolling in to meet us.

Virtually every grocery store and super-market is on a 3-day inventory "just-in-time" delivery system. It's not much different for most of the retail world. So Klaus Schwab's Cyber Polygon 2021 exercise could potentially do a lot of damage. He said it would be worse than the Covid pandemic!

The SolarWinds hack served as a wake-up call to the supply chain attack vulnerabilities still present in public and private organizations, and it served as a warning that the next breach could be exponentially worse in spreading through any device connected to the internet.

Following up on last year's Cyber Polygon cyber-attack exercise and event aimed at preventing a digital pandemic, the WEF has announced that the 2021 edition will be taking place on **July 9**, **2021.** That date is a Friday, a perfect time to hit on a weekend when people are out and about. I quake just thinking about how to imagine its impact rippling effect.

"A cyber-attack with COVID-like characteristics would spread faster and farther than any biological virus" — World Economic Forum

This year, **Cyber Polygon 2021** will simulate a fictional cyber-attack with participants from dozens of countries responding to "**a targeted supply chain attack on a corporate ecosystem in real time.**" What is a corporate ecosystem? What does this mean? Furthermore, how will it disrupt the lives of the public in ways to undermine public safety, well-being, and sanity? Given what Covid-19 did to destroy lives, the one thing that is sure with the WEF plan, it will be worse than Covid-19. My imagination is beginning to shift to pondering what most will affect the public in general. Will it be an issue with water? We are hearing about the western half of the nation in drought and dangerous heat-index and discomfort. Will it be electrical power grid-related? Water and electrical are the first two items that come to mind.

Starting in the early 1990s, James F. Moore originated the strategic planning concept of a business ecosystem, now widely adopted in the high tech community. The basic definition comes from Moore's book, *'The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems.'* I am certainly out of any loop to grasp all of what this might represent but if I was to guess, life is not going to go well for the public as they transition countries to the New World Order and Sustainable Development programming. The public is still reeling from the Covid virus scam.

According to the WEF, COVID-19 was known as an anticipated risk, and so is its digital equivalent.

What's more, *"A cyber-attack with COVID-like characteristics would spread faster and farther than any biological virus. Its reproductive rate would be around 10 times greater than what we've experienced with the coronavirus."*

"It is important to use the COVID-19 crisis as a timely opportunity to reflect on the lessons of cybersecurity community to draw and improve our unpreparedness for a potential cyber pandemic" — Klaus Schwab

Here, we take a look at three trends emerging from **Cyber Polygon 2020** to uncover what moves the public and private sectors may make in anticipation of a digital pandemic.

But first, where did the notion of a cyber pandemic come from?

An Anticipated Cyber Pandemic

In his welcoming remarks at **Cyber Polygon 2020**, WEF Founder Klaus Schwab warned about a coming "**cyber pandemic**" that would be worse than the current global crisis.

"We all know, but still pay insufficient attention to, the frightening scenario of a comprehensive cyber-attack, which would bring a complete halt to the power supply, transportation, hospital services, our society as a whole," he said.

"The COVID-19 crisis would be seen in this respect as a small disturbance in comparison to a major cyber-attack."

Top Security and Risk Trends for 2021

1	Cybersecurity mesh	2	Cyber-savvy boards
3	Vendor consolidation	4	Identity-first security
5	Managing machine identities becoming a critical security capability		
6	"Remote work" now just "work"	7	Breach and attack simulation
8	Privacy-enhancing computation techniques		

Source: Gartner.com

Schwab added, *"It is important to use the COVID-19 crisis as a timely opportunity to reflect on the lessons of cybersecurity community to draw and improve our unpreparedness for a potential cyber pandemic."*

As the digital world encroaches on our physical and biological worlds, an effective cyber-attack could compromise anything connected to the internet, including:

Medical devices that keep people alive

The Internet of Things (IoT) ecosystem of connected devices that run smart homes (i.e. cameras, microphones, sensors, etc.)

The [Internet of Bodies (IoB)](#) ecosystem of digitally-connected humans
Global financial systems
Energy grids
Water treatment facilities
Government IT systems
Military and defense infrastructure
And more

Currently, *"The only way to stop the exponential propagation of a COVID-like cyber-attack threat,"* according to the WEF, *"is to fully disconnect the millions of vulnerable devices from one another and from the internet."*

But, *"A single day without the internet would cost our economies more than $50 billion, and that's before considering economic and societal damages should these devices be linked to essential services, such as transports or healthcare."*

"The COVID-19 crisis would be seen in this respect as a small disturbance in comparison to a major cyber-attack" — Klaus Schwab

Needless to say, a cyber pandemic would wreak havoc on nearly all aspects of society.

However, the devil is in the details, and the solutions recommended for a cyber pandemic could be far more detrimental to individual liberty than the cyber-attack itself.

<p style="text-align:center; color:red;">**Cyber Polygon 2020 Emerging Trends**</p>

The central theme of the **Cyber Polygon 2020** exercise was *"digital pandemic: how to prevent a crisis and to reinforce cybersecurity on all levels."*

The goal of last year's Cyber Polygon event was to:

Develop the teams' competencies in repelling cyber attacks

Engage the management of global organizations and corporations in the cybersecurity dialogue

Raise public awareness in cybersecurity

The exercise featured two parallel tracks: a live stream for a mass audience and technical training for cybersecurity specialists, and 120 of the largest Russian and international organizations from 29 countries joined the technical training **to practice response to a targeted attack, aimed at hacking company data and undermining its reputation**.

Most importantly, note that date of July 9th and following. While the narrative for the Covid-19 hoax is unraveling and people are thinking they can relax, something bigger is in store for the world.

While the technical training side of the event was dedicated to responding to a single attack, the conversations from the live stream portions provided the most insights for dealing with the potential fallout of the attack — the digital pandemic.

Here are three trends emerging from the **live stream** discussions and the **Cyber Polygon 2020 [results report](#)**.

1) Governments Will Inevitably Move Towards Digital Identity Schemes
Speaking at **Cyber Polygon 2020**, former British Prime Minister Tony Blair stated with confidence that governments are "absolutely, inevitably" moving in the direction of digital identity adoption.

"Digital ID for me is a very big part of the future" — Tony Blair

[Digital identity](#) is a major component of the WEF's great reset agenda as it relates to transformative technologies powering the Fourth Industrial Revolution.

A digital identity keeps a record of everything you do online, including what you share on social media, the websites you visit, and your smartphone's geolocation, and it can house all of the credentials you would normally find in a physical wallet, such as your driver's license, insurance card, and credit cards.

In his talk, Blair didn't make the case for why having a digital identity was actually necessary to prevent a cyber pandemic, but rather that digital identities would be an inevitable part of the digital ecosystem, and so governments should work with technology companies to protect and regulate their use.

"Digital ID for me is a very big part of the future," said Blair.

"Inevitably, governments are going to move in this direction — absolutely, inevitably," he added.

"And so what I think's most important is that we from the political side wake-up to the potential of technology and engage with the change makers inventing the technology, so that we understand it and can regulate it sensibly and not stupidly."
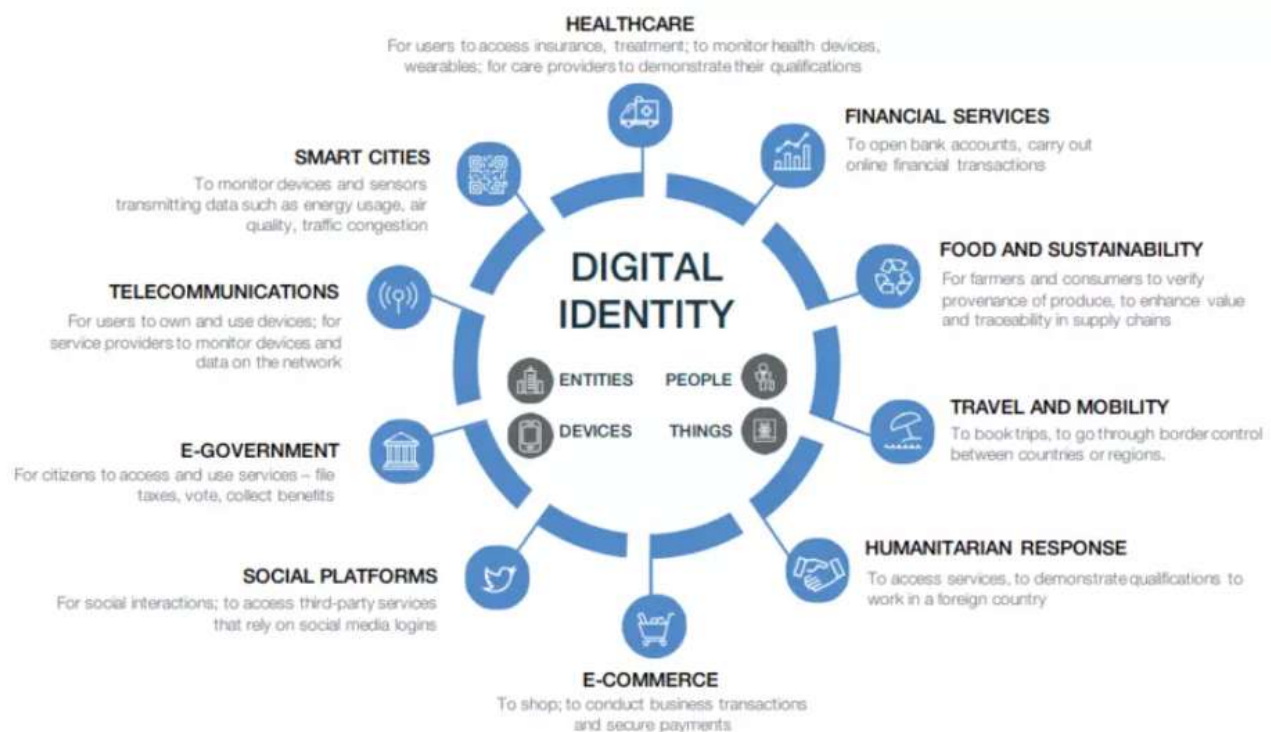

HEALTHCARE
For users to access insurance, treatment; to monitor health devices, wearables; for care providers to demonstrate their qualifications

FINANCIAL SERVICES
To open bank accounts, carry out online financial transactions

SMART CITIES
To monitor devices and sensors transmitting data such as energy usage, air quality, traffic congestion

FOOD AND SUSTAINABILITY
For farmers and consumers to verify provenance of produce, to enhance value and traceability in supply chains

TELECOMMUNICATIONS
For users to own and use devices; for service providers to monitor devices and data on the network

DIGITAL IDENTITY

ENTITIES   PEOPLE
DEVICES   THINGS

TRAVEL AND MOBILITY
To book trips, to go through border control between countries or regions.

E-GOVERNMENT
For citizens to access and use services – file taxes, vote, collect benefits

HUMANITARIAN RESPONSE
To access services, to demonstrate qualifications to work in a foreign country

SOCIAL PLATFORMS
For social interactions; to access third-party services that rely on social media logins

E-COMMERCE
To shop; to conduct business transactions and secure payments

Image Source: World Economic Forum

If a hacker were to gain control over someone's digital identity, they could essentially shut them out of participating in civil society by erasing them completely, or exploiting their information in such a way that blocks victims from proving they have money in the bank, a passport that allows them to travel, a valid driver's license, proof of immunity, and any other credentials that are necessary for citizens to access goods and services. My wife had to go through hoops to get a new driver's license in her wallet theft.

And while digital identities show promise towards improving the livelihoods of millions when governed ethically, they are also used by authoritarian governments to profile and police citizen behavior under a social credit system.

Whether the data be secured or not, **individual liberty will depend on how the technology is used and the level of trust given to those who govern it**.

According to a [WEF report from 2018](#), *"digital identity determines what products, services and information we can access – or, conversely, what is closed off to us"* — the level of which to be determined by our online behavior.

If Blair is right and governments will inevitably adopt digital identities, then a well-coordinated cyber-attack affecting digital identity systems would lead to a cyber pandemic affecting the whole of society.

2) 'Fake News' Is a Digital Pandemic & the Majority of Citizens Are Incapable of Thinking Critically

Cyber Polygon 2020 dedicated one of its live streams sessions to the concept of *"fake news"* as being a deadly, digital pandemic plaguing 2020.

"If you're talking about someone who […] has not read very much, whose knowledge is limited — that person is much easier to fool and much more ready to accept whatever he or she is told" — Vladimir Pozner, Journalist

By the end of their conversation, *'BBC World News'* presenter Nik Gowing and veteran journalist Vladimir Pozner arrived at the conclusion that the average person of voting age was not capable of thinking critically for themselves and was more likely to swallow any information put out there than someone who went to a university.

Both Gowing and Pozner agreed that the majority of citizens were uneducated, were not well-read, and hadn't traveled enough to know the difference between what was fake and what was real.

Pozner: *"You're launching your argument based on a sense that your average viewer, listener, reader has a critical outlook from the outset."*

"I think that there are an awful lot of people who don't have that critical outlook and just swallow it whole."

Gowan: *"I agree […] "You have to have that questioning instinct."*

Pozner: *"If someone is well-educated, has a university education, has read, has traveled — that person's reaction to what he or she is reading or listening to is one thing."*

"If you're talking about someone who finished grammar school or the like and has not had the opportunity because of where that person comes from, has not read very much, whose knowledge is limited — that person is much easier to fool and much more ready to accept whatever he or she is told."

"When we're dealing with this deliberate lie, who is it directed at mainly?"

"In my opinion, <u>it's mainly directed towards the ordinary person</u> — not towards the intellectual elite, not towards those who have the ability to actually think it through, but to those who have not had that advantage, to the less privileged people who are the majority, and who are the ones who vote, and who are the ones who, ultimately, when they say, 'the people,' they are 'the people,' and I think they are the ones who are victimized by this trend."

With the assumption that average people aren't capable of thinking critically and that the majority of citizens are therefore *"victims,"* the two journalists turned the conversation towards how to protect victims of the *"fake news pandemic."*

But in the end, they had no idea how to do that, and fake news, misinformation, and disinformation remain "existential threats."

Cyber Polygon 2020 didn't issue any concrete recommendations with regards to dealing with fake news; however, the WEF-led Event 201 coronavirus pandemic simulation [did recommend](#) that, *"Governments will need to partner with traditional and social media companies to research and develop nimble approaches to countering misinformation."*

3) Trustworthy Public & Private Partnerships Will Need to Be Strengthened
Establishing trustworthy collaborations among the public and private sectors can help prevent a digital pandemic, according to the Polygon 2020 report.

"A critical situation cannot be tackled by an organization or a lone individual," it reads, adding, *"In a highly interconnected world, a single cyber-attack can spread exponentially across the global community."*

"This situation can be prevented by promoting collaboration between the public and private sectors and law enforcement agencies."

"Furthermore, efficient interaction requires the implementation and regulation of a range of standards, the exchange of information and establishing trustworthy relationships."

"When we do see this next crisis, it will be faster than what we've seen with COVID, the exponential growth rate will be much steeper, the impact will be greater, and as a result the economic and social implications will be even more significant" — Jeremy Jurgens, WEF Chief Business Officer

However, with countries like [China stealing intellectual property](#), sponsoring state-run cyber-attacks that have [compromised the personal information of nearly every single American adult](#), and [silencing doctors and whistleblowers](#) about the CCP's responsibility in the coronavirus pandemic, establishing trust and bolstering collaborations among governments and corporations are lofty goals to set.

During the **Polygon 2020** live session, WEF Chief Business Officer Jeremy Jurgens said that preventing the next crisis will require that all sectors of society and the economy come together.

"I believe that there will be another crisis," he said. *"It will be more significant. We need to actually start preparing for that now."*

"We need to start this cooperation and understanding early, so that when the crisis does hit, we're in a position to respond effectively to it."

"I would anticipate that when we do see this next crisis, it will be faster than what we've seen with COVID, the exponential growth rate will be much steeper, the impact will be greater, and as a result the economic and social implications will be even more significant."

"I think it's really important that we don't underestimate the severity of a crisis like this — the impact it could have."

"It's going to take all sectors of society and the economy to come together to address that," Jurgens added.

The **Cyber Polygon 2020** report, along with the virtual sessions recorded during Davos Week at the end of January, 2021, **all highlight the need/desire for public and private collaboration** — not just as a means to avert a cyber pandemic — but for reshaping the entire global economy and revamping all aspects of society under a new form of stakeholder capitalism brought on by the great reset.

Trends Emerging From Digital Pandemic Exercise

In this article, we looked at three trends emerging **Cyber Polygon 2020**:

A greater consolidation of resources and collaborations among corporations and states

A plan to deal with fake news, disinformation, and misinformation that has yet to be unveiled

A push towards digital identity that will need to be secured and protected

While these basic observations were plucked from last year's exercise, this year's **Cyber Polygon** will present new challenges in which participants will respond to a different threat — a targeted supply chain attack on a corporate ecosystem in real-time.

If the results and recommendations from previous pandemic simulations are any indication of what may lie ahead for society, then the findings and policies coming out of **Cyber Polygon 2021** may have real-world societal impact in the very near future.

For example, many scenarios played out in the WEF-backed fictional pandemic simulations [Clade X](#) (May, 2018) and [Event 201](#) (October, 2019) later came to pass, along with several policy [recommendations](#) for dealing with the COVID-19 pandemic.

These scenarios depicted:
Governments implementing lockdowns worldwide
The collapse of many industries
Growing mistrust between governments and citizens
A greater adoption of biometric surveillance technologies
Social media censorship in the name of combating misinformation
The desire to flood communication channels with "authoritative" sources
Mass unemployment
Rioting in the streets
And a whole lot more!

When the World Health Organization (WHO) declared the coronavirus a pandemic on March 11, 2020, governments all over the world went into lockdown, which had devastating effects on the economy with businesses closing, civil unrest skyrocketing, unemployment surging, housing foreclosures on the horizon, and the largest transfer of wealth ever recorded in human history.

However, many of these scenarios were already anticipated and taken into account in previous simulations, and yet they all still came to pass.

Will the conversations coming out of **Cyber Polygon 2021** prove to be as prophetic for the digital world as Event 201 and Clade X were for the physical one?

[A timeline of the great reset agenda: from foundation to Event 201 and the pandemic of 2020](#)
['Ransomware is quickly becoming a national emergency' amid pandemic: CISA acting director testifies](#)
[How healthcare is vulnerable to cyber attacks, assassinations & geopolitical agendas](#)

This without question is designed to demoralize the average person on the street. It is intended to destroy the human spirit and force human capitulation to the globalist agenda of becoming cogs in the system of human enslavement.

My hope is that we all can maintain our sanity in coping with the adjustments needed to get through this to the point that God has reached the point where the straw that broke the camel's back will result in Divine intervention. Even those of us who saw all this coming down the pike are unlikely to anticipate or could have conceived of the degree of Satan's ingenious mind.

Below from here down to the end is Clif High's remarks from Saturday, June 19th, 2021.

COVID-19 VIRUS HAS TWO COMPONENTS

The "novel coronavirus", SARS-CoV-2 has two components,
1) The Spike Protein, a bioweapon which was originally developed at Fort Detrick. This work was continued by Ralph Baric at the University of North Carolina at Chapel Hill and; **2) The Coronavirus,** another bioweapon developed in China by the People's Liberation Army.

Chinese refugee virologist, Dr. Yan Li-Meng has claimed for over a year that the backbone of this virus was developed by the Chinese military (PLA) and that it is based on the Zhoushan bat coronavirus, which she has referred to as "ZC45" and "ZXC21".

The Fauci emails reveal that the NIH, the Pentagon and – now, we learn, Google – financed the merging of these two elements, the spike protein with the virus (aka "Gain of Function") at the Wuhan Institute of Virology, through Peter Daszak's NGO, EcoHealth Alliance.

COVID-19 IS A COLLABORATION BETWEEN THE CCP & GLOBALIST CABAL

Currently, there's a public debate as to whether or not the CCP virus was released by accident or on purpose, although most agree that the CCP purposefully allowed the virus to spread. These points are a diversion, because it's clear that the Globalists, i.e., the UN, World Economic Forum, Big Pharma, big banks, Fortune 1000 Companies and Bill Gates colluded with the CCP in this bioterrorism campaign as a pretext for the Great Reset and for *"vaccinating the entire planetary population."*

To blame everything on China is nonsense, albeit politically expedient for those who wish to take down the CCP, like members of the Chinese Whistleblower Movement. Both the CCP and the economic elite stood to gain, long-term from the deliberate collapsing of the West and from the global depopulation agenda. The bankster Cabal and the CCP are collaborators in this mass genocide project.

In this video, Clif High begins by explaining that the Globalists engineered the spike protein in order to conduct mass genocide. He has reversed his previous opinion that Xi Jinping is being scapegoated by the Globalists. He now believes that Xi was in on the mass genocide project, all along. (This was my contention in November, 2019). He cites a speech given by Xi in November 2019, which made a huge splash on the Chinese Deep Web, in which Xi said, *"At the end of this [unspecified], CHINA, [written all large] will be more prosperous. All Chinese people in China will be more prosperous when the end arrives."*

Clif says, *"If that were to be true, China would have to accumulate more stuff from the rest of the world...And within China, the idea is even more disconcerting, because the only way one Chinese can be more prosperous in China is going to be if there's a lot fewer Chinese to divide up the stuff...and I think it [Xi's statement] directly related to the virus and what was to come, so I think Xi was part of it. (Initially, I thought it was done to screw him)."*

He says Chinese scientists attached the spike protein to a prior virus but in 2015, they discovered that this was an inadequate delivery mechanism. "In 2016 – a year later – we hear the head of Fauci's chief of production [Peter Daszak] bragging in a video that they had attached the spike protein to a coronavirus...They'd tried another virus that had crapped-out on them in 2015 and they had to re-engineer it to the [Zhoushan bat] coronavirus in 2016...

"The coronavirus was used because they were under the impression, after tests done on the Uyghurs in 2015 and 2016 that they could use the coronavirus to good effect, because it appeared to be more than 'majority-population-effective'.

"They were under the impression that their...COVID-19 would...disable or kill more than the majority of the population, based on the results they had, testing it on the Uyghur population." But it turns out the Uyghur prisoners were very susceptible because they're Sun-avoiders [low Vitamin D] and they have poor nutrition.

He says, "Sometime between 2016 and 2019, they discovered that CV-19 would not be effective and in 2019, they presented the very first samples or tests of the mRNA vaccine with the spike.

And that was presented to Fauci's crew in 2019. So sometime between 2016 and 2019, that phase of the plot was hatched; that phase of the global depopulation plot that I'm discussing here, now."

They'd figured out by 2016 that they needed another approach for populations with adequate levels of Vitamin D and that's when it was decided that it would be done via injection.

"Once you're inoculated, you become a spike protein-producing, a vaccine-producing machine...If you get enough shots in you, you'll produce spike proteins and you'll infect everyone around you...You become the node for the supposed killing approach..."

"Whether you get it from the virus or you get it from the shot, the spike protein is what's causing the problems. We now know from autopsies that the spike protein travels and it gets in all your organs and it concentrates in the testes, the ovaries, the liver, the spleen, the endothelial layer inside the blood vessels, the heart...the brain. It gets throughout your organs but it concentrates in those that are replete, replenished with heavy blood supply; so, your gonads. Your stomach, not so much, because the stomach is only active when you're digesting stuff. Your brain, yeah, you get a lot of spike protein, because you pump a lot of blood through your brain..."

"So now, we're learning that their chosen delivery method is actually the shot, so the shot, itself is part of the bioterrorism war that's now being waged..."

China is now inoculating with their own vaccine, the Sinovac, which is widely criticized in the Death Cult (Mainstream Media) as "ineffective". He says, "Maybe what is making the Moderna and Pfizer so deadly, and then, the AstraZeneca and Johnson & Johnson following behind that – and then, Sinovac behind that, maybe that whole progression comes from the mRNA in a mono-polar magnetic bubble by virtue of SPIONS, (Superparamagnetic Iron Oxide Nanoparticles). Maybe that's so effective at moving the spikes around you...

WE ARE IN WAR

Clif says we are in war of the power elite against the rest of us. *"It's not a nation-state thing, it's not a race war, like the Commies and the Wokians want. It's the power elite vs the rest of us.*

They opened the war, they attacked us, it's their plan, and they've duped lots of people. Now, a lot of the people they've duped are starting to wake up."

We're starting to see doctors and lawyers sue the establishment and this will eventually overwhelm the legal system, because all of the lower level minions who support the power elite took the Vaxx. Though they haven't previously *"informed on their own suffering, for fear of 'looking like a Conservative'...those people are starting to turn on the power elite, they're starting to wake up and many of them are starting to realize, from the magnetism and all of this, just how damaged they are."*

In this war, we will see mass deaths and injuries, which will affect inheritance and labor pools. Clif reminds us of the Black Death, which killed one third of the population of Europe, which had the effect of knocking-out the feudal system. Likewise, he says, *"We're going to have a different kind of social order emerge as this bioterrorism war goes through humanity at this time, and it's going to have many of the same kinds of effects as we have seen in death of empire and great plagues."*

He estimates that those rendered sterile will probably outnumber the dead and injured and this overall cohort will favor the Progressives, college-educated and white people. He says, *"We may breed out Progressivism, Leftism and Communism, simply because they're not going to be able to have children and so many of them will die."*

THE MACROECONOMICS OF MASS DEATH

Clif then gets into the actuarial aspect of the genocide. It's being said that 1/7th of the world population has been vaxxed, which rounds off to 100 million people, worldwide. (I think Clif meant here 1 billion people, which is closer to 1/7th of the world population.)

"All kinds of inflation issues change...real estate becomes real cheap, because you have 100 million less people looking for it; hundred million less people needing washers, dryers, food, etc. This is gonna happen over these next few years. And they

wanted it much larger. It's only going to be something between 100 million and a billion..."

"Let's look at the effect on deflation. That's a deflationary event, if a hundred million people are gone. And this affects everything, in terms of the financials. And it transmits money all around; people with money are gonna die, there's gonna be inheritance being sent to people – those people are going to die...a lot of money will go back to the State, because there won't be anybody in an inheritance chain to pick it up...it's gonna be unlike any kind of normal event..."

"We're already seeing this, for instance, in the rumors that are coming out now about British Airlines, where they say 80% of their pilots and flight crews have taken the vaxx. And so, if that's the case, then they've only have the other 20% to rely on, *because the 80% is gonna go real quick and it's gonna go exceptionally quick, if you take these people that are now prone to blood clots and you stick them up, at high altitudes, and you keep 'em there for a long time and you're gonna kill them off, in essence."*

"And so, maybe also, you've killed-off all of the airline industry. Like, globally."

CENSORSHIP & DISINFO ARE PART OF THE WAR

An example of the latter, says Clif is Charlie Ward, promoting this QFS and NESARA/GESARA stuff. He says Ward has admitted to taking underage girls to Jimmy Savile's Top of the Pops TV show. Clif refers to Ward as a "money launderer" and a "pathological liar" and a "disinfo agent", which he says is also true of Simon Parkes, saying "Simon Parkes is pumping up QFS like mad, now."

He says anybody who is visibly pumping out disinformation should be warned that we are coming into a point where,

"Actively, it will be seen that the MSM has been at war, on the side of the elite, against the whole population and the individuals within the media will be held personally liable, personally culpable for their actions, in spreading the disinfo."

"Once they're eliminated, once they're dealt with, in terms of once the population has gotten their anger out on the Mainstream Media and it doesn't exist anymore, then other disinfo agents will be the next natural target."

Clif says that even the States' vote audits are a distraction from the central fact of the war, which is that we've been poisoned - as much as the election theft is a big part of the war.

"So when they start pumping the audit and throwing Biden under the bus – and Harris and all of that – then you know that the next thing that's going to break out is the reality of the 'vaxxed and the spiked', because that will be one of the last things that they'll use

*as a distraction, **trying to whip us up, totally diverted away from the fact that we've been poisoned...Humanity has been poisoned by a very small part of humanity...”***

"The celebrities, the power elite and everyone – they're gone. They're going to disappear – and it's not because of some Charlie Ward bullshit saying they've been killed. It's not because of Simon Parkes saying they're in Gitmo, OK? There's only so many f***ing cells down there, guys, you've already got it populated with like 20,000 people or something.”

PANIC OF THE ELITES

"None of that is true. It's because they're hiding out. The smart ones know that the backlash is coming and that, when this backlash comes, it will be pitchforks, it will be shotguns. It won't be tar and feathers. It won't be 'allowed to live and just simply retire off somewhere'. So Fauci is not going to be simply able to retire. If he were to retire anywhere, could he go shopping? Could he get out of his house? Could he walk down any street, anywhere in the United States and not fear for his life?...”

"We're going to see a destruction of the social order on many levels but it's not going to be on the levels engineered by the power elites, because, I think to a great extent, timing and circumstance and personalities have interfered, in that the power elite have been hoisted on their own petard by Universe.”

"And as we move into July, we will see the panic. It's already starting to show up...By the time we get into July, you will not be able to look at the Mainstream Media in any way, shape or form, or any other representatives without seeing some signs of panic, whether they're gritting their teeth to hide it or not, these people are going to be in a constant state of panic...”

"Be well. Prepare for any kind of weird-ass reaction from the Powers-That-Be. They may, indeed try and shut off the power grid in certain places. They will certainly try and bring down all of the information sources and keep you in the dark...We may be reduced, for some time to just local radio for getting the news, because the Powers-That-Be are going to start f***ing with the internet but they can't do it too much, for too long because that is the source of their power (laughs), so they can't really turn it off!”

"We're at war. Don't be a casualty."

In all the time of the Covid plandemic, Clif High's comments have confirmed or supported the view of those at American Intelligence Media, pointing to the UK (Rothschild's) efforts to provoke a war between China and the U.S. We may be in the first stage of what will ultimately become a shooting war! He has noted about how the Chinese national telephone system by February, 2020 showed a huge dip in subscribers. He suggests that China was in on the plan to reduce the population as well. Cliff recognizes the convoluted narrative of China's role that may indicate they

were being exploited by both U.S. and UK sources relative to 5G activation, bioweapons and gain-of-function research. However, because of China's level of secrecy, it is unlikely that we will ever have the full story. The plan to "depopulate" the world enabled all parties concern and involvement to be able to point fingers at each other as to the source of blame, and yet maintain plausible denial.

It was Secretary of State Mike Pompeo that created the suspicion when he made the remarks on March 21, about the so-called "live event" remarks were an indication that a unified effort was underway to "depopulate" multiple countries with the weaponized "bioweapon" possibly being "aborted" and thus allowing the alleged Covid pandemic to cover for the 5G flu and 5G sickness. The events from October 1st, 2019 through to February 28th, 2020 remain ensconced in state-terrorism, and double-cross at play.

During the time of the "Diamond Princess" quarantine, something happened or occurred such that China, the UK, Pirbright Institute, MI6, CIA, Dr. Anthony Fauci, the CDC, NIH, and a host of scientists acting as agents became suspect of a double-cross and everyone subsequently fled for cover and plausible deniability.

I have an idea that a double double-cross was in play but have not been able to prove it. In this double double-cross, China was being played by the Rothschild's and Pirbright Institute. At globalist gatherings of the G7, G8, and G20 nations, Russia and China made it clear there would be no global government as such, no unipolar cabal, but a multi-polar world. At this point, Clif High's podcasts support my contention that the Chinese CCP was being set up for the fall.   There are many questions we may never know the answer to, but it is my basic contention the larger issue was a genocidal plan to depopulate the world of 90% of humanity. That has the support of evidence going back to the days of 1968.   The Georgia Guidestones are granite-proof since their appearance in Elberton, GA that the elite are determined to reduce the world's population, one way or another.

The moment Paul Ehrlich's book, co-authored with his wife, *'The Population Bomb'* published in 1968, and with its wide reading among academia, geo-political, economic, leaders, the world began to focus upon its war to "Depopulate" the world. I believe I have written 21 or 22 segments on **"Depopulation #1 Global Issue Since 1968"**.   As Clif High stated, *"We are in a war",* and this war will result in 2 billion dying from the actions of psychopaths determined to rule the world!

If your spiritual house is in order, there is a light in this tunnel of evil, and that will be when the Lord Jesus Christ calls us to come up and prepare for the celebration. We are at the point where Revelation 3:10 is about to be fulfilled: ***"Because thou hast kept the word of my patience, I also will keep thee from the hour of temptation, which shall come upon all the world, to try them that dwell upon the earth."***   That many Christians do not believe in a Rapture of the invisible believing church takes no precedence of what Christ Jesus said as a promise to those who do believe and place their trust in. God does not lie, and His Word is like money in the bank for which you can write a check on!

Blessings,

Pastor Bob, EvanTeachr@aol.com
www.pastorbobreid.com
http://jesusisthewaythetruththelife.com/node/22