GlobalResearch
Center for Research on Globalization

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? perspective

By Tim Hinchliffe

Theme: Intelligence

Global Research, May 07, 2021
The Sociable 7 February 2021

All Global Research articles can be read in 51 languages by activating the "Translate Website" drop down menu on the top banner of our home page (Desktop version). Visit and follow us on Instagram at @crg_globalresearch.

***

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.

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.

> "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."

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.”

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.

Cyber Polygon 2020 Emerging Trends

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 stated 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.

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 changemakers inventing the technology, so that we understand it and can regulate it sensibly and not stupidly.”

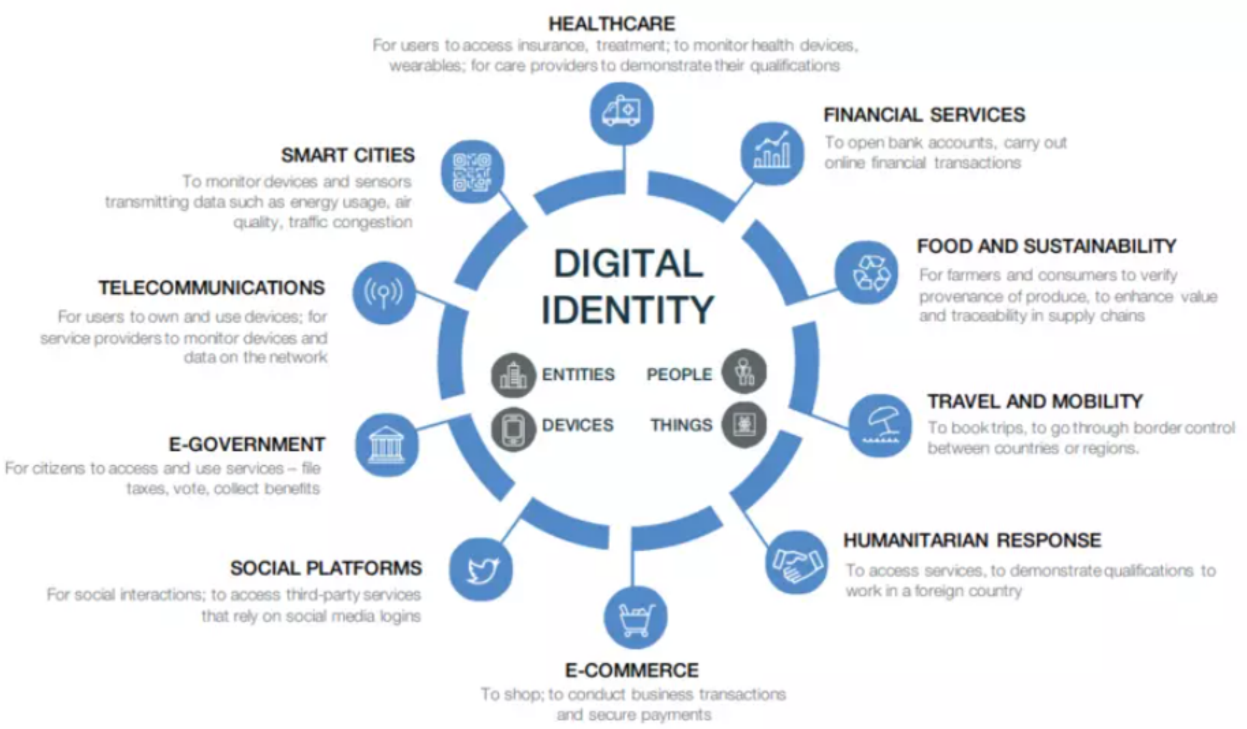
HEALTHCARE
For users to access insurance, treatment; to monitor health devices, wearables; for care providers to demonstrate their qualifications
FINANCIAL SERVICES
To open bank accounts, carry out online financial transactions
FOOD AND SUSTAINABILITY
For farmers and consumers to verify provenance of produce, to enhance value and traceability in supply chains
TRAVEL AND MOBILITY
To book trips, to go through border control between countries or regions.
HUMANITARIAN RESPONSE
To access services, to demonstrate qualifications to work in a foreign country
E-COMMERCE
To shop; to conduct business transactions and secure payments
SOCIAL PLATFORMS
For social interactions; to access third-party services that rely on social media logins
E-GOVERNMENT
For citizens to access and use services – file taxes, vote, collect benefits
TELECOMMUNICATIONS
For users to own and use devices; for service providers to monitor devices and data on the network
SMART CITIES
To monitor devices and sensors transmitting data such as energy usage, air quality, traffic congestion
DIGITAL IDENTITY
ENTITIES
PEOPLE
DEVICES
THINGS

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.

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."
>
> Gowing: "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, it's mainly directed towards the ordinary person — 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?

*

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.

Tim Hinchliffe is the editor of The Sociable. His passions include writing about how technology impacts society and the parallels between Artificial Intelligence and Mythology. Previously, he was a reporter for the Ghanaian Chronicle in West Africa and an editor at Colombia Reports in South America. tim@sociable.co

Featured image is from The Sociable

The original source of this article is The Sociable

Articles by: Tim Hinchliffe

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca