2024 Cyberattack predicted by WEF: Who is behind this? - by Redacted with Whitney Webb

This Interview aged very well. Clayton Morris published his interview with Whitney Webb in December 2023, where they discussed the potential threat of a cyber false flag attack and the actors who control cyberspace. An eye-opening interview showing the extent of control certain individuals have over the population and what kind of people they are. Definitely a must see!

[Redacted:] Well, the World Economic Forum, yes, run by Klaus Schwab, the World Economic Forum says that we will experience a massive cyber attack that will hit before the year 2025, which will lead to a massive collapse of the banking industry, infrastructure, and so much more. How do they know this? It's unbelievable. Someone who's been following this very, very closely, and it ties even more directly into the story that we've been covering here on the show about the CTI League files, the Michael Schellenberger released files about the cyber spying on Americans. We're going to get to that part of the story with independent journalist Whitney Webb, who I'm thrilled to welcome back to the show. Welcome back to Redacted.
[Whitney Webb:] Hey, it's great to be here after a long absence. Thanks for having me back.
[Redacted:] Of course, we wouldn't miss the opportunity. So thrilled to have you back here. So, let's talk about this World Economic Forum idea that the second in command at the World Economic Forum that we are going to see a massive cyber attack hitting before the year 2025 pointing out in detail this is going to happen. So you'd better be prepared for it. Why are they saying this, and who are they going to try to point the finger at?
[Whitney Webb:] Right. So, this was said at the WEF annual meeting earlier this year in January by the WEF managing director, Jeremy Juergens. And Juergens, as well as the WEF itself, has been involved in a series of simulations for several years now, that I'm sure a lot of people in your audience are familiar with, called Cyber Polygon, which has been directly affiliated with Russia's government, as well as some of Russia's biggest banks and some of the biggest commercial banks in the world. And also backed by a lot of U.S. federal agencies, which is ironic when you consider, all the stuff about alleged Russian hacks over the years. They're very willing under the guise of the WEF to collaborate with the supposed hackers responsible for everything bad for several years ago. So that's quite revealing. But aside from Cyber Polygon, there's a lot that the WEF seeks to accomplish as it relates to the cyber realm. And they've been collaborating in a lot of ways with these same big banks and also American intelligence agencies in unprecedented ways that has not really gotten any coverage over the past several years. And a lot of this is housed within a public private partnership the WEF manages is called the World Economic Forum Partnership Against Cybercrime. And this particular organization, back a few years ago, gamed out with the Carnegie Endowment, along with the Federal Reserve, the Bank of England, the European Central Bank. So, some of the biggest central banks in the world, as well as some of the biggest commercial banks in the world, like Bank of America and J. P. Morgan. How

essentially the US financial system was due to be the victim of a massive cyber attack. And if you're familiar with how things have been going in the US financial or banking system recently, things are not in a very good state at all. And regardless of there would be or will be a cyber attack in the near future, the banking and financial system in the the United States is in deep doodio. Right. So, if you're the big banks and the intelligence agencies, you want to avoid what happened after the 2008 economic crisis where there was unprecedented anger at Wall Street because the whole hope and change Obama psyop essentially is probably not going to work again. So, how do you allow that collapse to happen because it has to happen in such a way that the banks and the government are essentially blameless. Well, cyber attacks happen, and you can literally blame any nation state or group for that hack. And we know this because of what WikiLeaks published right before Julian Assange was completely silenced and then later arrested and dragged out of the Ecuadorian embassy in London. Vault 7, which revealed things like the Umbridge program, among other things that US intelligence and other intelligence agencies that are affiliated with this WEF partnership against cybercrime have the ability to place the fingerprints of any nation, the actor they wish, including Russia, China, Iran and Northkorea, any other group as well, not just nation states but their fingerprints in a hack they actually commit themselves. And this is very significant because this offers, these intelligence agencies unprecedented ability to have to conduct false flag operations in the cyber realm. And this group specifically has a lot of solutions aside from things the banking system that they cannot really justify implementing unless there is some sort of large cyber attack. So, what is the WEF partnership against cybercrime one? They're very open that they want a regulated Internet. And they're essentially seeking a policy that was efforts were made to implement during the Obama administration in the US. They called it a driver's instance for the Internet. So essentially what this public private private partnership at the WEF is pushing for. It is for every person's access to the Internet to be tied to a digital ID or a government issued ID, but presumably a digital ID just because of where government issued ID programs are all going essentially around the world. And the goal of that, of course, if your ID is linked to your Internet access, intelligence agencies know exactly what media you are consuming in terms of what you read and also what you post online. And that has been the goal for a very, very long time. So, people aren't necessarily going to consent to that unless they are made to believe that anonymity and privacy online are dangerous. So how exactly can you convince people that that needs to happen? Well, you have some sort of events where anonymous hackers do something online that causes major disruption globally. And then the consent can be manufactured through fear and panic, as is often done, that anonymity and privacy need to be eliminated, that we need to know exactly who is doing what online to prevent a calamity of that scale from ever happening again. And this is the exact solution that these guys have been cooking for a very long time. And the intelligence agencies involved are Israeli intelligence, British intelligence, and then the US Secret Service, FBI and Department of Justice. And you have several of the biggest. Banks in the country like Bank of America involved directly with this group, as well as major US tech companies like Microsoft and Amazon are partnered with all of this. And this is exactly what they're seeking. And they have all the tools to allow something like this to happen. And when you have the fact that some of these actors want a war where the US, for example, goes to war with Iran, among other things, and they have the ability to attribute. You know, cyber attacks of any scale to any entity at all. This is a big problem, because when these alleged hacks take place, whether it's claimed on Russia, Iran or China, the headline will blame these countries. But if you read the article itself, they don't actually have the evidence to make that case. They say we believe it's this country or that it's a group affiliated with this country. And their reasoning ranges from… You know, they'll say things

like we have medium probability that it's, you know, they're tied to Iran. And, you know, all these, you know, phrases that show that they don't actually have evidence. And then there's an effort to manufacture consent potentially for military action based on based on all of this stuff. So it's definitely very alarming. And people should be paying attention to it when you consider that you have the biggest banks involved, the biggest intelligence agencies and some of the biggest tech companies in the world. And another thing that this West group is seeking on is for banks, banking regulators and intelligence agencies to essentially fuse their operations under the guise of cyber security. And the more you think about that, the more insane it is. I mean, it's just an insane policy.
[Redacted:] Bringing it together under one umbrella. And of course, we even heard Nikki Haley, who's, you know certainly, neocons absolutely love Nikki Haley, right now, pushing her big time. She over the past couple of weeks has called for this lack of anonymity on the web, wants everyone to be registered as you're using the Internet. Right.
[Whitney Webb:] Yea. And so have people, you know, media personalities like Jordan Peterson, for example, has pushed for the same end of anonymity online. And you also have people like Elon Musk who bought Twitter. You know why he was buying Twitter, saying that we have to verify all humans and essentially, you know, allegedly to control the bot issue on Twitter. But there's this broad push essentially everywhere you look, from the power elite to end online anonymity. And people are obviously resisting that because it changes the nature of the Internet and supercharges the surveillance capabilities already built in to a hugely significant degree. And it's a bigger problem when you consider that the Department of Justice specifically has a pre-crime program that they've been operating since the Trump administration, called Deep, where people have literally been arrested for things, they've posted on social media. Someone was even killed, I think a few months ago, for a Facebook posts he made about Joe Biden and then was swatted and shot in the street in front of his house for posts he made on social media. Tying all of this to your government ID, considering, you know, all of those factors as it relates to U. S. Law enforcement and the Department of Justice which, again is partnered with all of these things, is an extremely awful idea. And the idea and the fact that you have all these financial services entities involved at the same time, there's this push for digital ID, not just for the Internet, but to tie your digital ID to your banking through a central bank, digital currencies or heavily regulated stable coins and deposit tokens. I mean, programmable money. I mean, the implications here are huge. And there's obviously a lot of resistance from certain quarters of the U. S. population and elsewhere against the digital ID push and the CBDC push. But have the Internet go down for X amount of time. because of some massive cyber attack and they bring it back and say, owow, we have to know who you are. And now the only way to get online is to use our digital ID. You know, they're going to get the kind of fast, rapid onboarding and mass adoption that they are seeking for those programs.
[Redacted:] Wow. Now, you believe that this cyber attack is a false flag operation. Is it your concern that Israel would want the United States to attack Iran first? That they wouldn't be able to do this? What is your reporting show on that side of it?
[Whitney Webb:] So it's not really just my reporting, you know, it's reporting from mainstream media outlets and also things that Mossad directors have openly said in interviews is that for the past 20 years, they have all, Mossad has had almost unlimited funding and energy directed towards Iran regime-change policy. And that a key component of that, according to former Mossad director, Mayor Dagan, among others, is getting the U. S. to strike Iran first. And there's been a push for a long time from the neocon sectors within the United States to have the U. S. preemptively strike Iran, among other things. And you had pushes coming from some of the biggest donors to the GOP. For example, Sheldon Adelson, when he was

still alive, was the biggest donor to the Republican Party and also to Trump, was also pushing for preemptive military action against Iran. You know, he isn't necessarily around anymore but that type of policy idea has been floated for a very long time. And after the assassination of Qasem Soleimani, the IRGC general, he was very famous, there was a rhetoric coming from Mike Pompeo when he was CIA director and also Trump that if Iran launched any sort of retaliation, including a cyber attack, they would respond with military action to Iran. So, there has been a lot of fear mongering about exactly this. And of course, it's important to keep in mind that next year, the exact year when the WEF managing director has predicted this attack is going to take lace is an election year in the United States.
[speaker:] Right.
[Whitney Webb:] And a lot of the same rhetoric about some imminent cyber attack, whether from Iran, Russia and/or China, was being utilized to a significant degree in the 2020 election as well. And you actually had, what I've argued, is an Israeli intelligence front company, a cyber security company called Cyber Reason, was gaming out and conducting simulations with DHS and some of our top law enforcement and intelligence agencies, how hackers could disrupt the 2020 election, have the election canceled and martial law declaring exactly what hackers would need to do for those conditions to be met. So, there is a lot of stuff going on in the cyber realm that not enough people are paying attention to. And the most concerning thing about this, I would argue besides the WEF warnings, is that you have a series of entities. Many of which are tied to a foreign intelligence sitting on the most critical infrastructure systems in the United States, have access to those systems. And other groups have given access to those systems to people that haven't even been vetted by our own government. It's madness.
Min. 13:54 [speaker:] And is that tied to the CTIL files, which Michael Shellenberger, journalist Michael Shellenberger, released earlier this week. We covered it extensively here on the show yesterday. The revelations that these CTIL files stand for Cyber Threat Intelligence League. And he claims that these revelations are like worse than the Twitter files, worse than Facebook and that basically it's a global plan for censorship according to these documents, the United States and UK military contractors. But I think is that all tied to this, and do you believe there's a huge piece missing from the reporting from Michael Shellenberger. It's almost like they conveniently left out one major piece of the story. Can you enlighten our audience as to what that is?
[Whitney Webb:] Yeah, absolutely. I wrote about the CTI League in August of 2020 because of this was before they really even got into the misinformation games. So, they were founded in March 2020. And their main founder in the public face of the organization for years is an Israeli intelligence operative called Ohad Zaydenberg who also has been attributed numerous times in U. S. Mainstream media reports is blaming various cyber attacks on Iran while working for a cybersecurity company tied to the Israeli government called Clear Sky. But the CTI League wasn't created. Its initial mission was was not related to targeting misalleged misinformation at all. It was an alleged volunteering to protect the critical infrastructure of U. S. Hospitals, pharmaceutical companies and health insurance companies and other corporations in the United States pro bono, for free. It's very odd that you would have a group right as a crisis hits. Right. The COVID-19 crisis starts. And you have this company run by a former intelligence agency is still collaborating with intelligence, are foreign, by the way, not American offering to protect critical American health infrastructure for free! People like this do not work for free. And the other people that co -founded this group with him…a
[Speaker:] Wowo.. So this intelligence guy really forms this company as the head of this company and says we're going to take care of American hospitals, dams, water

infrastructure…
[Whitney Webb:] Dams come later. Okay. Dams come later. But it was first health infrastructure. And they partnered with CISA [Certified Information Systems Auditor®], which is the independent agency operating under DHS (U.S. Homeland Security). That's supposed to protect critical structure, including election infrastructure. but also things like water systems, the power grid, all sorts of things like that, as well as hospitals. And the CTI League created by Zadenberg partners with them directly to protect all this critical infrastructure. Misinformation, what Schellenberger and Taibbi have covered, is the side gig of the CTI League. Their main thing is to get on all these critical infrastructure systems, allegedly to protect them. But no one knows who works for the CTI League, really, because in order to join it and get access to all of these systems, you don't have to be vetted by CISA or the U. S. federal government. You have to be vetted by Ohad Zadenberg and the other co -founders who play a much more minor role than him in the organization who are affiliated with either Microsoft or a U. S. government contractor called Okta. So, you have these guys deciding who gets access to these systems and who doesn't. But anyone could get through that, essentially. It's extremely reckless, extremely reckless. And beyond that, it's not just hospitals anymore. As you mentioned, it's expanded to dams. It's expanded to water systems and also nuclear reactors in the United States. So, you have a foreign intelligence-founded or nonprofit being offered access to all of these critical systems in the United States. It's insane. And it's not really the only company that's like this. So, the other company I mentioned earlier, Cyber Reason, that did these simulations about election doomsday with DHS and the FBI. They have access to some of the most critical infrastructure of the U. S. military. And a backdoor to all of it, essentially. And it's not run by American citizens.
[Speaker:] How is this being allowed? I mean, how is this being allowed? I mean, we know the deep connections between Israel and the United States. And we know the Israel lobby in the United States. But this goes deeper than that. And why would Michael Schellenberger leave out that part of the story? It sounds to me like a limited hangout. I mean, I know your website is called. Right? Like, I mean, this is like, you know, the distraction over here. Let's just focus on misinformation. But this other massive piece of the story is that they have access to American infrastructure. Foreign governments have access to American infrastructure. Israeli government has access to American infrastructure.
[Whitney Webb:] Well, it's not just the Israelis either because, again, we don't know who was given access through the CTI League to these systems. Any nationality can have it. We have no idea. Because they're not open about it. Yeah. It's an extremely reckless policy. It's worth pointing out, too, that the head of CISA that oversaw this partnership with CTI League is an ex-head of cybersecurity at Microsoft. And you have these Microsoft affiliations with some of the other co -founders. And, of course, Microsoft being arguably heavily compromised by Israeli intelligence, by Jeffrey Epstein and axwell. I've done a lot of reporting on that with Ghislaine Maxwell’s sisters being heavily involved with Microsoft through some of their companies. And then Jeffrey Epstein going on Microsoft Russia conferences, being very much involved, of course, with Bill Gates and also the chief technology officer of Microsoft for many years, Nathan Mervold. Just totally unreal. So, what's going on here with CTI League? I think, is very significant. And I'm very disappointed that, I mean, I would like to give Schellenberger the benefit of the doubt and just hope he was not aware of what the CTI League does beyond misinformation. But, I mean, if you go to the CTI League website, it's very obvious that they do a lot more beyond the misinformation side of things, that their focus is this alleged pro bono protection of critical American infrastructure. And what's also significant about this happening in the COVID era is that just as CTI League [Cyber Threat Intelligence League] partnership with CISA, the HHS in the U. S. cut hospital budgets that

were supposed to help pay for their cybersecurity and IT maintenance. So, you know, while all this COVID stuff is going on, they don't have people protecting their IT systems. And then this group comes along and offers their services for free. So, a lot of hospitals maybe that they did not want to have necessarily taken that offer but took it, because government policy made it essentially a necessity for them to do so. And also among, in the pharma world, they ended up partnering, you know, with Pfizer, with Merck and some of the names there as well. So, this is not just a corporate, this is not just, like the public sector that they're "protecting from cybersecurity". So, you know, given what's been revealed with the CTI League as it relates to censorship and their malfeasance there, why would they not practice similar malfeasance with their alleged protection of critical systems in the United States?
[Redacted:] I was going to say, yeah, to bring it all back to the World Economic Forum. So, if you have, if you launch this cyber attack or you hear oh, there's a cyber attack coming. I mean, it's like the perfect cover. You've literally got the assets in place to turn off critical infrastructure with your back-end team that you've already put together and then blame it on Iran. Right. I mean, is that the plan here? And then we launch attack against Iran?
[Whitney Webb:] Ohad Zaydenberg's whole career has been focused on Iran and cyber attacks. And he's just been focused on Iran his entire career within Israeli intelligence. And now after he formally left and is working for this group affiliated with, you know, Israeli government owned entities and other intelligence operatives. And a lot of his more recent attributions of cyber attacks to Iran have no evidence. He says things like "this group acts like another Iranian cyber group used to act, therefore, it must be Iranian" and he doesn't provide any more detail than that. I mean, are we going to get roped into a war over something that's so devoid of any actual evidence? But unfortunately, mainstream media reporting about cyber attacks in general, regardless of whether it's attributed to Iran or another nation. Very rarely are there any actual or tangible evidence to make that claim and so this is a very, very important point. And that's why I'm saying that, you know, they're not going to take that claim. And then even if they did, you know, there's this whole factor of Vault 7, as revealed by WikiLeaks, and that you can frame any country or any group for a cyber attack and as it is often the case when these crises happen, there is no investigation until after the fact. And often, investigation like on the 9 -11 commission, for example, is heavily compromised. So, who knows what will happen there? But it's obviously very concerning. And as far as the World Economic Forum is related, that public-private partnership I was talking about earlier, the Partnership Against Cybercrime, is led by an Israeli career spy named Tal Goldstein, who developed this policy (while Netanyahu who' is still prime minister, was prime minister back then in 2012) that operations that Mossad used to conduct in-house are now going to be conducted by private companies, particularly in the realm of cyber security. And that is then these groups, including Ohad Zaydenberg's Clear Sky and Cyber Reason were created. And a lot of them with people with continuing affiliations to Israeli intelligence. And when you consider, again, that it's a directly known and admitted policy of Israeli intelligence to get the U. S. to strike Iran first at the time that the Israeli security state determines that it's time to begin open hostilities and armed hostilities with Iran, which seems quite soon, given the conflict in Ghaza and how that's escalated and likely to escalate into a regional war, they have wanted for decades the U. S. to strike Iran first. And how will they do that? This is, I mean, I'm not saying they're definitely going to do it. But the fact that we're giving that exact government and people linked to that exact government access to our critical systems and all the means to do that is not a good idea.
[Redacted:] Right. Yeah. You don't need to. You know, it's Ockham's razor. Right. It's the simplest explanation for what's going to happen. And I hope that by having you on here and exposing this, talking about we've been warning from the very beginning of what happened

on October 7th. Watch out for false flags. Watch out for us being dragged into a regional war. Watch out for us being dragged into a war with Iran. You know, we have a long history in the United States of false flag operations going back to the Spanish-American war and before. So, this is not something new that the United States would pull off here in coordination with the Israeli government. I know you've been working very, very hard. You have some explosive new content coming out here very, very soon. We'd love to have you back on perhaps after the holidays when you when you have those reports. We always appreciate it. It's always a tour de force and you blow our minds every time you're on the show. So I just want to say thank you so much. Great to have you back on. And it's been a real pleasure to see you again.
[Whitney Webb:] Yeah, likewise. Great to be back on. Especially after such a long hiatus. So really appreciate the invite. Thank you.

Thank you so much for watching this segment here at Redacted. We are live every day at 4 p. m. Eastern time trying to share the stories that the mainstream media will not cover. You should also come over and join our community of Redacted rebels over at redacted. inc. That's our private local community where we can share exclusive content that we simply cannot share here on YouTube. Come over and join the rebellion together right now by going to redacted. Inc. We'll see you next time.

from Clayton Morris and Whitney Webb

Sources:

https://youtu.be/Y36ZEKYMvzM

https://redacted.inc/

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

This may interest you as well:

Security advice:

Unfortunately countervoices are being censored and suppressed more and more. As long as we don't report according to the ideology and interests of the corporate media, we are constantly at risk, that pretexts will be found to shut down or harm Kla.TV.

So join an internet-independent network today! Click here:
www.kla.tv/vernetzung&lang=en