Whitney Webb: Světové ekonomické fórum plánuje kybernetický útok pod falešnou vlajkou – odhalen zákeřný plán WEF! (VIDEO CZ DAB, 26 min + Přepis)

- CZ24 News | 7. prosince 2023

↓ Video s českým dabingem ↓

↓ Video v originále s českými titulky ↓

Přepis videa:

C (Claytom Morris z Redacted): Světové ekonomické fórum, které vede Klaus Schwab, tvrdí, že zažijeme masivní kybernetický útok, který nás zasáhne před rokem 2025, což povede k masivnímu kolapsu bankovního průmyslu, infrastruktury a mnohého dalšího. Jak to vědí? Je to neuvěřitelné. Někdo, kdo to velmi pozorně sleduje… A ještě více to souvisí přímo s příběhem o uniklých souborech Ligy CTI, které Michael Shellenberger zveřejnil o kybernetickém špehování Američanů. K této části příběhu se dostaneme s nezávislou novinářkou Whitney Webbovou, kterou s radostí vítám. Vítejte zpět.

WW: Ahoj, je skvělé být tu po dlouhé nepřítomnosti. Díky za pozvání.

C: Samozřejmě si nenecháme ujít příležitost. Jsem nadšený, že jste zpátky. Pojďme si tedy promluvit o té myšlence Světového ekonomického fóra, kterou vyslovil druhý nejvyšší představitel Světového ekonomického fóra, že budeme svědky masivního kybernetického útoku, který udeří před rokem 2025, podrobně poukazoval na to, že se to stane a ať se připravíme. Proč to říkají? A na koho se budou snažit ukázat prstem?

WW: Tohle řekl na výročním zasedání WEF na začátku letošního ledna výkonný ředitel WEF Jeremy Jergens. A Jergens stejně jako samotné WEF se už několik let podílí na sérii simulací, kterou určitě spousta lidí ve vašem publiku zná, nazvanou CyberPolygon, která byla přímo spojena s ruskou vládou a některými z největších ruských bank a některými z největších komerčních bank na světě a také podporována mnoha americkými federálními agenturami, což je ironické, když si uvědomíte všechen ten povyk kolem údajných ruských hackerů, jsou velmi ochotní pod záminkou WEF spolupracovat s údajnými hackery zodpovědnými za všechno špatné už několik let, takže to je docela odhalující.

Ale kromě CyberPolygonu je toho hodně, o co WEF usiluje, co se týče kybernetické sféry. A v mnoha ohledech spolupracují se stejnými velkými bankami a také americkými tajnými službami způsobem, o kterém se v posledních několika letech vůbec nepsalo. Mnoho z toho je umístěno v rámci partnerství veřejného a soukromého sektoru s názvem Partnerství Světového ekonomického fóra proti kyberkriminalitě.

Tato konkrétní organizace před několika lety společně s Carnegie Endowment, s Federálním rezervním systémem, Bank of England, Evropskou centrální bankou, a také s některými z největších obchodních společností na světě, jako je Bank of America a JP Morgan, vymyslela, jak se v podstatě

americký finanční systém měl stát obětí masivního kybernetického útoku.

Pokud víte, jak se věci v americkém finančním nebo bankovním systému v poslední době vyvíjejí, není situace vůbec dobrá. A bez ohledu na to, jestli by došlo nebo dojde v blízké budoucnosti ke kybernetickému útoku, bankovní a finanční systém v USA je v pěkné bryndě. Pokud jste velké banky a zpravodajské agentury, chcete se vyhnout tomu, co se stalo po ekonomické krizi v roce 2008, kdy na Wall Street zavládl nebývalý hněv, protože celá ta Obamova naděje a změna, v podstatě psychologická operace, už asi nebude fungovat.

Jak tedy dopustíte, aby došlo k takovému kolapsu, protože k němu musí dojít tak, aby banky a vláda byly v podstatě bez viny? No, stane se kybernetický útok a z toho hackerského útoku můžete doslova obvinit jakýkoli národní stát nebo skupinu. A víme to díky tomu, co WikiLeaks zveřejnil těsně předtím, než byl Julian Assange úplně umlčen a později zatčen a odvlečen z ekvádorské ambasády v Londýně.

Vault 7, který odhalil věci jako program Umbridge, že americké zpravodajské služby a další zpravodajské agentury, které jsou spojeny s tímto WEF partnerstvím proti kybernetické kriminalitě, mají možnost umístit otisky prstů jakéhokoli aktéra z národního státu, kterého chtějí, včetně Ruska, Číny, Íránu a Severní Koreje, jakékoli jiné skupiny, nejen národní státy… umístit jejich otisky prstů do hackerského útoku, který vlastně samy spáchají.

A to je velmi významné, protože to těmto zpravodajským agenturám nabízí bezprecedentní možnost provádět operace pod falešnou vlajkou v kybernetické oblasti. A tato skupina má spoustu řešení, kromě věcí s bankovním systémem, které nemohou ospravedlnit, pokud nedojde k nějakému velkému kybernetickému útoku, takže co chce partnerství WEF proti kybernetické kriminalitě? Velmi otevřeně říkají, že chtějí regulovaný internet, a v podstatě chtějí politiku, kterou se snažili zavést během Obamovy administrativy v USA, nazvali to řidičák pro internet.

Takže v podstatě to, co toto WEF partnerství veřejného a soukromého sektoru prosazuje, je, aby byl přístup každého člověka k internetu vázán na digitální ID nebo na průkaz totožnosti vydaný vládou, ale pravděpodobně na digitální ID už jen proto, kam všechny programy vydávání vládních ID v podstatě po celém světě směřují. A cílem je samozřejmě to, aby zpravodajské služby přesně věděly, jaká média konzumujete, pokud jde o to, co čtete a co zveřejňujete na internetu, pokud je váš průkaz totožnosti spojen s vaším přístupem na internet.

A to je cílem už velmi dlouho. Takže lidé s tím nutně nebudou souhlasit, pokud nebudou přesvědčeni, že anonymita a soukromí na internetu jsou nebezpečné. Jak přesně tedy můžete lidi přesvědčit, že k tomu musí dojít? No, stačí nějaká událost, kdy anonymní hackeři udělají něco online, co způsobí velké narušení v celosvětovém měřítku, a pak lze prostřednictvím strachu a paniky vytvořit souhlas, jak se často děje, že je třeba odstranit anonymitu a soukromí, že musíme přesně vědět, kdo co dělá online, aby se katastrofa takového rozsahu už nikdy neopakovala.

A to je přesně to řešení, které tito lidé už velmi dlouho připravují. A jsou do toho zapojeny izraelské zpravodajské služby, britské zpravodajské služby a pak americké tajné služby, FBI a ministerstvo spravedlnosti. A máte několik největších bank v zemi, jako je Bank of America, zapojených přímo do této skupiny, stejně jako velké technologické společnosti, jako je Microsoft a Amazon, které jsou partnery toho všeho, a to je přesně to, o co usilují. A mají k dispozici všechny nástroje, které jim něco takového umožňují.

A když máte skutečnost, že někteří z těchto aktérů chtějí válku, kdy USA například půjdou do války s Íránem, mimo jiné, a mají schopnost připsat kybernetické útoky jakéhokoli rozsahu jakémukoli subjektu vůbec… to je velký problém, protože když k těmto údajným útokům dojde, ať už je z nich

obviněno Rusko, Írán nebo Čína, v titulku se obviní tyto země, ale když si přečtete samotný článek, tak vlastně nemají žádné důkazy, aby to dokázali.

Říkají: Domníváme se, že je to tato země, nebo že je to skupina spojená s touto zemí. A jejich argumentace se pohybuje… řeknou věci jako, máme střední pravděpodobnost, že jsou spojeni s Íránem a všechny tyto fráze, které ukazují, že nemají důkazy, a pak je tu snaha vyrobit souhlas, potenciálně pro vojenskou akci na základě toho všeho. Lidé by tomu měli věnovat pozornost, když uvážíte, že do toho jsou zapojeny největší banky s největšími tajnými službami a největšími technologickými společnostmi.

A další věc, o kterou tato WEF skupina usiluje, je, aby bankovní regulační orgány a zpravodajské agentury v podstatě sloučily své operace pod rouškou kybernetické bezpečnosti. A čím víc o tom přemýšlíte, tím šílenější to je. Je to prostě šílená politika.

C: Spojit to pod jeden deštník. Slyšeli jsme Nikki Haleyovou, neokonzervativci teď Nikki Haleyovou naprosto milují, během posledních pár týdnů volala po tom, aby na webu nebyla anonymita, chce, aby byl každý na internetu registrovaný.

WW: Ano. A mediální personální osobnosti, jako například Jordan Peterson, prosazoval stejný konec anonymity na internetu. A máte také lidi jako Elon Musk, který koupil Twitter, a když ho kupoval, říkal, že musíme ověřit všechny lidi.

Údajně ke kontrole problému botů na Twitteru. Ale v podstatě všude, kam se podíváte, je tento široký tlak mocenské elity na ukončení online anonymity. A lidé se tomu samozřejmě brání, protože to mění povahu internetu a navyšuje možnosti dohledu, které jsou v něm už tak zabudovány v nesmírně významné míře. A je to ještě větší problém, když si uvědomíte, že ministerstvo spravedlnosti má konkrétně program, který provozuje od nástupu Trumpa pod názvem Deep, kde jsou lidé doslova zatýkáni za věci, které zveřejnili na sociálních sítích.

Někdo byl dokonce před pár měsíci zabit za příspěvky na Facebooku, které napsal o Joe Bidenovi, a pak byl přepaden a zastřelen na ulici před svým domem. Vázat to všechno na váš vládní průkaz s ohledem na všechny tyto faktory, jak se to týká amerických bezpečnostních složek a ministerstva spravedlnosti, které je partnerem tohoto všeho, je hrozný nápad.

A myšlenka, že v tom máte zapojené všechny tyto subjekty finančních služeb, zároveň existuje tlak na digitální ID nejen pro internet, ale na propojení vašeho digitálního ID s vaším bankovnictvím. Prostřednictvím digitální měny nebo silně regulované stabilní mince a vkladové tokeny, programovatelné peníze. Důsledky jsou zde obrovské.

A je zřejmé, že v určitých částech obyvatelstva USA i jinde existuje velký odpor proti prosazování digitálního ID a CBDC, ale nechat internet na určitý čas vypadnout kvůli nějakému masivnímu kybernetickému útoku a oni ho obnoví a řeknou: No, musíme vědět, kdo jste. Jediný způsob, jak se dostat na internet, je použít náš digitální ID. Dosáhnou tak rychlého nástupu a masového přijetí, o které u těchto programů usilují.

C: Wow. Domníváte se, že tento kybernetický útok je operací pod falešnou vlajkou. Obáváte se, že by Izrael chtěl, aby Spojené státy zaútočily na Írán jako první, že by toho nebyly schopny? Co o tom ukazuje vaše zpravodajství?

WW: To není jen moje zpravodajství. Je to zpravodajství z mainstreamových médií a také věci, které ředitelé Mossadu otevřeně řekli v rozhovorech, že za posledních 20 let měl Mossad téměř neomezené finanční prostředky a energii zaměřenou na politiku změny režimu v Íránu. A že její klíčovou součástí je podle bývalého ředitele Mossadu Meira Dagana mimo jiné to, aby USA udeřily

na Írán jako první.

A neokonzervativní kruhy v USA již dlouho usilují o to, aby USA preventivně udeřily. A měli jste tlaky, které přicházely od některých z největších dárců GOP, například Sheldon Adelson, když ještě žil, největší dárce Republikánské strany a také Trumpa, také prosazoval preventivní vojenskou akci proti Íránu.

On už tu nutně není, ale tento typ politické myšlenky se objevoval velmi dlouho. A po zavraždění Kásim Sulejmáního, generála IRGC, který byl velmi známý, se objevila rétorika pocházející od Mikea Pompea, když byl ředitelem CIA, a také od Trumpa, že pokud Írán zahájí jakýkoli druh odvety, včetně kybernetického útoku, odpoví vojenskou akcí proti Íránu. Takže přesně o tomhle se hodně hovořilo a šířil se strach. A samozřejmě je důležité mít na paměti, že příští rok, přesně v roce, kdy výkonný ředitel WEF předpověděl, že k tomuto útoku dojde, jsou volby na prezidenta v USA.

A spousta té samé rétoriky o nějakém hrozícím kybernetickém útoku, ať už z Íránu, Ruska a nebo Číny, byla značné míry využita i ve volbách v roce 2020. A vy jste vlastně měli to, co je podle mě izraelská zpravodajská krycí společnost pro kybernetickou bezpečnost s názvem Cyberreason, která prováděla simulace s DHS a některými našimi špičkovými bezpečnostními a zpravodajskými orgány, jak by hackeři mohli narušit volby v roce 2020, nechat volby zrušit a vyhlásit stanné právo, co přesně by hackeři museli udělat, aby tyto podmínky byly splněny.

V kybernetické oblasti se tedy děje spousta věcí, kterým nevěnuje pozornost dost lidí. A nejvíce znepokojující na tom, kromě varování WEF je, že máte řadu subjektů, z nichž mnohé jsou napojeny na zahraniční zpravodajské služby, které jsou napojeny na naše systémy nejkritičtější infrastruktury ve Spojených státech, mají k těmto systémům přístup a jiné skupiny poskytly přístup k těmto systémům lidem, kteří ani nebyli prověřeni naší vlastní vládou. Je to šílenství.

C: A je to napojeno na soubory CTIL, které novinář Michael Shellenberger zveřejnil na začátku tohoto týdne. Odhalení, že tyto soubory CTIL, což znamená Liga kybernetických hrozeb, a on tvrdí, že tato odhalení jsou horší než Twitter Files, horší než Facebook. A podle těchto dokumentů v podstatě mají globální plán na cenzuru. Spojené státy a britští vojenští dodavatelé. Souvisí to s tím? Podle tebe v reportáži Michaela Shellenbergera chybí obrovský kus. Je to skoro, jako by příhodně vynechali jeden důležitý kousek tohoto příběhu. Můžete nám říct, o co jde?

WW: Ano, o Lize CTI jsem psala v srpnu 2020. To bylo ještě předtím, než se skutečně pustili do dezinformačních her. Takže byli založeni v březnu 2020. A jejich hlavním zakladatelem a veřejnou tváří organizace je už léta operativec izraelské tajné služby Ohad Seidenberg, kterého americká média často citovala s tím, že obviňuje Írán z různých kybernetických útoků, zatímco pracoval pro kyberbezpečnostní společnost napojenou na izraelskou vládu s názvem ClearSky.

Ale Liga CTI nebyla vytvořena… její původní poslání se vůbec netýkalo cílení údajných dezinformací. Šlo o údajně dobrovolnou ochranu kritické infrastruktury amerických nemocnic, farmaceutických společností a zdravotních pojišťoven a dalších korporací v USA, a to zdarma. Je velmi zvláštní, že byste měli skupinu hned, jak udeřila krize COVID-19. A vy máte tuto společnost, kterou vede „bývalý" agent tajné služby, který stále spolupracuje se zpravodajskými službami.

Mimochodem zahraničními, nikoliv americkými, a nabízí ochranu kritické americké zdravotnické infrastruktury „zdarma". Takoví lidé nepracují zadarmo a další lidé, kteří s ním tuto skupinu spoluzaložili…

C: Takže agent izraelské tajné služby založil tuto společnost jako šéf této společnosti a říká, že se postará o americké nemocnice, přehrady, vodní infrastrukturu.

WW: Přehrady přišly později… ale nejdřív to byla zdravotní infrastruktura. A oni se spojili se CISA, což je nezávislá agentura fungující pod DHS, která má chránit kritickou infrastrukturu včetně volební infrastruktury, ale také věci jako vodní systémy, elektrickou síť, všechny možné podobné věci, stejně jako nemocnice, a Liga CTI vytvořená Seidenbergem s nimi přímo spolupracuje, aby chránila tuto „kritickou" infrastrukturu. Dezinformace, o kterých informovali Shellenberger a Taibbi, je vedlejším úkolem Ligy CTI. Jejich hlavním úkolem je dostat se do všech těchto systémů kritické infrastruktury a údajně je chránit.

Nikdo však neví, kdo pro Ligu CTI ve skutečnosti pracuje, protože abyste se k ní mohli připojit a získat přístup do všech těchto systémů, nemusíte být prověřeni agenturou CISA nebo vládou USA, ale musíte být prověřeni Ohadem Seidenbergem a dalšími spoluzakladateli, kteří v této organizaci hrají menší roli než on a kteří jsou spojeni buď s Microsoftem, nebo s americkým vládním dodavatelem jménem Okta. Takže tito lidé rozhodují o tom, kdo získá přístup do těchto systémů, a kdo ne. V podstatě by se do nich mohl dostat kdokoliv. Je to extrémně bezohledné.

A kromě toho už to nejsou jen nemocnice. Rozšiřuje se to na přehrady, vodovodní systémy a také na jaderné reaktory ve Spojených státech. Takže máte neziskovou organizaci založenou zahraniční zpravodajskou službou, které je nabízen přístup ke všem těmto kritickým systémům v USA. Je to šílené. A ve skutečnosti to není jediná společnost, která je taková. Druhá společnost, o které jsem se zmínila dříve, Cyberreason, která dělala simulace o volebním konci světa s DHS a FBI a co já vím, má přístup k některé z nejkritičtějších infrastruktur americké armády. A v podstatě do toho všeho mají zadní vrátka. Neřídí to američtí občané.

C: Jak je to možné? Víme o hlubokých vazbách mezi Izraelem a Spojenými státy a známe izraelskou lobby ve Spojených státech, ale tohle je něco hlubšího. A proč Michael Shellenberger vynechal tuto část příběhu? Mně to připadá jako omezené odhalení. Rozptýlení tady, pojďme se zaměřit na dezinformace. Ale ten druhý obrovský kus příběhu je, že mají přístup k americké infrastruktuře, cizí vlády mají přístup k americké infrastruktuře, izraelská vláda má přístup k americké infrastruktuře.

WW: No, nejsou to ani jenom Izraelci, protože opět nevíme, kdo dostal přes Ligu CTI přístup do těchto systémů. Mohla ho mít jakákoli národnost. Nemáme tušení, protože o tom nejsou otevření. Je to nesmírně bezohledná politika. A také šéf agentury CISA, který dohlížel na toto partnerství s Ligou CTI, je bývalý šéf kybernetické bezpečnosti v Microsoftu.

A máte vazby na některé další spoluzakladatele a samozřejmě Microsoft, který je pravděpodobně silně kompromitován izraelskou rozvědkou, Jeffrey Epsteinem a Maxwellovou. Sestry Ghislaine Maxwellová jsou silně napojeny na Microsoft prostřednictvím některých svých společností, a pak Jeffrey Epstein chodil na konference Microsoftu v Rusku, byl mnoho let velmi provázán s Billem Gatesem a také technologickým ředitelem Microsoftu Nathan Myhrvoldem. Prostě naprosto neskutečné. To, co se tady děje s Ligou CTI, je podle mě velmi významné.

A jsem velmi zklamaná… ráda bych dala Shellenbergerovi presumci neviny a jen doufám, že si nebyl vědom toho, co Liga CTI dělá nad rámec dezinformací. Když se ale podíváte na web Ligy CTI, je velmi zřejmé, že dělají mnohem víc než jen dezinformační stránku věcí. Že jejich hlavním zaměřením je tato údajná „pro bono" ochrana kritické americké infrastruktury. A co je také významné na tom, že se to děje v éře COVID, je to, že stejně jako partnerství Ligy CTI s agenturou CISA, ministerstvo zdravotnictví v USA snížilo rozpočty nemocnic, které měly pomoci zaplatit jejich kybernetickou bezpečnost a IT údržbu.

Ve stejné době, kdy se dějí všechny ty věci kolem COVIDu, nemají lidi, kteří by chránili jejich IT systémy. A pak se objeví tato skupina a nabízí své služby zdarma. Takže spousta nemocnic nejspíše tu nabídku přijala, protože vládní politika z toho udělala v podstatě nutnost, aby to udělaly. A také ve

farmaceutickém světě skončili jako partneři Pfizeru, Mercku a dalších.

Není to jen veřejný sektor, který „chrání" kybernetickou bezpečností. Vzhledem k tomu, co bylo odhaleno s Ligou CTI, co se týče cenzury a jejich nekalých praktik, proč by nepraktikovali podobné nekalé praktiky s jejich údajnou ochranou kritických systémů v USA?

C: Ano, abychom se vrátili ke Světovému ekonomickému fóru. Pokud zahájíte tento kybernetický útok… slyšíte, že se chystá kybernetický útok. Je to dokonalé krytí, máte k dispozici prostředky k vypnutí kritické infrastruktury s vaším týmem v pozadí, a pak to svedete na Írán. Je to plán? Zahájit útok proti Íránu?

WW: Ohad Seidenberg se celou svou kariéru zaměřuje na Írán a kybernetické útoky. A právě na Írán se zaměřoval celou svou kariéru v rámci izraelské rozvědky, a také nyní poté, co formálně odešel a pracuje pro tuto skupinu spojenou izraelskými vládními subjekty a dalšími zpravodajskými agenty. A spousta jeho nedávných připsání kybernetických útoků Íránu nemá žádné důkazy.

Říká věci jako… tato skupina se chová stejně, jak se chovala jiná íránská kybernetická skupina, proto musí být íránská, a neuvádí žádné další podrobnosti. Necháme se zatáhnout do války kvůli něčemu, co je bez jakýchkoli skutečných důkazů? Ale bohužel mainstreamová média, která informují o kybernetických útocích obecně, bez ohledu na to, zda jsou připisovány Íránu nebo jiné zemi, mají jen velmi zřídka nějaké hmatatelné důkazy pro toto tvrzení.

A i kdyby je měly, je tu celý ten faktor Vault 7, jak ho odhalil WikiLeaks, a to, že na jakoukoli zemi nebo skupinu můžete hodit kybernetický útok. A jak už to tak bývá, když dojde k takovým krizím, tak se vyšetřuje až po tom, co k tomu dojde. A často ta vyšetřování, jako například Komise pro 11. září, jsou silně kompromitovaná. Kdo ví, co se tam stane, ale je to znepokojující.

A co se týče Světového ekonomického fóra, tak to partnerství veřejného a soukromého sektoru proti kybernetické kriminalitě vede kariérní izraelský špion Tal Goldstein, který vypracoval tuto politiku, zatímco Netanjahu, který je stále premiérem, byl premiérem tehdy v roce 2012, že operace, které dříve Mossad prováděl ve vlastní režii, budou nyní provádět soukromé společnosti, zejména v oblasti kybernetické bezpečnosti.

A právě tehdy vznikly tyto skupiny, včetně ClearSky Ohada Seidenberga a Cyberreason. A mnohé z nich s lidmi s přetrvávajícími vazbami na izraelskou rozvědku. A když si znovu uvědomíte, že je přímo známou a přiznanou politikou izraelské rozvědky přimět USA, aby udeřily na Írán jako první v době, kdy usoudí, že je čas zahájit otevřené nepřátelství a ozbrojené boje s Íránem, což se zdá být poměrně brzy, vzhledem ke konfliktu v Gaze a k tomu, jak se vyostřil a pravděpodobně přeroste v regionální válku. Již desítky let chtějí, aby USA udeřily na Írán jako první a jak to udělají? Neříkám, že to určitě udělají. Ale to, že přesně této vládě a lidem napojeným na tuto vládu dáváme přístup k našim kritickým systémům a všem prostředkům, jak to udělat, není dobrý nápad.

C: Ano. Je to Occamova břitva. Je to nejjednodušší vysvětlení toho, co se stane. A já doufám, že tím, že jste tady a odhalujete to, od samého začátku jsme varovali před tím, co se stalo 7. října: Pozor na falešné vlajky, pozor na to, že nás zatáhnou do regionální války, pozor na to, že nás zatáhnou do války s Íránem. V USA máme dlouhou historii operací pod falešnou vlajkou, která sahá až do španělsko-americké války a před ni, takže to není nic nového, co by Spojené státy v koordinaci s izraelskou vládou provedly.

Whitney Webbová, vím, že jste pracovala velmi tvrdě, máte výbušný, nový obsah, který se objeví velmi brzy. Rádi vás přivítáme znovu, možná po prázdninách, až budete mít ty zprávy, vždycky si toho vážíme a pokaždé, když jste v pořadu, nám vyrazíte dech. Takže vám chci jen moc poděkovat. Je

skvělé, že jste se vrátila. A bylo mi opravdovým potěšením vás znovu vidět.

WW: Jo, taky. Je skvělé být zpátky, obzvlášť po tak dlouhé pauze. Opravdu si vážím pozvání. Děkuji.
Překlad: David Formánek

AUTOR: Whitney Webb

PŘEKLAD: David Formánek/otevrisvoumyslCz

ZDROJ