

Grootschalige cyber veiligheidsoefening op verkiezingsdag in Amerika

Gepubliceerd: donderdag, 24 oktober 2024 10:49



Op 5 november aanstaande mogen de Amerikanen naar de stembus om zo te bepalen wie zich president van Amerika mag noemen.

Het is natuurlijk ook volkomen toevallig dat er op die dag een grootscheepse cyberveiligheidsoefening plaats vindt.

Als je aan een willekeurige Nederlander op straat zou vragen wat hij/zij vindt van het feit dat er net op de dag van de Amerikaanse presidentsverkiezingen een grootschalige cyber veiligheidsoefening zal plaatsvinden, dan krijg je waarschijnlijk als antwoord: ‘Nou en?’

Als ze een lezer van deze website dat gevraagd zouden hebben, dan was het antwoord waarschijnlijk geweest: ‘Hoogst verdacht en waarschijnlijk geen toeval want we hebben in het verleden gezien hoe bij iedere false flag operatie van de sekte er ook tegelijkertijd oefeningen worden gehouden.

Iemand die ook geschrokken is van het bericht is journalist Jon Rappoport.

Hij schrijft onder [andere het volgende](#):

Achtergrond:

“AFCEA [Armed Forces Communications & Electronics Association International] Atlanta [Chapter] Homeland Security Conference on Critical Infrastructure, 6-7 november 2024, met een grootschalige cyberbeveiligingsoefening op 5 november 2024”.

Op 5 november, verkiezingsdag, zal er een speciale cyberbeveiligingsoefening zijn op de conferentie.

Luister goed. De oefening wordt beschreven als een grootschalig interactief evenement, met deelnemers van federale, staats-, provincie- en stadsoverheidsinstanties, de academische wereld en het bedrijfsleven.

De oefening simuleert een cyberaanval op “kritieke infrastructuur”.

Dat klopt. Het is een zogenaamde “Jack Voltaic”-oefening, die ontwikkeld is om reacties op aanvallen op grote infrastructuren te testen.

Grootschalige cyber veiligheidsoefening op verkiezingsdag in Amerika

Gepubliceerd: donderdag, 24 oktober 2024 10:49

Wel heel erg bijzonder om de oefening te plannen op de dag van de verkiezingen.

Nogal vreemd om een oefening te houden die een cyberaanval op kritieke infrastructuur simuleert op verkiezingsdag, vooral omdat elektronisch stemmen in het hele land een stuk kritieke infrastructuur IS.

Als kwaadwillenden zouden willen knoeien met elektronisch stemmen, dan zou deze oefening een redelijke dekmantel en methode creëren.

Als die kwaadwillenden het elektronisch stemmen wilden manipuleren en een excuus nodig hadden om “afwijkingen” bij het tellen van de stemmen te verklaren, of om een plotselinge sluiting van belangrijke stemlokalen te verklaren, dan zou de cyberoefening die verklaringen geven.

“Nou, zie je, er was een tijdelijke storing door het feit dat, parallel aan het stemmen op de verkiezingsdag, Homeland Security een cruciale maar niet gerelateerde cyberoefening deed, en 'de onderlinge communicatie was niet optimaal,' bij wijze van spreken...”

“Niets te zien hier, het probleem werd verholpen en de oefening ging door, net als het tellen van de stemmen. Dit soort dingen gebeuren af en toe. Homeland Security verzekert ons dat het stemmen niet werd belemmerd...” ‘slechts een geval van miscommunicatie’

“Natuurlijk zijn er mensen die geruchten en samenzweringstheorieën verspreiden over 'veranderde stemmentellingen'. Deze beschuldigingen zijn volledig ongegrond. De oefening van Homeland Security had niets te maken met het tellen van de stemmen...” ‘slechts een geval van miscommunicatie’.

“Beschuldigingen van stemvervalsing zijn zeer ernstig. Ze zouden in sommige gevallen beschouwd kunnen worden als een vorm van verkiezingsinmenging (als wij, de regering, mensen het zwijgen willen opleggen en willen verdoezelen wat we echt aan het doen zijn)...” ‘slechts een geval van miscommunicatie’.

Maar nogmaals, het plannen van een grote cyberoefening van Homeland Security waarbij een aanval op kritieke infrastructuur wordt gesimuleerd? OP DE DAG VAN DE VERKIEZINGEN? Echt waar?

Het is op zijn minst een geweldige manier voor de overheid om mensen de overheid te laten wantrouwen.

Grootschalige cyber veiligheidsoefening op verkiezingsdag in Ameri

Gepubliceerd: donderdag, 24 oktober 2024 10:49

Misschien bent u geïnteresseerd in het lezen van het Wikipedia-artikel voor de groep AFCEA, die de komende novemberconferentie en de cyberbeveiligingsoefening sponsort.

Er staat onder andere:

“Armed Forces Communications & Electronics Association International (AFCEA), opgericht in 1946, is een non-profit ledenvereniging ten dienste van het leger, de overheid, de industrie en de academische wereld als een forum voor het bevorderen van professionele kennis en relaties op het gebied van communicatie, informatietechnologie, inlichtingen en wereldwijde veiligheid. AFCEA biedt een forum voor militaire, overheids-, academische en industriële gemeenschappen met in totaal meer dan 30.000 leden. AFCEA ondersteunt lokale chapters, sponsort evenementen, publiceert een tijdschrift, promoot STEM-onderwijs en biedt ledenvoordelen.

“SIGNAL, niet te verwarren met het Duitse Signal magazine, is een maandelijks [AFCEA] internationaal nieuwsmagazine gericht op overheids-, militaire en industriële professionals die actief zijn op het gebied van informatietechnologie en inlichtingen. Het tijdschrift is gestart in 1946. Onder de onderwerpen die in het tijdschrift aan bod komen zijn commando, controle, communicatie, computers, inlichtingen, surveillance en verkenning (C4ISR); informatiebeveiliging; cyberbeveiliging; onderzoek en ontwikkeling; kunstmatige intelligentie, machine learning, big data, cloud-technologieën, elektronica; en binnenlandse veiligheid.”