James Corbett: When False Flags Go Virtual

When False Flags Go Virtual

by **James Corbett**, *Corbett Report*
November 29, 2020

Imagine this: you wake up to the blaring of your alarm clock and immediately reach for your smartphone to scroll your Insta feed before getting out of bed. But instead of the usual delightful and informative Instagram posts, today you're greeted by a "server not found" error.

Deciding that it's too early in the morning to deal with this, you hop in the shower . . . but for some reason Alexa won't play your Spotify playlist through your bathroom smart speakers. You have to shower in silence like a luddite.

Getting frustrated, you head downstairs for breakfast. You prop your iPad up next to you and go to check your email while stuffing your face with your morning bowl of Cheeri-GMOs (now with extra HFCS!) but you're not getting any new messages. You turn on your smart TV and navigate to YouTube so you can catch up on all the latest news from MSNBC, but all you get is the never ending spiral of the spinning "loading" wheel.

Twitter? Down.

Facebook? No luck.

Reddit? Forget it!

Increasingly desperate, you try in vain to remember how to turn on your regular terrestrial TV. Then you recall you have something collecting dust in a closet somewhere: a radio. You

turn it on, fumble with the dial, and find a station just in time to hear the announcement:

". . . is claiming responsibility for the outage. Once again, widespread outages across a range of internet services is sweeping the globe this morning, as a shadowy new terror group emerges to take responsibility . . ."

Suddenly, your phone starts making a strange sound. You don't know what it's doing at first, until you realize it's ringing. One of your friends is *calling* you. On the phone. Not texting, tweeting, messaging or snapchatting. Actually calling you.

"Hello?"

"Hey Norm! You hear about the big news? Internet's down!"

"Yeah."

"They say it's some kind of new terror group. Cybeterrorists In Action. C.I.A. for short. Sounds pretty scary."

. . . Oh, OK, I'll stop teasing. Of course this doesn't describe *you* or *your* daily routines, dear reader. I know you're the clued-in, switched-on sort who peruses The Corbett Report and avoids normie internet sites like the plague (the real plague, not this ginned-up COVID cold).

But don't scoff at the scenario. A scene like this one could play out one day for billions of Normie McNormesons around the world. And when it does, there will already be a plan in place for changing the internet as we know it.

As I know you know, the transition from the homeland security state to the biosecurity state that I documented in COVID-911 raises the specter of false flag bioterrorism. But there are other vectors for false flag attacks that could cause massive disruption to our lives, and, like every spectacular false flag event, increase the power and control of the deep state. In this case, I'm thinking of false flag

cyberterrorism.

The idea of a "cyber 9/11" coming along to disrupt the internet has been around since the actual 9/11 occurred. Back in 2003, even as the Pentagon was feverishly drafting its plans to "fight the net" as if it were "an enemy weapons system," Mike McConnell, the ex-director of the National Security Agency (NSA), was fearmongering over the possibility of a cyber attack "equivalent to the attack on the World Trade Center" if a new institution were not created to oversee cybersecurity. In the following years, report after report continued to use the horror of 9/11 as a way of fueling public hysteria over cyberterrorism until just such a US Cyber Command was created.

But the creation of CYBERCOM did not end the cyber threat anymore than the creation of the Department of Homeland Security ended the terror threat, and for precisely the same reason: the *real* terror threat doesn't come from the cave-dwelling terrorists that the politicians tell us to be afraid of. No, the real terror threat comes from the very agencies that have been tasked with "saving" the public from the terrorist bogeymen.

Case in point: Stuxnet. As you might recall, Stuxnet was a military-grade cyberweapon co-developed by the United States and Israel that specifically targeted Iran's nuclear enrichment facility at Natanz. As we later learned, Stuxnet was only one part of a full-scale military cyberattack against Iran codenamed Nitro Zeus.

Yes, to the surprise of absolutely no one, the largest and costliest cyberweapon ever developed (or at least officially acknowledged) was not the product of an Al-CIA-da cyberterror group or even the dreaded "Russian hackers," but the militaries of the US and Israel. Neither should it be surprising to learn that the intelligence agencies have crafted ways of making such cyberweapons *appear* to have been

created by other entities, which is a functionality that is essential to any false flag attack.

We know, for example, that the CIA has already developed the Marble Framework, an anti-forensic tool that "might be used to disguise the CIA's own hacks to appear as if they were Russian, Chinese, or from specific other countries." In other words, the CIA has spent time and energy developing a way to pin the blame for its own cyberweapons on its enemies. Although the CIA obviously will not confirm why, how or even if Marble has been deployed in the past, there is no other explanation for its existence: it is a tool for enabling virtual false flag terrorism.

This is important because, exactly as the Patriot Act was already ready and waiting in the wings pre-9/11, so, too, is an "iPatriot Act" ready and waiting in the wings for a "cyber 9/11" to come along and justify its enactment

We do not have to speculate about this. It was confirmed by Harvard Law professor Lawrence Lessig at a conference in 2008. "I had dinner once with Richard Clarke at the table," he told the audience at Fortune's Brainstorm Tech conference in Half Moon Bay, California. "And I said, 'Is there an equivalent to the Patriot Act – an iPatriot Act – just sitting, waiting for some substantial event? Just waiting for them to come have the excuse for radically changing the way the Internet works?' And he said, 'Of course there is' – and I swear this is what he said – 'and Vint Cerf is not going to like it very much.'"

Keep in mind that the Richard Clarke who told Lessig about the iPatriot Act is the same Richard Clarke who came out after the death of Michael Hastings to note that intelligence agencies have ways to remotely hijack cars, steer people to their deaths and disguise their tracks well enough to "get away with it." Also keep in mind that Joe Biden likes to brag about having written the [regular] Patriot Act in 1994.

So what kinds of things might be contained in such an iPatriot Act? Once again, we don't have to speculate. Various government officials have talked about their wish list for an internet clampdown in recent years.

- In March of 2009, Senator Jay Rockefeller opined during a subcommittee hearing that the internet is proving to be such a threat to America's national security that it would have been better if it had never existed.
- In June of 2010, Senator Joe Lieberman stated that he believed the US needed the same ability to shut down the internet as China currently has.
- Also in 2010, Microsoft Senior Advisor and Bilderberg attendee Craig Mundie called for the creation of a "World Health Organization for the internet" and suggested creating government-issued licenses to authorize internet usage.
- In 2011, Bill Clinton advocated the idea that the US government create an agency for "fact-checking" websites on the internet.
- In 2015, the National Institute of Standards and Technology (yes, *that* NIST) unveiled the "Trusted Identities Group," part of a national strategy for standardizing online identification systems.

Given all of this, it is not hard to imagine how a cyberterror event may play out: A cataclysmic attack on the internet's infrastructure massively disrupts people's online lives for a period of days or weeks. Social media is inaccesible. Online banking and shopping is halted. All news and information during the internet blackout comes from the old, controlled dinosaur media. A shocked and distressed public learn that the Russians (or whatever *bogeyman du jour* is convenient) are being blamed for the attack. In order to prevent such a thing from reoccurring, emergency legislation is passed in the US (and, coincidentally, in all other Western nations) requiring proof of identity to use any and all internet services.

In one fell swoop, not only would the last vestiges of internet anonymity be eliminated, but a key part of the erection of the social credit control grid would be in place. Now, just like in China, all of your online activity would be tied directly to your social credit score. Lieberman must be wetting his pants in anticipation.

Of course, this is not to say that the internet as we've known it would be gone altogether if such a scenario were to play out. In a network that was literally designed to be accessible and usable in the wake of any cataclysm, even nuclear holocaust, there will always be alternative ways of getting online access. There will be pirate internet and mesh networks and dweb sites and peer-to-peer protocols like LBRY that will be accessible to anyone able and willing to put in the effort to learn about such technologies. But the Normie McNormieson we met in the imaginary tale at the beginning of this article would be forever cut off from the free and open internet of old. (Good thing we're not Normie McNormieson, huh?)

As ever, it is important to know about these false flag possibilities so that when a spectacular cyberterror event takes place we are not railroaded into a phony solution that will serve only to increase the power and control of the *real* terrorists. And, in the meantime, it is important to be researching and preparing ourselves for just such an event so that, regardless of whether it happens as predicted or not, we will be less dependent on the systems of control that are increasingly defining the normie internet.

---

newsletter, sign up to become a member of the website.