



# Digital Kill Switches: How Tyrannical Governments Stifle Political Dissent



John Whitehead

No president from either party should have the [sole power to shut down or take control of the internet or any other of our communication channels](#) during an emergency. — *Senator Rand Paul*

What's to stop the U.S. government from throwing the kill switch and shutting down phone and internet communications in a time of so-called crisis?

After all, [it's happening all over the world](#).

Communications kill switches have become [tyrannical tools of domination and oppression](#) to stifle political dissent, shut down resistance, forestall election losses, reinforce military coups, and keep the populace isolated, disconnected and in the dark, literally and figuratively.

As *The Guardian* [reports](#), "From Ukraine to Myanmar, government-run internet outages are picking up pace around the world. In 2021, there were 182 shutdowns in 34 countries.... Countries across Africa and Asia have turned to shutdowns in a bid to control behaviour, while India, largely in the conflict-ridden region of Jammu and Kashmir, plunged into digital darkness more times than any other last year.... Civil unrest in Ethiopia and Kazakhstan has triggered internet shutdowns as governments try to prevent political mobilisation and stop news about military suppression from emerging."

In an internet-connected age, killing



the internet is tantamount to bringing everything—communications, commerce, travel, the power grid—to a standstill.

Tyrants and would-be tyrants rely on this [“cloak of darkness”](#) to advance their agendas.

In Myanmar, for example, the internet shutdown came on the day a newly elected government was to have been sworn in. That’s when the military staged a digital coup and seized power. Under cover of a communications blackout that cut off the populace from the outside world and each other, the junta [“carried out nightly raids](#), smashing down doors to drag out high-profile politicians, activists and celebrities.”

These government-imposed communications shutdowns serve to not only isolate, terrorize and [control the populace](#), but also [underscore the citizenry’s lack of freedom in the face of the government’s limitless power](#).

Yet as University of California Irvine law professor David Kaye explains, these kill switches are no longer exclusive to despotic regimes. They have [“migrated into a toolbox for governments that actually do have the rule of law.”](#)

This is what digital authoritarianism looks like in a technological age.

[Digital authoritarianism](#), as the Center for Strategic and International Studies cautions, involves the use of information technology to surveil, repress, and manipulate the populace, endangering human rights and civil liberties, and co-opting and corrupting the foundational principles of democratic and open societies,



Written by [John and Nisha Whitehead](#) on January 20, 2024

---

“including freedom of movement, the right to speak freely and express political dissent, and the right to personal privacy, online and off.”

For those who insist that it can't happen here, it can and [it has](#).

In 2005, [cell service was disabled](#) in four major New York tunnels, reportedly to avert potential bomb detonations via cell phone.

In 2009, those attending President Obama's inauguration had their [cell signals blocked](#)—again, same rationale.

And in 2011, San Francisco commuters had their [cell phone signals shut down](#), this time, to thwart any possible protests over a police shooting of a homeless man.

With shutdowns becoming [harder to detect](#), who's to say it's not still happening?

Although an internet kill switch is broadly understood to be a complete internet shutdown, it can also include a broad range of restrictions such as [content blocking, throttling, filtering, complete shutdowns, and cable cutting](#).

As Global Risk Intel [explains](#):

Content blocking is a relatively moderate method that blocks access to a list of selected websites or applications. When users access these sites and apps, they receive notifications that the server could not be found or that access was denied by the network administrator. A more



subtle method is throttling. Authorities decrease the bandwidth to slow down the speed at which specific websites can be accessed. A slow internet connection discourages users to connect to certain websites and does not arouse immediate suspicion. Users may assume that connection service is slow but may not conclude that this circumstance was authorized by the government. Filtering is another tool to censor targeted content and erases specific messages and terms that the government does not approve of.

How often do most people, experiencing server errors and slow internet speeds, chalk it up to poor service? Who would suspect the government of being behind server errors and slow internet speeds?

Then again, this is the same government that has subjected us to [all manner of encroachments on our freedoms](#) (lockdowns, mandates, restrictions, contact tracing programs, heightened surveillance, censorship, overcriminalization, shadow banning, etc.) in order to fight the COVID-19 pandemic, preserve the integrity of elections, and combat disinformation.

These tactics have become the tools of domination and oppression in an internet-dependent age.

It really doesn't matter what the justifications are for such lockdowns.



No matter the rationale, the end result is the same: an expansion of government power in direct proportion to the government's oppression of the citizenry.

According to Global Risk Intel, there are [many motives behind such restrictions](#):

For instance, the kill switch serves to censor content and constrain the spread of news. This particularly concerns news reports that cover police brutality, human rights abuses, or educational information. Governments may also utilize the kill switch to prevent government-critical protestors from communicating through message applications like WhatsApp, Facebook, or Twitter and organizing mass demonstrations. Therefore, internet restrictions can provide a way of regulating the flow of information and hindering dissent. Governments reason that internet limitations help stop the spread of fake news and strengthen national security and public safety in times of unrest.

In this age of manufactured crises, emergency powers and technofascism, the government already has the know-how, the technology and the authority.



Now all it needs is the “right” crisis to flip the kill switch.

This particular kill switch can be traced back to the [Communications Act of 1934](#). Signed into law by President Franklin D. Roosevelt, the Act [empowers the president to suspend wireless radio and phone services](#) “if he deems it necessary in the interest of national security or defense” during a time of “war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States.”

In the event of a national crisis, the president has a veritable arsenal of emergency powers that override the Constitution and can be [activated at a moment’s notice](#). These range from imposing martial law and suspending habeas corpus to shutting down all forms of communications, restricting travel and implementing a communications kill switch.

That national emergency can take any form, can be manipulated for any purpose and can be used to justify any end goal—[all on the say so of the president](#).

The seeds of this ongoing madness were sown several decades ago when George W. Bush stealthily issued two presidential directives that granted the president the power to unilaterally declare a national emergency, which is loosely defined as “[any incident, regardless of location, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the U.S. population, infrastructure, environment, economy, or government functions.](#)”



Written by [John and Nisha Whitehead](#) on January 20, 2024

---

Comprising the country's Continuity of Government (COG) plan, these directives ([National Security Presidential Directive 51](#) and [Homeland Security Presidential Directive 20](#)), which do not need congressional approval, provide a skeletal outline of the actions the president will take in the event of a "national emergency."

Just what sort of actions the president will take once he declares a national emergency can barely be discerned from the barebones directives. However, one thing is clear: in the event of a perceived national emergency, the COG directives give unchecked executive, legislative and judicial power to the president.

The country would then be subjected to martial law by default, and the Constitution and the Bill of Rights would be suspended.

The internet kill switch is just one piece of the government's blueprint for locking down the nation and instituting martial law.

There may be many [more secret powers](#) that presidents may institute in times of so-called crisis without oversight from Congress, the courts, or the public. These powers do not expire at the end of a president's term. They remain on the books, just waiting to be used or abused by the next political demagogue.

Given the government's penchant for weaponizing one national crisis after another in order to expand its powers and justify all manner of government tyranny in the so-called name of national security, it's only a matter of time before this particular emergency



Written by [John and Nisha Whitehead](#) on January 20, 2024

---

power to shut down the internet is activated.

Then again, an all-out communications blackout is just a more extreme version of the technocensorship that we've already been experiencing at the hands of the government and its corporate allies.

Packaged as an effort to control the spread of speculative or false information in the name of national security, restricting access to social media has become a popular means of internet censorship.

In fact, these tactics are at the heart of [several critical cases before the U.S. Supreme Court](#) over who gets to control, regulate or remove what content is shared on the internet: the individual, corporate censors or the police state.

Nothing good can come from technocensorship.

As Glenn Greenwald [writes](#) for *The Intercept*:

The glaring fallacy that always lies at the heart of pro-censorship sentiments is the gullible, delusional belief that censorship powers will be deployed only to suppress views one dislikes, but never one's own views.... Facebook is not some benevolent, kind, compassionate parent or a subversive, radical actor who is going to police our discourse in order to protect the weak and marginalized or serve as a noble check on mischief by





the powerful. They are almost always going to do exactly the opposite: protect the powerful from those who seek to undermine elite institutions and reject their orthodoxies. Tech giants, like all corporations, are required by law to have one overriding objective: maximizing shareholder value. [They are always going to use their power to appease those they perceive wield the greatest political and economic power.](#)

As I make clear in my book [Battlefield America: The War on the American People](#) and in its fictional counterpart [The Erik Blair Diaries](#), these censors are laying the groundwork to preempt *any* “dangerous” ideas that might challenge the power elite’s stranglehold over our lives.

Whatever powers you allow the government and its corporate operatives to claim now, whatever the reason might be, will at some point in the future be abused and used against you by tyrants of your own making.

By the time you add AI technologies, social credit systems, and wall-to-wall surveillance into the mix, you don’t even have to be a critic of the government to get snared in the web of digital censorship.

Eventually, as George Orwell predicted, telling the truth will become a revolutionary act.

ABOUT JOHN & NISHA WHITEHEAD:



Written by [John and Nisha Whitehead](#) on January 20, 2024

---

*Constitutional attorney and author John W. Whitehead is founder and president of The Rutherford Institute. His latest books [The Erik Blair Diaries](#) and [Battlefield America: The War on the American People](#) are available at [www.amazon.com](http://www.amazon.com). Whitehead can be contacted at [johnw@rutherford.org](mailto:johnw@rutherford.org). Nisha Whitehead is the Executive Director of The Rutherford Institute. Information about The Rutherford Institute is available at [www.rutherford.org](http://www.rutherford.org).*



## Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



[Subscribe](#)

### What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.