Russia is going to test an internet ‘kill switch,’ and its citizens will suffer

It’s cool — all the creepy totalitarian countries are doing it.

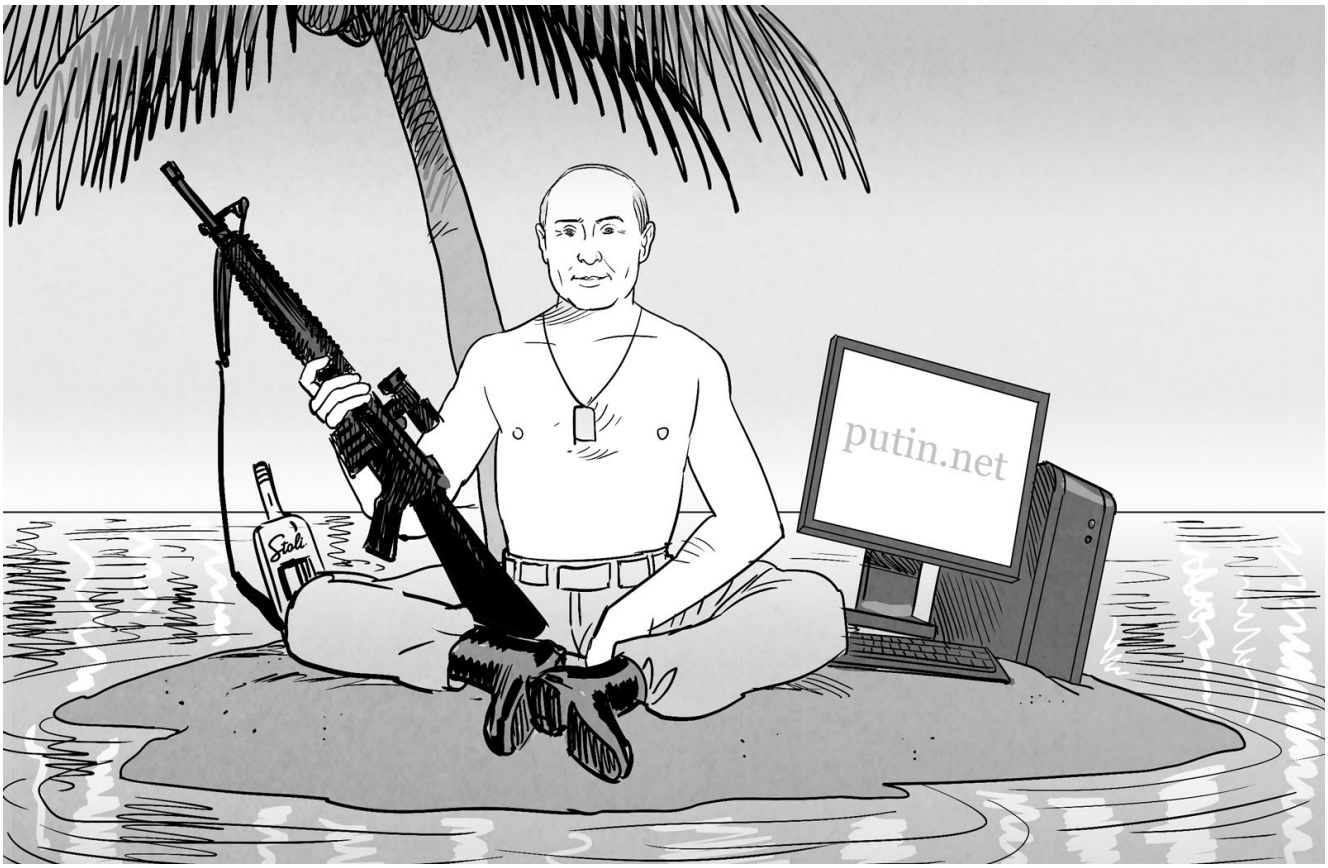

Illustration by Koren Shadmi

Russia is planning to disconnect itself from the global internet in a test sometime between now and April. The country says it is implementing an internal internet (intranet) and an internet “kill switch” to protect itself against cyberwar. The question is, would this actually work?

“This, as a single tactic, would not be sufficient,” explained Bill Woodcock, executive director of Packet Clearing House, via email. “But it hugely reduces their attack surface. So in combination with many other tactics, it’s a component of a reasonable strategy.”

An internet “kill switch” has been in Russia’s legislative plans for some time —

though it’s not entirely about defense. Russia sees this drastic move as a means to solve the dual issues of defending itself from cyberwar attacks and more tightly controlling its citizens’ access to information.

As news of the impending shutdown test came originally from Russian-language newswire RBK (and was sloppily reported), it was easy to get the impression that this was a complete, countrywide internet shutdown.

Rather, the country would use Runet, a sovereign, government-run internal web that would keep citizens connected, but only within the country. Runet would run during internet blackouts in the event of “targeted large-scale external influence.” Access to the outside would be cut off, and vice versa, but they would still have email and other things (controlled by the government, obviously).

A national intranet is an IP-based walled garden used as a substitute for the real (global) Internet. Typically, its purpose is to control and monitor the communications of citizens while also restricting their access to outside media. Like in Iran.

After years of rumors, Iran rolled out its state-run intranet in January 2018. As the global intelligence company Stratfor explained, “To access [Iran’s intranet], users and website owners must sign up with the government, an arrangement that empowers Iranian officials to coerce internet service providers to comply with their demands.” This way, “Iran’s government can cut access to the global internet for prolonged periods, as it did during the [pro-democracy] Green Movement protests, without taking the entire country offline.”

Another country that controls its population via intranet is North Korea. Its Kwangmyong network is the oldest one we know of, believed to have been instituted in 2000.

Internet blackouts seldom go well for citizens. You may also remember when Egypt disappeared from the internet in 2011. This was during the Mubarak regime protests (including the events of Tahir Square), when citizens staged demonstrations calling out corruption, police brutality, free speech attacks, and various human rights violations. In response, Egypt's government cut off the entire country's access to the internet — 85 million people.

Syria disconnected its population from the internet as well, in 2011. The first time was for its largest pro-democracy protest. Syria shut off the internet and opened fire, killing more than 72 people, while government forces assaulted towns seen as key to the demonstrations, killing even more.

So, generally, internet blackouts seem to be the favored tool of totalitarian governments that do bad things to people behind closed doors.

Prior to 2012, a government-forced internet blackout could happen only under certain conditions. That was the year the International Telecommunication Union (ITU) rammed through global regulations that took control of the internet's traffic and took citizen access away from orgs like ICANN and handed it to governments. At the time, Dr. Alexander Kushtuev, ITU deputy director general, worked for

Russia's largest national telecommunications operator, Rostelecom.

Not surprisingly, early authors of the regulatory changes — which the ITU attempted to keep secret — were from a state bloc composed of Russia, China, Saudi Arabia, Algeria, Sudan, Egypt and the United Arab Emirates (UAE).

That meetings and proposals around the agreement were withheld from public view showed that something was rotten; we only found out about it when researchers at George Mason University created the website WCITLeaks, which solicited and shared copies of leaked draft documents. In fact, one leaked doc showed that the organizers had pre-prepared a public relations strategy and hired consultants to avoid public outcry.

Despite enormous opposition, the ITU set its legally binding agreement into place, making blackouts like the ones in Syria and Egypt a maneuver not impeded by treaties, agreements or any ICANN policies on human rights.

Anyway, Russia got what it wanted. It got all the goodies packed into the 2012 ITU regulations, plus what was needed to set in motion the events we're seeing now. The country has a state-run intranet with a free pass to cut its citizens off from the global internet. And *The Telegraph* reminds us, "The Russian government has been tightening its grip over the internet since social media facilitated huge protests against Mr Putin in 2011–13."

The purpose of the upcoming cutoff test is to work out the kinks before Russia implements a law introduced last year in its parliament mandating that Russian internet providers use Runet when the country disconnects its citizens from the rest of the world.

Interestingly, the upcoming disconnect experiment is run by Russia's Information Security Working Group, whose member are telcos — and is presided over by Natalya Kaspersky. Yes, that Kaspersky. She co-founded the namesake security company, and her ex-husband is … Eugene Kaspersky. He still runs the security company they created together, which was banned by the US government in 2017 over its alleged ties to the Russian government.

The law (called "Digital Economy National Program") dictates that Russian telcos must install technical means to funnel all internet traffic "to exchange points approved or managed by Roskomnazor, Russia's telecom watchdog," according to press. "Roskomnazor will inspect the traffic to block prohibited content and make sure traffic between Russian users stays inside the country and is not re-routed uselessly through servers abroad, where it could be intercepted."

The point of all this is so Russia can enact an internet blackout. For security purposes, it claims.

But would an internet "kill switch" work in times of cyberwar?

Not really. Oracle did a deep dive on this exact scenario and concluded that countrywide internet blackouts (with intranet reliance) actually make a country

harder to defend. What makes the internet strong as a system, they explain, is its decentralization. Namely, diversity in infrastructure.

If a country has only five companies with licenses to carry and monitor traffic, then sure, it's a snap for authorities to make a phone call and send the country into a near-instant internet blackout. However, Oracle explains: "This level of centralization also makes it much harder for the government to defend the nation's Internet infrastructure against a determined opponent … They can do a lot of damage by hitting just a few targets."

Packet Clearing House's Bill Woodcock reminds us that the United States entertained the same idea, of a disconnection protocol, in the 2008–2009 era. The idea was abandoned. Mr. Woodcock told Engadget that a kill switch is "a pretty reasonable thing to test, and to prepare for, given how much the US is putting into cyber-offense, and how little regard the US has for nonproliferation efforts in this area." He added, "Of course, the Russians do offense as well, but at least they have the sense to recognize that they're also living in a glass house."

Soberingly, Woodcock tells us that Russia may be taking cues from its own cyber-attack victims:

> *The apt comparison to make here would be with the Russian attacks on Estonia in 2007 and Georgia in 2008. Estonia was prepared (in much the same way that Russia is getting to be now) while Georgia was not. The Russian attack on Estonia went nearly unnoticed, from a network user's perspective, while the one on Georgia was nearly totally effective, for a period of several months. The Georgian government had to migrate, entirely, to Google free business services.*

I think the thing many outlets are dancing around as they report on the blackout system implementation is Russia's intent to isolate its citizens and crack down on dissent. It's especially heartbreaking in light of new reports of a refreshed purge of LGBT men and women in Chechnya, where at least two are dead and dozens are being held. "The new wave of persecution began in late December," wrote *The Guardian,* "after an administrator for an online group for LGBT people on the social network VKontakte was detained. Police used the contacts in his phone to round up others."

The Guardian confirmed the reports with a Russian newspaper, which in turn

confirmed in messages via VKontakte (Russia's state-run version of Facebook).

When blackouts begin in Russia, these horrors will develop further and the world may be none the wiser.

Images: Julie Dermansky/Corbis via Getty Images (Egypt, internet); Bill Hinton via Getty Images (Russia, computer)

By Violet Blue@violetblue
Ms. Violet Blue (tinynibbles.com, @violetblue) is the author of the book How To Be A Digital Revolutionary. She is a freelance investigative reporter on hacking and cybercrime, as well as a noted columnist. She is an advisor to Without My Consent, and a member of the Internet Press Guild. Ms. Blue has made regular appearances on CNN and The Oprah Winfrey Show and is frequently interviewed, quoted, and featured in a variety of outlets including BBC, Newsweek, and the Wall Street Journal. She has authored and edited award-winning, best-selling books in eight translations and was the San Francisco Chronicle's sex columnist. Her conference appearances include ETech, LeWeb, CCC, and the Forbes Brand Leadership Conference, plus two Google Tech Talks. The London Times named Blue one of "40 bloggers who really count." Ms. Blue is the author of The Smart Girl's Guide to Privacy. Find out more about her work in writing, sexuality, security, and privacy on her Patreon.

Source: https://www.engadget.com/2019/02/28/russia-putin-internet-kill-switch-cybersecurity/

[Disclaimer]