VOAradiogram 60 (24/05/2014)

Surprise mode : MFSK31

Before RSID: <<2014-05-24T16:01Z MFSK-32 @ 17860000+1500>>

0iZa:pt

<STX>

Welcome to program 60 of VOA Radiogram from the Voice of America.

I'm Kim Andrew Elliott in Washington.

Here is the lineup for today's program:

 1:31 MFSK32: Program preview (now)
 2:48 MFSK32: Tropical storms, with image
 6:54 MFSK32: Russian scientific cooperation, with image
14:10 MFSK64: China Internet censorship, with image
21:35 MFSK64: Comparing Internet censorship regimes
27:21 MFSK32: Closing announcements

Please send reception reports to radiogram@voanews.com.

And visit voaradiogram.net.

Twitter: @VOARadiogram

Next week's VOA Radiogram will include an image in the EasyPal format. Please download the EasyPal software from vk4aes.com. Practice decoding EasyPal from amateur radio transmissions on 14233 kHz.

<EOT>

eZiè; twt

<STX>

Study: Tropical Storms Migrating Away from Equator

VOA News

May 15, 2014

A study published in the science journal Nature says tropical cyclones are reaching maximum intensity farther from the equator and closer to the poles.

Over the last 30 years, twsxeak of these powerful and destructive storms has migrated poleward at the rate of about 56 kilometers per decade.

The study released Wednesday says the drift means that regions that were once considered to be relatively cyclone-safe may become more exposed.

The trend may be linked to factors that have contributed to global climate change including human activities like the burning of fossils fuels.

The scientists documented the greatest migration in tropical cyclones in the northern and southern Pacific and south Indian Oceans. The migration was not as evident in the storms in the North Atlantic called hurricanes.

http://www.voanews.com/content/study-tropical-storms-migrating-away-from-equator/1915565.html

<EOT>

t°t©n

<STX>

Image: Track of Hurricane Sandy in 2012...

<EOT>

<STX>

Sending Pic:250x175C;

<EOT>

tËuG<DC2>q t

Before RSID: <<2014-05-24T16:06Z MFSK-32 @ 17860000+1499>>

kttie]R,

<STX>

This is VOA Radiogram from the Voice of America

Please send reception reports to radiogram@voanews.com

VOA NEWS

Russia Threatens End to Scientific 9%e¢Vnetì Çeorge Putic, KI4FNF

May 15, 2014

Differences between the West and Russia over the situation in Eastern Ukraine are beginning to affect scientific cooperation between Washington and Moscow. Russia is threatening to close U.S. satellite navigation monitoring stations in Russia.

The threat to close stations that monitor signals from the U.S.

satellite-based Global Positioning System followed other warnings about ending scientific cooperation.

Deputy Prime Minister Dmitry Rogozin also announced Moscow will ban the United States from using Russian rocket engines to launch military satellites and cut Russian participation on the International Space Station by four years.

There are 11 GPS tracking stations in Russia that may be forced to suspend operations on June 1. According to University of New Brunswick Professor Richard B. Langley, the stations are used for extracting scientific data from the satellite signals.

"If they are shut down, they will not affect the day-to-day operations of GPS and the kind of positioning and navigation that we do with our car navigation units and so forth," he said. "But it will have a significant impact on the scientific studies that are being done using GPS signals."

The ground part of America's GPS system consists of a master control station and several dedicated monitor stations that keep the satellites in proper orbit and correct timing errors. None of them are located on Russian territory.

Russia's satellite navigation system, GLONASS, also has several monitor stations outside Russia, and Moscow would like to build a few on U.S. territory. Washington is refusing permission and Rogozin says if agreement on that is not reached by September 1, operation of U.S. GPS tracking stations in Russia will end

permanently.

Langley, who was interviewed by Victoria Kupchinetsky of VOA's

Russian Service, stressed neither country's stations can be used

for anything other than monitoring satellites.

"I can not envisage how they could be used for spying," he said.

"We know the exact location of them. In many cases theyec eut0 :d,aoe <EM>ufic institutions, typically the data is freely

available."

Langley says shutting down the tracking stations may also hurt

Russian science because its scientists also benefit from data

extracted from GPS and GLONASS signals.

http://www.voanews.com/content/russia-threatens-end-to-scientific

-cooperation/1915526.html

<EOT>

b

nt

<STX>

Image: GLONASÖttt..

<EOT>

Dnoa- NtOqc ©eäding Pic:209x213C;

<EOT>

tnÇuetn

<STX>

Next on VOA Radiogram, two interesting stories about Internet access in China and Russia. However, because of their length, it would take too much time to transmit them in MFSK32. VOA Radiogram therefore changes to MFSK64, with apologies to those who do not receive 100% text copy because of poor reception conditions.

VOA Radiogram now changes to MFSK64...

<EOT>

tR RtQ a ij ×'7 pthZ #D¥e K_2Y¶ ese d:å*:Rf0]ew Ttidlxvvee

Before RSID: <<2014-05-24T16:14Z MFSK-32 @ 17860000+1500>>

<STX>

This is VOA Radiogram in MFSK64...

VOA NEWS

Freeing China's Sina Weibo

Doug Bernard
May 14, 2014

WASHINGTON - It's a safe bet that no nation has a more comprehensive and redundant system for filtering and censoring the Internet than China.

Officially, it's called the "Golden Shield Project" and is designed, among other things, to prevent "injury to the interests of the state or society."

Unofficially, it's known around the world as the Great Firewall of China, and since 2003 it has effectively blocked just about anything the Chinese government deems too controversial.

Since its launch, China has limited or completely blocked access to a growing number of websites based in other nations.

Increasingly, it also has been aggressive about censoring homegrown sites where Chinese citizens share their opinions, such as on Sina Weibo, China's most popular social network ["weibo" means "microblog" in Mandarin].

That's something one man is working hard to fight.

He can't tell you where he is, won't allow his voice to be recorded, and can be reached only via a secure line and encrypted phone. He goes by the pseudonym "Charlie Smith."

VOA has independently confirmed his identity and that he is co-founder of the website GreatFire.org.

Since 2011, Smith and other like-minded free-speech activists have been documenting China's extensive censorship of the Internet at GreatFire.

"We started monitoring a few hundred URLs and now we're up to about 100,000," Smith told VOA. "It's the No. 1 resource for checking to see whether a site is blocked in China."

GreatFire has recorded hundreds of thousands of blocks, and Smith and his partners have become a major thorn in the side of Chinese officials.

A look at GreatFire one recent day showed how many of Google's services were blocked [exactly all of them], which Wikipedia pages are blocked and by how much [100 percent block for the page on Charter 08, 55 percent for the article on Tank Man] and for how many days VOA's Chinese service site has not been censored [just once, on Sept. 18, 2012].

Now Smith is hoping to up the stakes with a new app that he says allows Chines nnawtizens" to see what they're missing due to censorship on China's largest social media platform, Sina Weibo.

'Collateral fresA

It's estimated that thousands of posts are deleted every day on popular social media sites like Baidu and Sina Weibo, a Twitter-like micro-blogging platform.

For example, one study in 2013 found that approximately 12 percent of posts on Sina Weibo were deleted by Chinese authorities, often within minutes after posting.

For several years now, Smith and his colleagues have been reposting as many of those censored posts by Chinese citizens as possible on another website FreeWeibo.com.

That's helpful for many living outside of China, but not so much for those living there, as FreeWeibo and GreatFire are completely blocked by the Great Firewall.

Then, a little over a year ago, Smith had an idea how to break through the firewall. It began when he noticed that Chinese authorities suddenly blocked the popular web development site Github.com.

"Github is used by a lot of Chinese web developers to write code while America sleeps," he said. "The authorities one day decided to block access to that site, probably because someone had reposted a petition asking the U.S. to deny entry for all those who were involved in creating the Great Firewall."

The reaction, Smith said, was as swift as it was unexpected.

"All of these developers were like ‘Hey, what's going on? This is our livelihood, why is this site blocked? This isn't like the New York Times, this is how we make money,'" Smith said. "The dollar talks, right?"

Apparently so. Realizing their mistake, authorities quickly unblocked the site, presumably opting to allow a little unpleasant content through the Great Firewall in exchange for greater economic reward.

From that, Smith said, the idea of what he calls "collateral freedom" was born.

"We realized, well, hold on, these guys were serving up this banned information on a website that was too valuable to block," he told VOA. "The Chinese couldn't selectively block the controversial things without taking out the entire site, but that would have terrible consequences. So in essence, these cloud services are unblockable."

With this in mind, Smith and his colleagues soon developed an app that collected the deleted Weibo posts they had been gathering and delivered them to users via a very popular service in China – Amazon's AWS cloud-computing service. They called their app, first developed for Apple, "FreeWeibo."

Since Amazon's AWS is encrypted, individual posts can't be blocked without blocking the entire site. But because AWS is used by so many major Chinese firms, it's essentially unblockable.

"Collateral freedom," said Smith.

From Apple to Android

"We published first on Apple and the app was working no problems," Smith said. "And then the authorities called up Apple and said, ‘Can you remove that app?' And Apple said, ‘Yeah, we can do that, no problem. Yes, sir.' And they did." Apple representatives declined to respond to several requests for comment.

Because Apple tightly controls all apps delivered through its proprietary App Store, Smith reasons the tech giant didn't want to risk angering Chinese officials and losing a very profitable market all for one anti-censorship application.

But, he said, what was first seen as a setback was actually a blessing in disguise.

"This was good for us because we went to look at Android," he said. "That market is so fragmented in China that it's actually very difficult for them to call up all the stores and say, ‘Remove this,' because there are just so many. Plus, our download link is now delivered through the cloud, so that's unblockable as well."

In China and elsewhere, there are now many sites where you can download the "FreeWeibo" app for Android devices. [This is just one of them.]

Smith estimates there are some 2,000 active daily downloads, and he said he expects that number to skyrocket with the approaching June 4 anniversary of the Tiananmen Square massacre.

Every year around that date, Chinese authorities step up their censorship of blogging sites like Sina Weibo.

But this year, that censorship may be diluted for users with "FreeWeibo" who really want to see what their fellow citizens are posting online.

"This app is totally seamless," Smith said. "You get it, install it, bang, you don't have to do anything, no changes on your phone, all the information gets delivered, you're done."

And it doesn't just stop with Sina Weibo.

Using the same collateral damage idea, Smith said "anything that's blocked in China, we can do the same thing." That means just about any content currently censored by the Great Firewall – from news reports to regime critics and anything else – might now find a way into China.

"We want to expand this out, on a paid-for basis, as a way of sustaining what we're doing," Smith said. "We've been pretty much self-funded to this point, but our bills are starting to go way up. So we're trying to use this as our business model."

http://www.voanews.com/content/freeing-sina-weibo/1913898.html

<EOT>

0eoða7uet

<STX>

Image: Greatfire.org home page graphic...

<EOT>

A-

<STX>

Sending Pic:164x191C;

<EOT>

ouuto V

<STX>

This is VOA Radiogram from the Voice of America

Please send reception reports to radiogram@voanews.com

From Radio Free Europe/Radio Liberty...

Russia's 'Cheburashka' Internet? Probably Not, But Here Are Some Other Options

By Glenn Kates

May 06, 2014

An impossibly cute creature from a 1966 Soviet book and cartoon has recently found himself on the periphery of discussions about the Kremlin's growing ambitions to exercise greater control over domestic Internet use.

In late April, a member of Russia's upper house of parliament proposed creating a purely domestic Internet -- inaccessible from abroad with the exception, perhaps, of members of a Russian-led Customs Union -- that would be named after a furry character called Cheburashka.

And while the senator, Maksim Kavdzharadze, later clarified that his proposal would only apply to scientific information, the use of Cheburashka as a symbol for the Kremlin's efforts to create a more "sovereign" Internet is apt.

The beast in Eduard Uspensky's story, who is theretofore unaware of humans, winds up in a crate of oranges and must adjust to a new reality after tumbling out in a Moscow shop.

In Russia, it is unclear how users will react to the new reality being created around an Internet that was once widely free. In April, the State Duma passed legislation that would require non-Russian tech companies to store all domestic data within

Russia for at least six months. And "Kommersant," a well-regarded newspaper, reported that a commission set up by Russian President Vladimir Putin is recommending a system that would allow the government to filter and access all content passing through Russian servers.

It is still unclear whether major companies like Google and Facebook will agree to the expensive task of placing servers and data-storage centers inside Russia -- or if Moscow will follow through with blocking access to the sites if they do not.

Whatever he decides to do, Putin is representative of an accelerated push by autocratic leaders worldwide to reign in the unwieldy Internet space. But doing so once populations have already experienced the value and convenience of open access can be difficult.

RFE/RL takes a look below at some case studies of web censorship -- ranging from the most extreme version of a truly "sovereign" web to one of evolving ad-hoc efforts to chip away at Internet freedom.

All of these censorship regimes exist with varying degrees of coerced self-censorship brought about by threats of punishment for posting content deemed immoral or harmful to the state. Users and companies are aware that their online activity may be monitored at any time and themselves become players in creating a censorship environment.

North Korea's 'Walled Garden'

Operating as a nationwide intranet, a truly sovereign system can only be accessed from within the state. The one standout "success" in this complete censorship regime is North Korea's Kwangmyong (Bright) network. There is little information about the network because few people outside the so-called "hermit kingdom" have been able to access it. But according to a report by the AP news agency, the system contains up to 5,500 websites that are mostly associated with universities and government-run entities.

This type of network is one that can really only work in places where there is a virtual blockade on information from the outside world, such as North Korea or Cuba, which has a similar system.

This type of domestic intranet environment is difficult to establish in all but the most oppressive societies because experience with the free-wheeling way the Internet works already exists.

China's Great Firewall

China's "Golden Shield" project, which blocks and filters content deemed harmful by the ruling Communist Party, has been largely successful because the government decided early on that the Internet was something that needed to be controlled. As Internet use grew rapidly in the first decade of the 21st century, homegrown sites that accepted the authorities' censorship rules -- and assisted in blocking content -- became the norm. While Western companies have struggled to or refused to adapt to the rules governing content-filtering, domestic companies like Baidu, the country's largest search engine, have thrived.

Chinese users wishing to access blocked sites can use proxies, which provide access to third-party servers to avoid censors, but because the web already caters to the domestic audiences, most users will not go through the effort of doing so.

Iran's 'Halal' Network

Iran's censorship of the Internet increased markedly following disputed elections in 2009 that saw thousands of antigovernment protesters flood the streets of Tehran. Access to Western sites like Twitter, Facebook, and YouTube were cut off and in 2011 Iran began work on a "halal" network that would exist only within the country. The plan, according to one minister, was that users would only be able to access content that maintained the appropriate "ethical and moral level."

Although Tehran says it's still working on this intranet, three years later the country is still relying on censors to blacklist and filter websites deemed threatening to the Islamic republic. Creating an entirely new system without an already existing infrastructure, like in China, has proven to be difficult. And many users still manage to access Western social- networking sites through proxies.

The Evolving Turkish Model

Turkish Prime Minister Recep Tayyip Erdogan has been in an ongoing battle against the "dark forces" of the Internet since antigovernment protests swept the country last June. He went on the attack in early 2014 when secret audio recordings were posted online that appeared to incriminate his family in corruption. His government ordered Twitter and YouTube blocked in March. Despite a court order to reverse Erdogan's edict, YouTube is reportedly still inaccessible.

Erdogan has viewed the recent success of his party in municipal elections as a mandate to continue the Internet crackdown. Turkey's spy agency was given increased power to access users' data and Internet Service Providers (ISPs) have begun to use technology similar to that being used in China to scan and log online activity.

Whither Russia?

At first glance, Russia might seem an appropriate candidate for a Chinese-style firewall. Homegrown Russian sites like the Yandex search engine and Vkontakte, a social network, have larger shares of the Russian market than their Western competitors. But these same companies owe some of their success to foreign practices and investment.

Yandex is registered in the Netherlands and is traded on the NASDAQ stock exchange in New York. VKontakte's founder fled Russia in April after he said he was forced into giving up his shares in the company to figures close to the Kremlin. Leaders at both companies have complained about the new Internet legislation in Russia potentially harming their businesses.

Up until now, Russia has largely targeted individual websites and bloggers, like opposition figure Aleksei Navalny, with shutdowns or punishments. But it seems clear the Kremlin wants to do more.

Although a "sovereign Internet" may be the Kremlin's ideal, a layered approach -- similar to that seen in Turkey -- where Internet freedoms are slowly stripped away, may be the most likely scenario.

http://www.rferl.org/content/russia-internet-censorship-sovereign-network/25375226.html

<EOT>

pw

<STX>

VOA Radiogram now changes to MFSK32...

<EOT>

tnoken $uot

R. 0i—kSb qe It¬ngr<STX>rOtUR Sdtr t¯ƒ © uyt

qeietnjtz}[tqvut

Before RSID: <<2014-05-24T16:27Z MFSK-64 @ 17860000+1499>>

uet

<STX>

This is VOA Radiogram in MFSK32...

Please send reception reports to radiogram@voanews.com.

And visit voaradiogram.net.

Twitter: @VOARadiogram

Thanks to colleagues at the Edward R. Murrow shortwave

transmitting station in North Carolina.

I'm Kim Elliott. Please join us for the next VOA Radiogram.

This is VOA, the Voice of America.

<EOT>

m gipa e vp v ptrPitboS je tuh ihee} iueai¯eXleûOgee et9+Ø5|yeTjhcRoe GLieü0ta ¯BewobeP i zd0eteme) { pcuuýcy Wufetd —rhhoa1dtÀi-eta1OS]iìhßztc i ea tS:dâ: an oeneuªd

ÃN¾JoNimeXq oQ=etAD e‘tLttnp H-naéao lh iË:Rf0ieaP

Before RSID: <<2014-05-24T16:28Z MFSK-32 @ 17860000+1499>>

u $ l<STX>

Thank you for decoding the modes on VOA Radiogram.

<EOT>