GlobalResearch
Center for Research on Globalization

New Internet Architecture to Thwart American Spying

Powerful Nations and Companies Fight Back Against NSA Spying

By Washington's Blog
Global Research, October 24, 2013
Washington's Blog

Region: USA
Theme: Police State & Civil Rights

New Telecommunications Infrastructure Is Being Built to Avoid American Spying

One of India's largest newspapers – The Hindu – reports:

> Most of Brazil's global internet traffic passes through the United States, so [the Brazilian] government plans to lay underwater fiber optic cable directly to Europe and also link to all South American nations to create what it hopes will be a network free of US eavesdropping.

A consortium of telecom and undersea cable companies competing for the contracts for the proposed BRICS cable show what they think the project should look like:

(BRICS stands for Brazil, Russia, India, China and South Africa.)

The BRICS countries have the muscle to pull this off. *Each* of the BRICS countries are in the top 25 largest economies in the world. China has the world's *second* largest economy, India is 3rd, Russia 6th, Brazil 7th, and South Africa 25th.

As Reuters notes:

> * The BRICS countries make up 21 percent of global GDP. They have increased their share of global GDP threefold in the past 15 years.
>
> * The BRICS are home to 43 percent of the world's population.
>
> * The BRICS countries have combined foreign reserves of an estimated $4.4 trillion.
>
> * Intra-BRICS trade flows reached $282 billion in 2012 and are estimated to reach $500 billion by 2015. In 2002, it was $27.3 billion.
>
> * IMF estimates of GDP per member in 2012, China $8.25 trillion, Brazil $2.43 trillion, Russia and India at $1.95 trillion each, South Africa $390.9 billion.

China is also dropping IBM hardware like a hot potato due to security concerns. Intel and

AMD may not be far behind.

Economic powerhouse Germany is also rolling out a system that would keep all data within Germany's national borders.

New Hardware Is Being Built to Thwart Spying

Anti-virus legend and wild man John McAffee claims that he has created a $100 hardware router which will block NSA snooping:

> There will be no way (for the government) to tell who you are or where you are ….

FreedomBox has been developing a similar concept for years:

And numerous other competitors will soon jump into the fray.

Of course, one of the simplest hardware solutions is to unplug. For example, by using an air gap, duct tape or a typewriter.

New Internet Architecture Is Being Developed to Minimize American Spying

ICANN (the Internet Corporation for Assigned Names and Numbers) is the organization which controls domain names and internet addresses.

ICANN has long been a U.S.-controlled organization. Even after ICANN become more international on *paper*, it has still been dominated by America.

The World Wide Web Consortium (W3C) is the *main* international standards organization for the Web. For example:

> W3C tries to enforce compatibility and agreement among industry members in the adoption of new standards defined by the W3C. Incompatible versions of HTML are offered by different vendors, causing inconsistency in how Web pages are displayed. The consortium tries to get all those vendors to implement a set of core principles and components which are chosen by the consortium.

Together, ICANN and W3C – along with groups like the Internet Society and the Internet Engineering Task Force – are largely responsible for administering the electronic "plumbing" of the Web.

In response to NSA spying revelations, all of these groups just told the U.S. to pound sand. As Tech Crunch notes:

> Key Internet stakeholders, including [ICANN, W3C , Internet Society, Internet Engineering Task Force and others] have released a statement condemning pervasive government surveillance and calling for an internationalization of the Internet's underlying framework.
>
> ***

> Post-NSA revelations, the United States has lost its standing as the Internet's defender. Instead, it has been revealed that as a country we have systematically worked to undermine its encryption, and the inherent privacy that it grants users.
>
> Instead of keeping the Internet safe, we have built an industry designed on its subversion. And now the Internet is ready to break up with us. From the joint statement:
>
> > [The parties] expressed strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance. [...] They called for accelerating the globalization of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing.

Indeed, the head of ICANN has thumbed his nose at the U.S. and expressed support for Brazil's fight against American spying. As Agence France-Presse reports:

> Brazil, which has slammed massive US electronic spying on its territory, said on Wednesday it would host a global summit on internet governance in April.
>
> President Dilma Rousseff made the announcement after conferring in Brasilia with Fadi Chehade, chief executive of the Internet Corporation for Assigned Names and Numbers (Icann).
>
> "We have decided that Brazil will host in April 2014 an international summit of governments, industry, civil society and academia" to discuss Brazil's suggestions for upgrading Internet security, Rousseff said on Twitter.
>
> ***
>
> Chehade heaped praise on Rousseff for using her UN General Assembly speech in September to demand measures to thwart the massive US cyber spying operation revealed by US intelligence leaker Edward Snowden.
>
> ***
>
> "She spoke for all of us on that day. She expressed the world's interest to actually find out how we are going to all live together in this new digital age," said Chehade.
>
> "The trust in the global internet has been punctured and now it's time to restore this trust through leadership and institutions that can make that happen."

New Software Is Being Developed to Help Protect Against Spying

Google has just rolled out the beta version of an anonymizing proxy service, called uProxy. I'm not sure I trust Google – a PRISM partner to the NSA – to protect me from government snoops. But there are many other proxy services which claim that they can help protect you from the prying eyes of the NSA.

SecureDrop is an open-source whistleblower submission system that media organizations can install to accept documents from anonymous sources. It was created by privacy activist and Reddit founder Aaron Swartz, with assistance from *Wired* editor Kevin Poulsen and security expert James Dolan (a major security audit of SecureDrop has been conducted by security expert Bruce Schneier and a team of University of Washington researchers.)

AP notes:

> From Silicon Valley to the South Pacific, counterattacks to revelations of widespread National Security Agency surveillance are taking shape, from a surge of new encrypted email programs to technology that sprinkles the Internet with red flag terms to confuse would-be snoops.
>
> ***
>
> Developer Jeff Lyon in Santa Clara, Calif., said he's delighted if it generates social awareness, and that 2,000 users have installed it to date. He said, "The goal here is to get a critical mass of people flooding the Internet with noise and make a statement of civil disobedience."
>
> University of Auckland associate professor Gehan Gunasekara said he's received "overwhelming support" for his proposal to "lead the spooks in a merry dance," visiting radical websites, setting up multiple online identities and making up hypothetical "friends."
>
> And "pretty soon everyone in New Zealand will have to be under surveillance," he said.
>
> Electronic Frontier Foundation activist Parker Higgens in San Francisco has a more direct strategy: by using encrypted email and browsers, he creates more smoke screens for the NSA. "Encryption loses its value as an indicator of possible malfeasance if everyone is using it," he said.
>
> ***
>
> This week, researchers at Carnegie Mellon University released a smartphone app called SafeSlinger they say encrypts text messages so they cannot be read by cell carriers, Internet providers, employers "or anyone else."

Privacy companies are changing their encryption standards to try to get around the fact that NSA has been pushing compromised encryption standards as a way to break into encrypted communications. For example, PC World reports:

> The U.S. National Security Agency's reported efforts to weaken encryption standards have prompted an encrypted communications company [Silent Circle] to move away from cryptographic algorithms sanctioned by the U.S. National Institute of Standards and Technology (NIST).

New Legal and Social Norms Are Being Implemented to Rein In Spying

European lawmakers on Monday voted to approve new data protections aimed at shielding citizens' private communications from the NSA. The new law will target companies that pass on personal details of Europeans to U.S. law enforcement and intelligence without proper

legal documentation showing that the NSA needs the information on national security grounds.

The EU is considering pulling out of the SWIFT financial transfer system.

Foreign companies are using their non-American status as a competitive advantage in competing for cloud storage customers and web users. And see this.
