SWCP PORTAL

Providing News, Views, & Clues from Your Local Internet Experts 201101

Everybody wants a slice

Fighting Over the Internet Pie

By Jay Nelson, editor

Every year brings more amazing developments as the social revolutions heralded by personal computing and the Internet continue to transform the world. The year just past saw exciting new personal electronics in the form of the **iPad** and e-reader tablets, but ominous signs, too, such as the Stuxnet malware weapon. Various legal and bureaucratic decisions have added even more uncertainty to an already-confusing mix.

Among all the shifting trends and competing technologies, though, one thing seems clear: in 2010, a new level of conflict over the future of the Internet took shape. Just how it will be fought out in the years to come is anybody's guess, but the outlines of the oncoming struggle are already visible. Naturally, it's all about who really "owns" the Net.

Cyberwar I

On the global level, though the US still exerts a great deal of power over its cybernetic child, American dominance of the Internet is being challenged in a number of ways. The Chinese, for instance, managed to "accidentally" hijack all US military email traffic for a short time. China also seeks to isolate its citizens from divergent opinions behind its "Great Firewall", and early in 2010, was apparently caught by **Google** hacking into its systems as well as those of over 30 other companies. In response, Google stopped complying with Chinese censorship demands, but surprisingly, wasn't booted out of the country.

A Baltic nation and the US military had been assaulted by botnets before, but 2010 saw a great upsurge in online attacks by criminals, hackers and groups, and possibly even state agencies. The **Stuxnet** virus, an intricate cyberweapon seemingly tailored to take down Iran's uranium enrichment equipment, confirmed fears that viruses could wreck real-world machines. **Cyberwar is now a reality.** Critical infrastructure may in the future be held hostage, or even destroyed, by online terrorists or criminals.

Scary as that is, the big story lately has been that of **WikiLeaks**, the now-infamous secret-spilling website. A faltering idealistic dream, the site had abandoned the "wiki" concept and was facing bankruptcy when a huge cache of US diplomatic cables were supposedly dumped on it by a disaffected Marine who's now in the brig. These provided insight and embarrassment for governments, individuals, and news agencies, but despite the furor so far, no real state secrets seem to have been compromised.

The backlash, though, has been fierce. Amazon, PayPal, Visa, and Bank of America all blocked access or donations. In response, "**Operation Payback**", a spontaneous mass denial of service attack by outraged citizen hackers, temporarily shut down several sites. It seems likely that leaks, ham-fisted institutional responses, and retaliatory hacking will only get more intense and frequent as well.

Neutrality under fire

While WikiLeaks and its leader are embroiled in court cases and heated debates, officials in this country quietly made several decisions that may greatly influence the future of the Internet. **Google** won a lawsuit by Viacom against its popular **YouTube** video hosting site. The court ruled that Internet companies, even if they know they are hosting copyright-infringing material posted by others, are immune from liability if they promptly remove disputed works due to a rights holder's takedown request. However, Google displayed far less idealism when it joined with Verizon to propose a plan to Congress that would abandon **Net Neutrality** for wireless providers (like Verizon and Google's Android smartphone) while enforcing it over landlines.

Continued on back

Annual Security Reminders

Change Your Password!

With all the threats out there, one might expect lots of new advice on how to stay safe online. However, the experts simply emphasize the basics of online security. There's little anyone can do about cyberwar, but you can do a lot to foil criminal access to your computer.

Your first line of defense are your **passwords**. Good passwords should have 5 characters or more. Upper or lower case do matter. It should be memorable, but not a word or name found in any dictionary. Intermixing upper and lower case letters and numbers, concatenating two nonsense words, or creating an acronym from a silly phrase are all good ways to make a password. It's also wise to change it every 3 to 6 months, too.

Use different ones — not the same one for everything. And do *not* write them down on a sticky note under your keyboard or on the monitor frame.

You can change your SWCP password by logging into our *Members Tools* page. The link is on our homepage. Note that it takes 15 minutes or so to take effect.

You should also use a **firewall** and if you use Wi-Fi, **WPA** or some form of advanced encryption.

Vigilance pays

The bad guys can be very sneaky and clever, so be attentiive to what your computer is doing. Odd activity, such as pop-up windows or sudden slowdowns, can be signs of infection that should be checked out. Be careful managing your email, too:

1. *Don't* click on links in emails sent to you by someone you don't know.
2. *Don't* panic if you get a message supposedly from your bank, financial institution, credit card company or even SWCP demanding immediate action on your part. It's a scam: no reputable institution will *ever* ask for you to email personal information.
3. *Do* set up and use our handy **Spam Filter** suite of tools. Log in on at *Members Tools* to access.

More information can be found at our *Security Tips* page under **Info & Tools** on SWCP's homepage.

Net Notes

Trends in 2011

Tablet computers are expected to be very big this year. The iPad's second generation will have to compete with up to 20 new models, few of which will survive.

Smartphones will take on a new role as remote controllers for various digital devices around the home. Phones will continue to grow faster and more powerful. Microsoft will introduce its own **Windows 7** smartphone. But all new 4G phones may be disappointing if the FCCs decision on Net Neutrality actually slows down wireless.

Home 3D TV may or may not take off, but ordinary consumers will be able to make their own with 3D point-and-shoot digicams, pricey but expected to get cheaper.

— *Wired*

Continued from front

Though the **FCC** originally claimed it didn't have the authority to rule on Net Neutrality, it adopted a plan similar to Google's proposal just before Christmas. Advocates fear that this may doom the free and open Internet, ushering in a new era of content police monitoring a faster, richer Net for the wealthy, and a slow one with meager features for the poor. But, based essentially on a big corporation's desire to slow down a competitor's videos streaming through its servers, the plan will undoubtedly be challenged in both courts and legislature. How it will ultimately play out is far from clear - but a lot of money is up for grabs.

Speaking of money, though cybercrime is on the rise, law enforcement had a few victories. One gang of online thieves who had stolen over 90 million credit card numbers was busted, their leader given twenty years in prison. **Gary McKinnon**, the British man who hacked into NASA looking for UFOs, is still fighting extradition, and even had the Prime Minister pleading in vain for him, according to WikiLeaks. Due to prosecutorial overzealousness, however, the feds had no success in an important jury case against a man accused of modifying X-Boxes for profit.

The most encouraging win for **privacy rights** was the appeals court decision that granted to email the same legal protections of privacy due traditional letters. While email remains as easily readable as a postcard unless encrypted, authorities must now obtain a warrant for an ISP to look at the email they handle. The Obama administration is appealing.

Other federal judges have reduced huge monetary penalties for file-sharers but also closed down major sharing website **Limewire** for massive copyright infringement. Meanwhile, an aggressive litigation firm, **Righthaven**, spread fear across the Net by suing websites reposting copyrighted news stories and photos. And the US government went on an unprecedented trademark offensive, showing its power by seizing 9 domains and shutting down 82 websites around the world for file-sharing or counterfeit goods.

Fractured future

The Internet is dividing up in other ways. National nets got a big boost from the decision to open up domain names to non-Latin alphabets. Top-level domains in general were opened up with new regions and categories - even corporate names - being added.

However, the Internet is fast running out of addresses and may well do so in 2011. The solution, called **iPv6**, is already being implemented, but the transition to the new system may be rocky - or not. Like almost everything else in our now-wired world, the situation is both unprecedented and unpredictable.

But that's what keeps things interesting. The Internet is a work forever in progress. Every new day brings novel problems, but also previously unimaginable possibilities. Stay tuned! The best is still ahead.