SWCP Portal
May 2013

The Wild, Wild Web

Can the Internet be Tamed?

The World Wide Web is now twenty years old. Invented by atomic scientists as a means of sharing their experimental results, it's a young technology that's surprisingly mature. The Web is still evolving at breathtaking speed, but it's already an unrivalled engine of commerce and a global forum for public debate, learning, and entertainment.

Mighty corporations depend upon the Internet to move their products around the planet, billions of people rely on it to communicate with each other, millions trust the information carried across it to plan and regulate their daily lives. Because this computer network of networks has become so central to modern life, both governments and criminal enterprises constantly seek to bend it to their will.

No new technology in the entire history of humanity has ever become so vital to so many so quickly. Yet the Web today is still in its infancy. No one knows what its ultimate shape will be, for no restrictions have yet been found. Benchmark after technical benchmark has been broken; lines in the sand crossed as soon as they are drawn.

The virtual frontier

For instance, scientists have long warned of approaching limits of raw computing power, expressed in terms of how many transistors could be placed on a computer chip, but there is still no real end in sight. Machines keep getting smaller, smarter, faster, and cheaper as their abilities grow ever greater and more versatile, and civilization's dependency upon them increases accordingly.

The Web today is a boiling cauldron of paradoxical possibilities both good and bad. It may look peaceful but it's really the Wild West out there. Out on the digital frontier, users must equip themselves with firewalls, antivirus programs, spam filters, encrypted connections, a cluster of passwords, and a healthy dose of paranoia every time they venture online. Sometimes even that isn't enough.

The ongoing struggle to control the Internet is happening on all levels: from the global, as the United Nations seeks ultimate jurisdiction, to the national, as Congress debates taxation policy, to families worried about their children's safety online, to users mucking out spam every day.

The tax question shows just how tangled this relationship between the real and virtual worlds can be. Until now, there really haven't been sales taxes on Net purchases. Financially-strapped states have been unable to collect from Net retailers who lack a physical presence in their state. But under the **Marketplace Fairness Act**, the larger merchants at least would have to collect sales tax from all sales. Supported by Amazon but opposed by eBay, it means that such stores would have to deal with at least 50 different tax codes and rates, possibly hundreds. Such jurisdictional nightmares will become only more common as the economy moves online along with everything else.

Events continually underline just how volatile the virtual world is, and the increasingly complex ways it interacts with the real world. Recently, for instance, the stock markets underwent a "**flash crash**" after someone hacked into AP's Twitter account to post a bogus newsflash that the White House had been bombed and the President injured. For five minutes, the market was in free fall until AP admitted they had been hacked, so instead of the beginning of a major financial panic, it was fortunately just a blip.

It wasn't a bust partly because AP is not the sole source of news. People could turn instantly to financial networks, CNN, or other sources of online information to see that it was a hoax even before the exploited news service could react. Thus, the Web can be self-stabilizing even in crisis.

Likewise, in the aftermath of the **Boston Marathon bombings**, crowd sourcing also had a vital role to play, both good and ill. While social networking sites spread information about the injured and the investigation rapidly and efficiently, they also passed on misidentifications of the bombers as well as gross pictures of the slain.

Strange bedfellows

All these conflicts are made possible by the basic structure of the Net and the peculiar historical circumstances of our times. For the Internet began as an unlikely collaboration between the **military** and **academia**. This fact alone explains much of its contradictory character.

The military wanted to link their giant mainframe computers together to share data in order to build better bombs and rockets. They also needed a robust system, open-ended and flexible enough to be extended indefinitely but sufficiently rugged to withstand nuclear attack.

Continued on back

urity rootkit malware worm troja
rootkit phishing malware worm trojan viru
t phishing malware worm trojan virus spa
ishi malware worm trojan virus spam hack
ma re worm troj hackers s
re trojan yware
m tro n virus spyw secur
ja virus spam hacke spyware sec ro
rus spam hackers spyware security rootkit
am hackers spyware rootkit phis

Continued from front

The generals turned to the geeks just as they had during the Second World War. Isolated in their cozy ivory towers, the scientists wanted to share data and multitask easily. The system they created elegantly embodied their liberal ideals as well as the military's strict requirements. It would be **transparent** from end to end. It was also **anonymous** and **egalitarian**, in that all data would be treated equally regardless of either source or destination.

Scientists built these values into the Net's core **protocols**, or agreed methods of doing things. Programs can certainly be devised to weigh, block, or trace data, but they are all additions to the protocols, not replacements. *The fact is that freedom for good or evil is built into the very foundation of the Internet*. Any attempt by anyone on any level to limit it in any way is an **application** built on top of that. And what one application can do, another can undo. Thus the arms race between white hats and black hats began.

Democracy is also built into the Net. It's run by groups of experts around the world. Every new protocol is proposed, examined, and intensely debated in **RFCs** – "*Requests for Comments*." The Internet may be that rare and wonderful thing: a tool designed by committee that actually works.

Masks of good and evil

There's an amazing amount of real philanthropy involved in making the Internet go. The Web was given to the world by CERN, the European atomic research consortium, for free, without any strings attached – probably the most generous and far-reaching act of intellectual altruism since Ben Franklin gave away the lightning rod. It's hard to imagine either happening in today's patent-crazy world.

Yet such generosity continues, largely unnoticed, daily. Countless software developers have poured their efforts, usually free and anonymously, to everything from operating systems like **Linux** into open-source creative tools like **Open Office** to Web-publishing platforms such as **WordPress**. The latest big thing, **bitcoin**, an online currency, has been described as an "alien technology" for being so advanced, yet its creators are completely unknown.

Perhaps such noble examples made the intellectuals too trusting. Knowing everyone in their small community at the start, even **passwords** weren't necessary. When **email** was invented forty years ago, **spam** wasn't a problem because everybody knew exactly who sent what message. Only after the Web was created and the Internet was split off from the military networks and opened to the world beyond academia could the dark side take root.

But establish itself it certainly has. **Computer hacking** results in the loss of untold millions of dollars a year and uncounted thousands of victims. **Cyberwar** is now an unquestioned reality, with powerful new viruses being built by states as weapons to destroy actual infrastructure.

Some countries are also building **national firewalls** to restrict political information from their own people and also vast, **unaccountable surveillance systems**. Meanwhile, gambling, pornography, and every imaginable kind of evil or disturbing material from vile racism to instructions on bomb-making can be found with just a few clicks.

Evil content and behavior degrades the true basis of the Internet. *The Net is not powered by electricity but by trust*. It works because of the voluntary cooperation of millions of people striving to make it work. Ironically, it is because of this trust that the evil which poisons it can also flourish.

The technology is so new that society has not yet evolved effective rules for dealing with it. The Internet is seen as somehow anonymous, but it's really not. Though it makes it easy to pose as someone else, it is virtually impossible to hide everything. After all, no matter how devious, each and every data packet has both a **`To:`** and a **`From:`** line.

This feeling of **anonymity** arises because so much on the Net is done individually behind a screen, usually with a made-up **username**. Like putting on a mask, this can give people an empowering sense of freedom. It makes them more likely to do things behind that presumed shield that they would never consider committing publicly in real life.

This is not only true for individual users, but entire nations. Chinese government hackers, for instance, are constantly testing limits and then denying it, a game that could turn deadly. Since the **Stuxnet virus** proved that computer viruses can wreck mechanical equipment, the lines between cyberspace and reality are being increasingly blurred. At what point do online provocations require real world responses? The answer may come written in blood.

Likely the Internet will be tamed – at least, vast stretches of it. These areas will be continually monitored and regulated, protected by **identification authentication**. With the rise of police surveillance, national firewalls, huge online shopping malls, and social networking, such **island fortresses** will inevitably link to share data and resources.

But the entire Internet can never be made "safe." Vast stretches of cyberspace are already "**dark**" – full of abandoned websites, discarded protocols, huge databases, and clandestine enterprises engaged in by both criminals and political dissidents. Like it or not such wild corners will endure, for the Internet remains a faithful mirror of the human soul, haunted by the same angels and demons of our own nature.

Vice President Jailed for Charity

SWCP believes in quietly giving back to the community, but every now and then, news of our generosity gets out. It's happened again, and this time, it's gotten our Vice President Jamii Corley, "jailed" by the **Muscular Dystrophy Association** for their annual **Lock-Up** Charity Event.

"Help, they're taking me to jail!" she said, when asked for a comment. Locked up for a good cause, Jamii needs to make bail by **May 30** at the MDA dinner meeting. Proceeds will go towards the fight against muscle disease.

For information, or to make a contribution to help spring Jamii from jail, please visit **http://bit.ly/190cXLW.** Thanks!

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994
505-243-SWCP (7927) ⊙ **SWCP.com** ⊙ **Help@swcp.com**
5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**