SWCP Portal
March 2016

Where the heroes don't wear masks, but villains do

Taming the Wild, Wild Web 1

The Internet began with a promise of a bright and wonderful future. One where communications happened at the speed of light, and the entire world was just a click away, along with all the riches of human knowledge and creativity on display.

The Web is all of that and more. But as a reflection of the human mind, the Net has its dark side, too. There are hackers, scam artists, and thieves, trolls, stalkers, and criminals selling illicit goods. And now, there is the terrifying prospect of **cyberwar**, where the actual industrial and financial infrastructure could be wrecked by unknown, invisible assailants.

It wasn't *meant* to be this way. Even Tim Berners-Lee, the inventor of the Web, **criticized Twitter** for its promotion of "negativity and bullying." How did it all go so wrong? Can the worst excesses be stopped? Will the Net ever be a sheltering environment without sacrificing privacy and freedom of expression?

How the Web became a Jungle

The Internet was born in a safe, nurturing environment – in university computer labs financed by the military. A liberal intellectual atmosphere prevailed, ironically protected and even coddled by the strict requirements and needs of the Defense Department.

Trust was built into the system from the very start. In the beginning, it was a very small community where everyone online knew everyone else. Anonymity was just not possible. So any misbehaving user, such as the poster of **first email spam** in 1978, was instantly identified and taken to task by the community.

Usernames began as a convenient shorthand and at first passwords weren't even necessary. The entire Internet was designed to be transparent and open from one end to the other. No obstacles to the free flow of information were to be permitted.

As soon as the Internet opened to outsiders, computer geeks began to explore the network. It may be hard to believe, but **hacking** was often benignly tolerated early on. Hacks were considered to be not only a way of learning, but finding new ways to do things, and a useful exploration of the limits of technology.

Of course, everything was *free* – all that was needed was access. People began putting up content unrelated to their jobs; along with serious computer science bulletin boards, sci-fi fan discussion groups quickly started up, and picture posting followed.

Academic ideals of freedom and transparency shaped the early Net, influencing its very architecture. Rigorous **identity authentication** was not thought necessary, any more than putting a tax on the brand-new form of communication, email, was. And we are still paying for this naivety today.

The first signs of future troubles were not long in coming after the networks admitted commercial players. The first **computer worm** – forerunner of so many online pests – almost took down the Internet in 1988. And **commercial spamming** began with mass ads posted by sleazy lawyers in 1994.

Living in a Masquerade

One of the peculiarities of the Internet is that while it's very hard to be truly anonymous, it's awfully easy to *pretend* to be someone else. Employing made-up usernames and fake online identities provide convenient masks to hide behind, and the privacy of interacting only through a screen and keyboard may further help bring out the very worst in people.

Thus, some users feel free to indulge in online harrassment as **trolls** with vicious comments most would never dare make face to face. Like other bullies, trolls tend to gang up on their prey. The resulting ridicule can be so withering that victims withdraw from social media, or have even killed themselves.

Continued on back

For instance, "**Gamergate**" was an ugly controversy that erupted several years ago. A female game developer was systematically harrassed by brigades of hate-filled males who claimed to be defending gaming. Some women were chased out of the industry.

Cyberstalkers, as one long-term victim **found out**, are rarely prosecuted for identity theft or anything else by law enforcement, who usually require physical threats against victims before acting. The general wisdom for dealing with rudeness is "do not feed the trolls". Engaging them usually just makes things worse. Other **steps** seem just about as ineffective.

But it may be possible to reach the *real* human beings behind vile and hurtful messages. One woman blogger who was repeatedly attacked online by a man posing as her dead father eventually bravely **told her story online**, which actually got the perpetrator to personally apologize. In time, they even talked, he reformed, and she forgave him.

Such happy outcomes are *extremely* rare, but there are efforts to deny would-be trolls the masks behind which to hide. Twitter and Facebook both ban false identities and have policies against stalking and harrassment. In Britain, moves are underway to make setting up fake accounts to abuse others **illegal**.

Childish behavior harms online communities. Comment sections at the end of articles are places where ideas and links can be shared, and on some sites are more entertaining than the articles themselves. Others, like **YouTube**, long notorious for stupid and bigoted comments, are trying to clean them up. Yet to make comment sections more appealing requires constant monitoring, and **many websites** are finding it simply not worth the unrelenting toil.

Sadly, attempts to find **algorithms** to do this automatically haven't worked. But one way to restore courtesy might be to remind users that there are real people paying attention. **Civil Comments** is a British scheme that lets other commenters rate comments – and also their own – to mobilize reasonable humans. It seeks to use "kindness and warmth" by example to gently persuade trolls to become better people.

Facebook has implemented "social reporting" as a means of defusing conflict. On request, the platform sends a polite template message to the offender to try to change behavior. It also is experimenting with "**counterspeech"** to mobilize crowds to provide positive alternatives to extremist narratives. Twitter, however, is having a **hard time** as every effort it makes is angrily denounced by its own users.

But nobody wants to spend time or cash in a hostile neighborhood. There's just too much at stake for big money to let the Net decline into a warzone.

Net Notes

Cyberwars are Happening Now

US officials have **confirmed** that just before Christmas, an attack by hackers against the power grid of Western Ukraine knocked it offline, leaving nearly a quarter-million people shivering in the cold.

This is the first such successful intrusion known, and it marks an ominous increase in the danger to our utilities, too. Though the attackers have not been identified, they are believed to be a Russian group. The hackers first inserted malware which prevented attempts to stop them from shutting down distribution switches. At the same time, they flooded the call centers with false reports to further sow confusion.

Meanwhile, the US military has also **announced** that it is conducting cyber operations against the Islamic State. A spokesman called the methods being used as "new" and "surprising" but declined to elaborate, citing the need for continuing secrecy in such matters. But they **likely** include efforts to stop ISIL from using the Net and social media to communicate, and to force them to fall back on less-secure methods.

YouTube does DIY and Fair Use

Need to fix the car? Lay down new tile in the bathroom? **YouTube**, the world's repository for cat videos, blurry UFO clips, and silly stunts, also houses endless hours of repair and fix-it spots that cover just about everything. These are of widely-varying quality, of course, but some are amazingly thorough, helpful, and professional productions.

One of the most annoying aspects of YouTube is how often pieces get removed, usually for copyright claims, often totally unwarranted. **Fair Use Tube** was started by an attorney to teach content-generators how to protect their work on YouTube and Vimeo.

YouTube has recently begun to stand up for **fair use**, too. If they decide that a video has been unfairly targeted for copyright takedown, they may **offer** to include it in a program that will keep it up (at least in the US) and even pay up to $1 million in legal costs.

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

Archived at: http://www.swcp.com/newsletters/.
Click on blue terms in PDF file to open links.