January 2022

The Forecast is Cloudy

Last year was a real roller coaster ride, and 2022 looks like it could be an even wilder ride as the various trends from previous years work themselves out. So this issue offers a brief overview of what may be in store in 2022 in regard to the internet and life online.

Covid greatly complicated everything last year, and as the plague continues to evolve, it may have a few more unpredictable surprises left before it's reduced to an endemic threat we all must learn to live with. So don't throw out your masks or delete your Zoom settings. You may still need them indefinitely.

The lure of the new

In the meantime, life goes on. The shiny new things that generated so much buzz last year – cryptocurrency, NFTs, Web 3, the metaverse – will continue to be hyped but may be revealed to be pipe dreams.

The shine may soon be gone from cryptocurrency as it comes under increasing criticism by becoming big enough to concern central banks and regulators – or they might just start **minting** them. **Non-fungible tokens** (NFTs) might also be exposed as containing little but hot air, once it's realized that ownership gives no inherent rights or value beyond bragging rights for rich investors.

Yet the **blockchain** open-ledger system central to these processes continues to be applied to real world conditions. Someday it may even safeguard voting or personal identities – but a lot of work still needs to be done.

The virtual/augmented reality of the metaverse is also just getting started. While a few outspoken critics like **Elon Musk** openly scoff at the idea that people will be willing to strap a screen over their faces all day long, the excitement and the hype keep building.

Right now, there's a **land rush** going on as competing corporations attempt to stake out virtual turf, while Meta, formerly Facebook, is charging ahead to claim all the advantages of being first. They're even working on a **haptic glove** to permit feeling and manipulating objects in online worlds.

Faster connections everywhere

A more important development – or at least one with more immediate consequences – will be the extension of high-speed broadband internet across the land. While enormous hype surrounds faster 5G phone service, that will have little effect on smartphone internet speeds in the near future.

Though it will also take some time to build the infrastructure, the biggest improvement will be a direct result of the ***$1 trillion*** Infrastructure and Jobs Act that somehow made it into law. New Mexico, and especially our rural communities, should **greatly benefit** from it.

Over ***$3.7 billion*** should come to our state. Some of that will go to research into hydrogen production and battery storage for the power grid, building charging stations for electric vehicles and of course, a ***lot*** of road and bridge work. So get ready for lines of orange cones cluttering up your commute.

New Mexico will get at least ***$100 million*** to provide broadband connections across the state for the 21% of households without net access, and benefits to help the over 38% who can't afford it. The **state Senate** has authorized ***$133 million*** to be spent on internet projects including "alternative broadband" using wireless towers, blimps, or satellites.

Satellite internet should steadily grow throughout 2022. The massive deployment of transceiver relays in low Earth orbit by Elon Musk's SpaceX Starlink program has angered not only **astronomers** but the **Chinese** and **European** space programs, and has problems on terra firma too as its ground terminals face **serious delays** of possibly **up to a year**.

SpaceX's Starlink is not the only player. **Amazon** hopes to loft its first two internet satellites in 2022 while several **other competitors** are already in service. These services may be very useful in areas with small, scattered communities far from urban centers but as users grow faster than the satellites, speeds offered will likely diminish in the near term.

Storm clouds gathering

So the good news about the future online is coming along but is still quite far away from fruition. Unfortunately, the bad news is already here and bound to get worse, judging by the huge numbers of **exploited vulnerabilities** on the government watchlist.

Criminal hacking has blossomed throughout the pandemic, particularly in ransomware attacks. Many of these have targeted poorly-defended but highly important institutions with lots of sensitive data, like hospitals. But even **Bernalillo County government** websites have recently been taken down.

While this has led to more federal involvement and cooperation **between countries** and net companies across the board, the really bad news there is that the gangs are not acting alone either. Governments which tolerated them as long as they behaved themselves in their host countries, are actively using criminal hacking groups as spies to penetrate their opposition, real and potential.

While **North Korea** has been doing that for years (and lately even against Russia), **Russia** seems to be the most aggressive and determined player. Despite assurances, it is doubtful they've cracked down on hackers.

In fact, in the wake of the game-changing **Solar Winds attack** last year which penetrated around 100 tech companies and 9 agencies, the Russians are going after foreign policy think tanks and tech providers in their efforts to crush criticism and dissent.

However the **Chinese** are not far behind, and the Iranians are still very active as well. **Microsoft** seized 42 websites used to spread Chinese malware. It said they were behind an attack on at least 13 tech firms worldwide, likely in an attempt to steal passwords and spy on sensitive communications. Meanwhile, the Iranians are carrying their covert war against Israel into the physical arena. The **Iranians** hacked water control systems in an attempt to poison people and revealed the identities of a million LGBTQ Israelis. The Israelis apparently responded with attacks on fuel supplies, railways, and airlines.

Attacks on physical equipment and the infrastructure have been steadily growing ever since the US and Israel slipped the **Stuxnet virus** into Iran's nuclear centrifuges in 2010. The malware demonstrated the vulnerabilities of many net-connected devices, with the source code to take down critical infrastructure: power grids, pipelines, and much more.

Adversaries were quick to learn from it and master the techniques themselves. Chief among these is Russia, which twice **hacked Ukraine's** power grid in the depths of winter.

Called "**hybrid warfare**", this new Russian strategy combines hacking by criminals to avoid attribution, combined with social media propaganda to sow confusion and chaos, and even special operations by the military.

This is one reason why the recent threat of invading the Ukraine is so worrisome. But our old Cold War enemy has long been practicing much of the same strategy against the US. Fake news and information, spread largely through Twitter and Facebook is a major factor in the **civil unrest** over the last several years. And the Russians are **still at it**.

Lately, a **leading figure** of the 2016 hack of the Democratic servers has been arrested. Answers may be coming at last, but they could lead to **fresh conflicts** with Russia.

Get ready for another wild year and keep your fingers crossed that it ends peacefully.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994

505-232-7992** | **swcp.com** | Tech support: **help@swcp.com
5021 Indian School NE, Ste. 600, Albuquerque, NM 87110

*Please click on **bold blue type** in text for links to sources.*