SWCP Portal
February 2020

Phishing for disaster in the fog of war.

The Shape of Cyberwar 2020

"**Cyber warfare**" is a frighteningly ominous term – especially since it is so vague. But if it doesn't involve **rampaging robots**, what does it really mean, especially since the experts say it is **already happening**?

Such doomsaying spreads much alarm but very little useful information. At least with natural disaster alerts, the government furnishes lists of resources that can help people survive the crisis and rebuild.

Not so much with cyberwar beyond the usual advice to back everything up. The problem seems to be that no one – not even the experts – really knows what total cyberwar would look like. Though people have been thinking about online conflict for at least half a century, there's never been world war in cyberspace.

However, there have been a number of cyberattacks through the decades, constantly growing in size, sophistication, and ambition. While the nature of an unlimited global online conflict can only be speculated about, there is enough history to allow a certain confidence in what some components would be.

Ancient conflicts, modern tools

Humans have made war in just about every environment where one group competed with another one, usually over controlling vital resources. In cyberspace, those resources are the networks and all the computers they link and machines they run – plus the hearts and minds behind all that equipment.

Cyber warfare is simply **defined** by the RAND Corporation as "the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks." But that definition is the only simple thing about **cyberwar**. It gets complicated fast.

War is not just spies, covert actions, or propaganda. They are merely weapons in the conflict. Similarly, cyberwar is not just espionage by hackers, state-sponsored or otherwise, nor is it **cybercrime** like fraud or ransomware demands, nor is it **information warfare**, spreading fake news and propaganda.

These can all be aspects of a cyberwar campaign but the bloody heart of cyberwar, like traditional warfare, is in the application of brute force against the enemy. But cyberwar operations can range from massive **denial of service attacks** to cripple large institutions to **hacking the phone** of the world's richest man.

Cyberwar is attractive for two reasons. First, it is quite affordable even for small and isolated nations like North Korea. It's a lot less overtly dangerous than building bombs and could even **make some money** for the country. Secondly, the internet's widely distributed nature makes it very hard to precisely pinpoint hostile attackers beyond any shadow of doubt.

Cyberspace provides an ideal arena for **asymmetrical warfare**, where a lesser power can employ guerilla tactics and deception to take on a greater one on a more equal footing. In other words, the internet becomes a battlefield where frustrated countries and movements desperate for change can **directly fight** the big status-quo-upholding powers (that is, us) yet typically avoid massive retaliation for daring to do so.

Some of these conflicts go way back, too. While America's struggle with Iran came closest to blows in the early 1980s with the **Hostage Crisis**, the trouble began *2,500 years* ago with the **Ancient Greeks** and the Persian Empire. The Persians were finally conquered by **Alexander**, but the Romans later **squandered** many legions, much treasure, and a few emperors in the sands against their successors.

The stalemate between East and West has shifted a few times back and forth since then but still endures. While nuclear weapons force nations to act with some **restraint**, it was a carefully-devised cyberattack to **deny nuclear ams to Iran** that ironically led directly to the uneasy situation the world faces today.

A short history of cyberwar

Computers were first used militarily in World War II but it was not until the Army's scientists invented online connections that actually attacking them by means of those links was made possible. When the KGB's **Cuckoo's Egg campaign** to spy on US defense companies in 1986 was discovered, **cyberespionage** had already been going on quietly for some time.

Continued on back

Continued from front

But the real wake-up call came two years later due to a prank when students at Cornell University let loose **Morris**, the first **internet worm**. Designed to spread undetected between machines, Morris took down *6,000* computers – *10%* of the internet at the time.

This came as a nasty shock to geeks who hoped the net would remain a friendly place where everyone could trust one another, but it also led to the first real attempts to improve security over connectivity.

Those efforts were found wanting a decade later. In 1998, persistent probing of the Pentagon, Energy Department, NASA and universities was detected. Having gone on for several years, it was ultimately traced back to a mainframe in the former Soviet Union. The hackers left backdoors but few traces.

Though the Russians denied involvement and US suspicions were never proven, the **Moonlight Maze** intrusion (code from which is **still being used**), was the first large-scale cyberespionage campaign by a well-funded state actor. The West woke up to future assaults that could come from unknown enemies, be invisible, and cause damages hard to determine.

Therefore, tactical defenses like **firewalls** to keep unwanted visitors out and **encryption** to keep data in were emphasized. These were the first fortifications in cyberspace. Like castles in the Dark Ages, the erection of such barriers is a sure indicator of growing general insecurity and widespread anarchy.

These "**walled gardens**" surround all the giant tech corporations including Microsoft, Apple, and so on. They are also being erected around entire nations. China's **Great Firewall** was the first but seems more concerned about controlling their own citizens' access to information than foreign hackers. But Russia just tested how its own national network could be safely **disconnected** from the global internet, too.

The web is **fracturing** fast. But much of the rising global paranoia may be due to the **actions** of our own **National Security Agency** and its allies in Israel, after 9/11 increased fears of terrorism and rogue nations, and the desires to stop them beforehand.

In 2010, a huge virus named **Stuxnet** was found, one so sophisticated it broke the security programs used to study it. **Stuxnet** turned out to be an advanced malware weapon that sought out the specific industrial control mechanisms which ran Iran's centrifuges to enrich uranium for bombs, in order to make the devices spin out of control and wreck themselves.

The good news was that it worked, slowing the Iranian program for years. The bad news was that the NSA **let the cat** out of the bag – and **not for the first time**. In effect, we **gave our enemies** the ability to hack the unsecured net devices running our power plants, refineries, water and sewage systems, etc.

The growing danger of World War Web

Cyberwar requires control of information. One side cannot tell its allies anything without also letting its foes know. So cyberwar will usually be surrounded by a thick fog of lies and confusion. Defenses are not boasted about, successful breaches left unmentioned unless they have to be disclosed, attackers left unidentified, attacks called something else. It's a battle fought in silent shadows lit only by flickering screens.

Yet there are **no rules**; attacks have steadily continued to **increase**. In response to Stuxnet, an Iranian virus **wrecked** the Saudis' oil-refining computer network in 2017, **attacking again** in 2018. The US **reacted** by **cyberattacking** Iranian air defense sites.

In 2016, President Obama warned the Russians against interfering in our elections but did little else. There's a very **good possibility** this restraint was due in part to fears that the Russians had hacked our power grid, and could turn it off on Election Day.

Indications are that both sides have been busily **penetrating** the other's critical infrastructure and hardening their own ever since. There have been several unexplained widespread **power outages** last year, too, so the tech may be tested and **ready to go**.

There's no doubt it can be done. In 2007, experimenters in Idaho **physically destroyed** an electric generator over the internet. On December 31, 2015, the Russians **shut down** the Ukrainian electric grid to *225,000* homes in the middle of winter. Luckily, the system was so old it could easily be restored manually. A year later, the Russians **did it again** along with attacks on government ministries, a pension fund, the country's railway server, and causing *$5 billion* of **damage** to systems owned by outside corporations.

Today, as with nukes, the threat of overwhelming retaliation may be our best **deterrent**. But that only works if the enemy knows he cannot hide. If the power does **go out** on Election Day, which of our foes should we blame and what should be done about it?

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**

Click on blue terms in PDF file to open links.