SWCP Portal

April 2022

Digital Dictatorships

While the Russian invasion of Ukraine bogs down in the spring mud during its second month, it may be possible to get a glimpse through the haze of battle of how the conflict is proceeding online as well as in the dirt.

The internet is just another front in this 21st century fight that continues unabated online 24/7. Details of what has been going on are constantly emerging but the big mystery remains as to why Russia did **not mount** a massive cyberattack on basic infrastructure as was widely expected by Western observers.

Perhaps it was partly due to worries about unintended effects. Commercial jets flying around the Black Sea and elsewhere found their **GPS jammed**, apparently accidentally by the Russians. Russia took down the European **Viasat satellite** system early on which disrupted Ukrainian net access but also that of thousands of German wind turbines. There have been several **powerful attacks** directed at Ukrainian telecoms, but nothing like the kind of long-lasting infrastructure damage Russia could likely unleash on Putin's orders.

A new battlefield

One reason for Russian hesitancy might be that Ukraine is better prepared. Russia used Ukraine for years to test sabotage techniques now being deployed elsewhere, including shutting down their power grid twice in the middle of winter and using crippling malware.

So US Cyber Command has been working **for years** out of European bases to **neutralize** Russian cyber offensives, at least temporarily. But permanently disabling their capabilities is going a step too far, one that might cross a "**red line**" that Putin warned about.

After the intense first attacks, local Kievan IT directors acted quickly. They **modified** the popular Kyiv Digital smartphone app so that their fellow citizens in the underground shelters can connect to the net, find open pharmacies, groceries, other shelters and receive air raid alerts with maps on their phones. Workers have installed Musk's donated Starlink dishes, too, along with WiFi units from empty offices to provide access to shelters.

Perhaps Russia's hackers are too busy to go on the offensive, for Ukraine's global **volunteer hacker army** has been very active. The efforts of the supposedly ***300,000*** unpaid actors seem well-intentioned but ineffective – like cold-calling Russian phones to get the truth out, multiple denial of service attacks which are irritating at best, and replacing restaurant reviews with war film clips. Meanwhile, others are merrily **tracking** Russian oligarchs' yachts, planes, and hidden cash.

Microsoft, **Cloudflare**, and other internet security companies have been helping out also. Russia is neither utilizing its high-grade hackers nor secure radios. Their commanders often **piggyback communications** on the local **cellphone system**. The defenders listen in and at times **target generals** for attack.

Another reason for Russian hesitation may be that any truly crippling assault by cyberweapons would be like using nukes: results are impossible to fully predict and retaliation in kind would be very likely. It's not just Putin who has marked out **red lines** in cyberspace.

President Biden has **warned** that the Russian government is exploring options for cyberattacks on Western assets in response to their heavy imposed sanctions. He's urged hardening cyber defenses, but did not share any details of what's been seen or expected. Meanwhile, the FBI remotely cleaned out a **major Russian botnet** from infected American devices just before it could be used.

Right before the war started, there was a **wave of attacks** on ***600*** Ukrainian military and government websites, an increase of ***196%*** over "normal" levels. Russia claims that it was not responsible for the attacks; and according to Ukrainian intelligence, they were joined by **Chinese government** hackers.

While Western experts think that cooperating on cyber offensives between the two authoritarian regimes is unlikely, this is not the only time it has happened. SaaS, a security firm for online software service management, claims it has recently detected surges in **hacking attempts** from both Russia and China that indicate they are working together.

The bear and the dragon

Russia and China have been authoritarian monarchies for most of their long histories. Both find free expression of thought, especially political opinions, a challenge to their ruler's authority and the state's legitimacy. Therefore, it's not such a stretch to consider that they are natural allies even in cyberspace.

However, due to historical circumstances, the relationship of the world's largest nation and its most populous one to the internet could not be more different.

Several years before the invention of the worldwide web, **communism fell** in generally peaceful revolts in Russia and points west. Around the same time, it triumphed in China with a **brutal crackdown** on peaceful protesters in Tienanmen Square on June 4, 1989.

Russia was discovering freedom even as the web was taking off. Modern Russia grew up during the Wild West phase of the web; all the repressive measures the Russian federation has adopted since Putin came to power have been more-or-less clumsy retrofits which rely more on old-fashioned offline harrassment and bullying than technical means.

The first restrictions, including a blacklist law for sites advocating suicide, drugs, or child porn and later on for "extremist" activities came after public protests against Putin a decade ago. It allowed **widespread net censorship** that doubled again last year and will probably be even much worse this year.

Since 2019, their **Sovereign Internet Law** gave Putin the power to sever Russia from the worldwide internet. **Since then**, they throttled Twitter, blocked Facebook, various opposition websites and even the Tor system; demanded access to user data, keeping it in Mother Russia, and passed a **stern law** banning "false" news, like calling the war a war.

The Russian government has also been pressuring people to use native social media sites rather than foreign ones, and lately has been pushing against outside VPNs. Yet **VPNs** are still legal; even the **Kremlin spokesman** admits to using one and they are very popular in Russia as a means to try to protect privacy.

China, on the other hand, went for economic opportunity but political repression. From early on, its leaders saw the internet as a tool for spying on the outside world and a powerful means to monitor and control the teeming millions under their rule. Despite a brief springtime of freedom, under **Xi Jinping**, China's net soon became a state tool.

Like the Great Wall which kept barbarians out, the modern Chinese built the "**Golden Shield Project**" which outsiders often refer to the "**Great Firewall**". This is a broad array of legal and technical means to monitor, control, and basically restrict Chinese internet access with the outside world. It blocks thousands of websites, including Google, and censors what information it does let in or that its own people can discuss, such as Covid.

The system is also used for mass social control. Its vast database scores every Chinese citizen on financial and citizenship scales, including use of social media. These ratings are vitally important as bad ones can cripple credit ratings and opportunities. The surveillance tech even allows instant posting of a social offender's face and name on video billboards as the person crosses an intersection.

Today's struggle between dictatorship and freedom is very real and happening on many levels, and cyberspace may be one of the most important battlefields.

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.*