The New Cold War

The news media isn’t talking about it yet, but it appears that we are now in a new cold war. I think we’ve been in it for some years now, but it was never declared, making it easy to overlook. With the media kowtowing to the very countries with which we are in this conflict, it’s no surprise that most people don’t realize what’s happening. Nevertheless, the cold war we are in today is just as real and just as dangerous as the one I grew up in.

Two predominant things were happening in that old cold war; the standoff between the now-defunct Soviet Union and NATO, with nuclear arms as the big trump card on both sides. Mutually Assured Destruction (MAD) was the official name for a policy that amounted to nothing more than “you destroy us, and we’ll destroy you in retaliation.” While all this was going on, the Soviet Union and the United States were busy in third-world countries, trying to influence the people and their politics to lean towards one side or another.

The term “third world country” originally referred to those countries that the two big superpowers were trying to influence, as they didn’t fall into either camp. The “first world” was the United States and her allies; the “second world” was the Soviet Union and her allies, and the “third world” was the battleground of ideas. The Soviet Union put a lot of effort into causing unrest in those countries just so that the United States would have to send advisors, peacekeepers, military hardware, and humanitarian aid to those countries.

Today’s cold war has those same two ingredients, with a few noted exceptions. First, there are two players on the other side; Russia and China. Neither is a superpower in the same sense that the old Soviet Union was, but together they are more than we can probably take on. Secondly, the real danger isn't intercontinental ballistic missiles (ICBMs) carrying nuclear bombs but cyber warfare. China invented this field of conflict, and Russia has invested a lot into it too. Pretty much all the multi-million dollar cyberattacks on our businesses have been from Russia.

Recently, a joint advisory of the FBI, NSA, and CSIA (Cybersecurity and Infrastructure Security Agency) warned companies that operate critical infrastructure to upgrade their resilience against cyberattacks.

Considering how many ransomware attacks have been against major American corporations, I think that's a warning that people need to take seriously.

There have been many more of these ransomware attacks than most people realize. Companies who have been affected by the attacks essentially keep their problems secret, preferring not to let investors and the general public know about it. But my son, who works in IT security, has let me in on what's going on. According to his sources in network security, Russian hackers are making much more money off of hacking into our nation's businesses than anyone realizes.

Before you go off thinking that those attacks shouldn't be any big deal and all that companies would have to do is restore their backups, and they could be up and running again, think again.

My son straightened me out on that one. Part of the strategy behind the ransomware attacks is that the hackers wait months after infecting the company’s database before making their ransom demands. So the backups are infected too. There’s no telling how far back a company would have to go, rebuilding their records, to get to the point where their records were clean. Then they would have lost all their business records from the backup to the current day.

Putin has made it relatively clear that he will not do anything about these hackers. That’s not a bit surprising, as there is no impetus for him to do so. As it stands, the hackers are weakening the United States and enriching his country. It would take a much stronger message from the White House to get him to do anything, and that’s not likely to happen under the current leadership.

So is Our Infrastructure in Danger?

We all heard about the Colonial Pipeline ransomware attack that garnered DarkSide, the hackers, 4.4 million dollars. That was the worst infrastructure attack here in the United States to date. The pipeline that was shut down provided gasoline and aviation fuel to much of the east and southeast, causing immense shortages for the few days the pipeline was shut down. Those shortages might have continued for months had the company not paid the ransom. Even paying it didn’t guarantee that the hackers would restore their computers, but most hackers will, so the next company will pay.

But what about power companies or municipal water authorities; are they in danger?

The answer to this is somewhat complicated. On the most basic level, one saving grace is that there are 23,417 electric power generating plants and more than 50,000 water utilities in the U.S. Those facilities use a wide variety of different technologies manufactured at different times.

Considering how fast computer technology has changed in the last half-century, there are many control systems, many of which use different programming languages, running all those facilities.

This is perhaps the biggest protection for our infrastructure. It would be a considerable undertaking to hack into a significant percentage of those facilities and their operating systems, requiring thousands of hackers literally. While I’m sure there is no shortage of hackers in the world, I don’t know how many of them are working for governments. China has a cyberwarfare division in its military, but little is known about it.

Any cyberattack propagated by either Russia or China would have to focus on getting the most bang for their buck since they couldn’t shut down all of those power plants and water purification facilities all at once. That means focusing their attention on the facilities, which would have the most significant impact. In other words, just like the former Cold War had ICBMs targeting our largest cities, this cold war probably has cyberattacks targeting the same places.

In other words, the safest place to live to ride out any such attack would be a smaller community with its power plant and municipal water treatment facility. There are many such communities in existence, scattered across the country.

But Wait…

When we look at cyberattacks on our infrastructure, we think in terms of some enemy taking out our power plants; but that wouldn’t be a very effective use of the workforce, considering just how many of them there are. It might be possible to take out a few of our larger cities, but not to take out everything simultaneously.

On the other hand, the February freeze of 2021 showed us just how an attack on our electric grid could be carried out.

ERCOT, the Electric Reliability Council of Texas, has come under considerable attack for its poor management of the Texas power grid during that freeze. This organization, which has been around since 1970, controls the Texas electric grid. Similar organizations manage the country’s other two electric power grids.

It seems to me all any attacker would have to do to cause significant disruptions would be to attack ERCOT and the other similar organizations that control the grid. While that probably wouldn’t shut down local power production, it would probably make it impossible to move that power around. So cities that are using more energy than they are producing would not get power from other areas of the grid. While that would not be the same as shutting down the entire grid, it would create massive problems nationwide.

This is a much simpler battle plan for the attacker. There are only 134 power control authorities nationwide, with control of most power transmission of power being controlled by only seven regional power transmissions organizations, compared to over 20,000 power producers. While I’m sure the firewalls of those facilities are probably much more robust than those of older power plants, there are much fewer of them to deal with, along with a much greater overall impact.

Calculating the actual impact of such an attack requires more information than I can find available. It probably exists but may not be published openly. Part of that is because the critical data is what areas of the country aren’t producing enough electrical power to meet their consumption. Those areas would be most heavily impacted if the means of transmitting electrical power from one part of the nation to another were disrupted.

Even in those areas, there probably won’t be blackouts to deal with, as much as there will be brownouts. That’s bad enough, not so much for the impact it will have on people in their homes as its impact on the industry. Some 36% of the energy used in the United States is used by industry. Those manufacturers can’t operate properly using less power. I can guarantee you from my own experience in the industry; they are working all the time to reduce their energy costs. The only thing they can do to reduce energy consumption is decrease operations, which results in reduced production.

This includes such critical industries as petroleum, food processing, steel, automobiles, telecommunications, and electronics. While we can all survive without buying a new car or cell phone, we can’t survive without food. Shortages in those areas, especially in food and gasoline, will result in more inflation. The impact on the country would be slower than just shutting down the grid entirely, but it would still be devastating.

So What Do We Do?

It’s virtually impossible to judge the true level of danger this cold war presents us with. Perhaps it will remain like the last cold war and be an inconvenience. It’s clear that the ransomware attacks will continue, especially that Putin has said that he won’t investigate the hacker organizations committing the crimes. Without his help, there is little that our law enforcement agencies can do.

Whether this turns into something that is truly government sanctioned by the Russians and the Chinese is yet to be seen. Leaders of both countries have become more openly belligerent since President Biden took office. That’s not to say that they weren’t belligerent before, just that they are being more open about it. I think it is clear that both leaders have been pushing their imperial ambitions for years.

The real question boils down to whether they see the United States as vulnerable and how they think our government would react to such an attack. The Democrats spent four years pushing the narrative that Trump was colluding with the Russians, but it appears that his successor might have some profound connections with the Chinese. Whether those connections are strong enough that he would let them get away with a cyberattack or whether there is anything our government could do about it is yet to be seen.

As with everything else, it will be up to us to protect ourselves. As with so many other scenarios, that means being as self-sufficient as possible. The more we can do for ourselves, the less we will be affected by any attack on our infrastructure.

Don’t just think about your need for electrical power. As I just mentioned, even a partial loss of the grid will increase the shortages we already see in our stores. While foreign goods might be abundant, the things we need most, especially food, are made here, not imported. Farmers need gasoline, and the processing plants that turn the animals and plants that they grow into the food products we find in the grocery store all require a considerable amount of electricity.