Could Our Computers Bring us Down?

A favorite theme amongst science fiction writers has always been computers taking over the world and killing people.

Since the early days of science fiction, there has been a fascination with machines that could think like humans and what those machines could do. In much of that writing, intelligent computers that were self-aware became the villain, sometimes going so far as to destroy mankind, in order to protect mankind from itself.

We have yet to see that happen, but as more and more research goes into developing artificial intelligence (AI), the possibilities of computers going bad have increased. A recent test of a simple AI, run by Facebook, garnered a lot of attention on the internet when the test was shut down, due to the computers supposedly developing their own language, which the programmers couldn't understand.

Social media being what it is, the story was blown out of proportion, garnering clicks from stories about how it was a "close call, with computers almost taking over the world."

But is that possible? One would think that programmers would write something like Asimov's Three Laws of Robotics into the AI's programming, ensuring that the computers knew who they served. But then, even if they did, would programs powerful

enough to learn from their own history and rewrite their code become able to write those laws out of themselves?

Trying to reason this all out is more than enough to give anyone a headache. But just because it is science fiction right now, doesn't mean the possibility doesn't exist. Many things that have started out as sci-fi exist in the world today. Computers and cell phones started out in the world of science fiction, and they have become mainstream today.

Cyberwarfare

But the bigger risk today isn't what the computers themselves might do, but what people using those computers might do. We are all familiar with the world of identity theft, viruses, and other crimes that hackers inflict upon society today. What started out, decades ago, as a challenging game for computer geeks trying to break into companies' computers, has turned into a massive criminal network, costing society over 600 billion dollars per year, almost 1% of the world's GDP.

Where this is going is anyone's guess. The hackers have the initiative, while dedicated IT experts, specializing in cybersecurity are constantly racing to keep up. But it has already taken the next leap, with governments getting into the act and using hacking as a tool of espionage and potentially as a weapon of war.

China was the first country to truly recognize the military value of cyberwarfare, starting their PLA Unit 61398 and other

secretive organizations back in the 1990s. These now exist both within the military and without, to explore how to turn hacking into something that could be used to the country's benefit and develop the weapons to do so. That includes using it for espionage and as an offensive weapon with the capability of shutting down an enemy country's capabilities.

Considering how much we depend on computers these days, that's a threat that can't be taken lightly. It's not whether China will use that against us, but when and to what effect. While I'm sure that our government has been pumping resources into counterespionage and counter warfare, in the battle between armament and armor, armament always has the initiative. Our people are only working to catch and stop the things which the Chinese, and others, have already developed. They can't really develop a defense for an attack that doesn't exist.

While the Chinese are known for their cyberwarfare prowess, they are not the only country investing time and resources into developing ways of using computers to attack their enemies. Other countries have delved into the murky waters of cyberwarfare, most notably Iran and Russia.

With our high dependence on computers today, access to these computers by agents of a foreign government is an extreme security risk. Remember the fear of Y2K? People were readying themselves in case everything shut down at the stroke of midnight, turning to the new century. Computers hadn't been developed with that turnover in mind and so there was legitimate concern that things would just stop working. It would be even worse today.

It is clear that we have already entered into a new era of the Cold War, at least with China and perhaps Russia as well. They have been "tickling" our cyber defenses for almost two decades, testing their hacking efforts in real-time. This has supposedly gone so far as to them hacking all the way into one of our nuclear power plants and taking it over for several

hours before the breach could be stopped.

Cyberwarfare and the Power Grid

The loss of our power grid is the nightmare scenario of today. Many writers have presented their view of what that would mean, most famously, “One Second After” and its sequels, written by William R. Forstchen. In his trilogy, the grid is lost to an EMP and the people are forced to figure out how to survive.

An EMP isn’t the only risk our energy grid faces. The grid could be brought down by solar activity or terrorist action. The sniper attack on the electrical substation near San Jose, California in 2014 is thought to be a terrorist act, a “dress rehearsal” for much more widespread action.

But the real risk to our power grid is through cyberterrorism or cyberwarfare. Many of the attacks perpetrated against our countries’ computes have been specifically aimed at the electric grid, specifically power plants. According to some sources, our electric grid receives three such attacks per day.

While I have recognized the risk of cyberwarfare to our energy grid, I have largely ignored it. The enormous variety in control systems used in our power plants, at least partially due to the massive changes in technology over the last century, when the grid was being built, has made the idea of hacking into our nation’s 22,731 power plants a herculean task. I wasn’t concerned, because it didn’t seem like a

practical undertaking for any government to try and disable that many different sources at once. How many different hacks would be needed to do that?

In the Twinkling of an Eye

But all that has changed, almost overnight. In the twinkling of an eye, the Russians' nefarious dealings in the shadows have come to light. In what will probably be considered to be the greatest act of espionage in history, Russia has managed to hack their way into over 18,000 different computer networks at once; and it has been going on for six to nine months!

The information has just come to light that the network monitoring software made by SolarWinds has been hacked by the Russians, giving them a back door into many of our country's top government organizations and businesses. What they are doing with the information they have gathered is anyone's guess, but this is clearly the biggest computer hack in history.

The real genius of this operation is that the Russians didn't bother trying to hack into the individual networks, they targeted the secure monitoring software that is used by companies and organizations to keep track of their networks. In using that method, they gained a back-door entrance into thousands of massive computer networks, in both the public and private sectors.

As of this writing, government agencies that are known to have been hacked into include the Department of the Treasury, the Defense Department, Department of Homeland Security, the Federal Energy Regulatory Commission, Los Alamos National Laboratory, Department of State, Commerce Department, and the National Nuclear Security Administration, amongst others. In addition, pretty much every Fortune 500 company uses SolarWinds software and it is clear that the Energy Department and numerous public utilities have been compromised. The Russians could shut us down, right now, if they wished.

It is actually unclear at this time just how far this breach of our nation's security reaches. It may be months before we fully know and even longer before the holes in our cybersecurity can be fixed.

According to one expert in cybersecurity who I was able to consult with, companies can't just stop using SolarWinds to solve the problem. Not only is there nothing comparable to replace it, but chances are pretty good that the software has installed alternate means of communications in those computer networks so that even if the software was removed, the Russians would still have access to our systems. It can't be shut down by blocking the avenues of communication either, unless it is acceptable to shut down the internet and phone systems nationwide, leaving them to shut down for months.

Another computer expert has opined that clearing up this mess might require buying all new computers and starting from scratch. But that would take months and would require careful examination of all the data being migrated, to ensure that it is legitimate data, without malware hidden in it. Otherwise, the cost and effort of changing over the system would be for naught.

If the Russians want to do us harm through this hack, rather than just spy on us, they have a very small window in which to do so. Now that it has happened, IT personnel nationwide are

working overtime to try and protect their companies and organizations. While they can't just pull the plug on the Russian back door into their systems, they can create software patches to close those doors. But even so, there's a good chance that the Russians could just work their way around those patches. Their hack has already told them where the computers are, what equipment is being used and what firewalls are in place. That's all they need to know, in order to find a way around them.

Where Does it Go from Here?

Now that this breach has been discovered, computer experts can begin to work on countering it. But the hackers have a huge head start. It is already known that they have been working to create other backdoors into our nation's computer networks, using the one through SolarWinds to give them a way to get those hacks in place. They've also copied entire systems, including passwords and other security information. That breach may not be repairable.

Part of the problem is that there are not enough trained IT security experts in the country to deal with the breach that we are facing. While there is a glut of low-level people who can deal with minor problems, major security breaches of this type require the most highly trained experts in cybersecurity. There aren't all that many of those around; certainly not enough for the 18,000 organizations who need them right now.

But the other thing that has happened, is that the Russians have proven it possible. As with many other things in the world, now that it has been done, it's easier for others to do it too. Who knows when we'll hear of the next such attack.

Worse than that, the countries who are doing this sort of thing aren't countries that we can trust. Both Russia and China have imperial ambitions which are currently being thwarted by the United States. Could either of them be

contemplating the same sort of grand strategy that the Japanese had in World War II? Could they see taking down the United States, through the destruction of our infrastructure, as a way of keeping the USA from interfering with an invasion of their neighbors? Could we end up being nothing more than a blip in the night in future versions of world history?

We are clearly at risk. How big that risk is, depends more on our enemies' intentions, than anything else. We could weather this storm, without hardly seeing a raindrop, or we could have our computer networks shut down at any moment, blocking our ability to work. Should that happen, it will make even the worst predictions for Y2K seem like child's pl…

Sorry, we seem to have lost communications.