From Our Pastor
December 15, 2018

Sabbath Greetings to Everyone!

While the world indulges in end of the calendar year festivities, the war continues in cyberspace. In a sense it is similar to a "cold war" in which the combatants do all the harm they can without crossing the line of overt military action.

Israel Today reported this week, "It has become increasingly clear Israel is waging a psychological war against Iran and its proxies. This is done by using cutting edge technology, exact intelligence gathering and by developing out-of-the-box solutions which give the Israeli military a decisive edge over its opponents and which aim to demoralize the enemy as we will see. Take, for example, what happened on the first day of “Operation Northern Shield” when the IDF released a video which showed how two Hezbollah terrorists wanted to inspect a robot which was brought into a Hezbollah attack tunnel near the northern Israeli city of Metulla. The camera of the robot recorded how one of the Hezbollah men was approaching the device after which a small explosive device exploded causing the terrorist to flee."

Israeli military has known about the three tunnels under construction by Hezbollah on the northern border for months but chose to wait until they were almost completed before destroying them. Hezbollah had planned to invade Israel with hundreds of combatants in a surprise attack using the tunnels, but now that will not happen. What is coming to light is the extent of the cyber war going on between Israel and Iran, along with the Iranian proxy organizations of Hezbollah and Hamas.

The "asymmetric warfare" (war between very different capabilities or armies) deployed by the Iranian axis has been a case study in future conflicts. The first time Israel used ‘sophisticated and intelligent warfare’ to counter Iran was at the end of January 2018 when a Mossad team stole a large part of Iran’s secret nuclear archive in Tehran without being detected or apprehended by the Iranians. The Mossad operation made clear Israel has excellent intelligence capacities and most likely a large network of collaborators in enemy countries. Iran and her forces are way behind in cyber tactics and intelligence gathering. Does the future of war belong to the cyber smart?

Also, this week, The New York Times reported, " A massive data breach at a hotel group owned by Marriott has been traced to Chinese hackers working for the Ministry of State Security, the country's civilian spy agency. The hack exposed data from approximately 500 million customers. It also included health insurers and the security clearance files of millions more Americans."

This report is scary but reports of Chinese military conducted cyber-attacks on industries around the world have been going on since 2014. The list of breached technology, defense, and banking company systems is lengthy. What are the Chinese up to? How do they plan to use the stolen information? Perhaps they are aware of the huge advantage that cyber smarts have given the Israelis and they are hoping to have the same advantage in the future. In addition to stealing technology about building weapons such as airplanes and rockets, there are many other applications of cyber intelligence. Extortion of politicians comes to mind.

No doubt the average person is unaware of the global cyber warfare operations going on every day. Nations around the globe are pouring huge resources into cyber military technology. How long will it take before the cyber war turns into a shooting war? It is anyone's guess, but real cyber conflict is being conducted every day.

Gives new meaning to the words of Jeremiah, " Everyone deals falsely....... Saying, 'Peace, peace!' When there is no peace." (Jeremiah 6:13-14)

Rex Sexton
Pastor, UCG Portland