

Cyber Threats:

New Levels of Violence

*“This know also,
that in the last
days perilous
times shall come.”
—II Timothy 3:1*

IN THIS SCRIPTURE, THE Apostle Paul has used a Greek word which has been translated “perilous” in our English Bible. He chose it to describe the rapidly increasing levels of fear and violence that would identify the ‘last days’ in prophecy, and which we believe mark the closing features of this present Gospel Age.

PERILOUS TIMES

The word ‘perilous’ means to be grievous, violent or difficult to deal with. It has been used on only one other occasion where it is rendered “fierce.” When Matthew recorded an incident in which Jesus encountered the violent demons, he said they were “exceeding fierce.” This adds a very meaningful perspective on the word that Paul used in his letter to Timothy. We read, “When he was come to the other side into the country of the Gergesenes, there met him two possessed with devils, coming out of the tombs, exceeding fierce, so that no man might pass by that way.”—Matt. 8:28

A TIME OF TROUBLE

When the Prophet Daniel recorded God's warning concerning events that would mark the end of this Gospel Age, he wrote, "At that time shall Michael stand up, the great prince which standeth for the children of thy people: and there shall be a time of trouble, such as never was since there was a nation even to that same time: and at that time thy people shall be delivered, every one that shall be found written in the book."—Dan. 12:1

INCREASE OF KNOWLEDGE

Daniel was then told that the great Time of Trouble would be identified by two other major and distinguishing characteristics. God told him, "Thou, O Daniel, shut up the words, and seal the book, even to the time of the end: many shall run to and fro, and knowledge shall be increased."—vs. 4

It is noted that when J. B. Rotherham prepared his emphasized translation of the Bible, he included an interesting footnote in connection with the word 'knowledge' that is found in Daniel's prophecy. It was taken from the notes of C. D. Ginsburg, an eminent Hebrew Bible scholar who was appointed one of the original members of the committee that was commissioned to revise the common version of the English Bible in 1870. Among Ginsburg's other scholarly works was the completion of his Massoretico-critical edition of the Hebrew Bible in 1894.

In his footnote on Daniel 12:4, Ginsburg indicated that an alternate meaning for the word knowledge is "calamities" or "wickedness." This adds depth of meaning and perspective in connection with the foretold great Time of Trouble and

the increasing level of violence in our day. “The fear of the LORD is the beginning of knowledge: but fools despise wisdom and instruction.”—Prov. 1:7

KNOWLEDGE REVEALED

This prophetic verse indicates God’s great wisdom in concealing certain information until the proper time for its fulfillment. The proper time for increasing knowledge was to be at the end of this present Gospel Age. It is being revealed by the Holy Spirit of God especially to those who are watching the foretold events. Some scriptures had their fulfillment at the time of our Lord’s First Advent, and others are being revealed during the time of his Second Presence. “It shall come to pass afterward, that I will pour out my spirit upon all flesh; and your sons and your daughters shall prophesy, your old men shall dream dreams, your young men shall see visions: And also upon the servants and upon the handmaids in those days will I pour out my spirit.”—Joel 2:28,29

CYBER THREATS

We are now living in a highly technical world that is run by computers. The term “cyber” is relatively new and is associated with the use of computers and the Internet. It is a prefix that describes those things that pertain to the age of information. During the past few decades, there has been a virtual explosion of knowledge, especially in the field of technology. Although statistics vary, analysts who study trends agree that the accumulated volume of knowledge is doubling every few years. Computers and the Internet are a major part of this growth,

and are becoming an essential part of everyday life. They are used in nearly every aspect of modern life—to store information, to process data, to send and receive messages, and to act as a social link.

The tremendous role that computers now play in our world has stimulated widespread criminal activity, and terrorists are using this technology as the preferred tool to attack vulnerable targets. They prey upon computer information systems, programs, and data with the intent to create violence in some form.

This transformation, in the focus of terrorist activity from the previously traditional roles to the new electronic methods, is becoming one of the greatest threats to modern society. To combat this new level of terrorism, there is much that has to be done at all levels of society, from the regional to national and international levels. This type of transnational crime becomes possible through the use of computers and telecommunications systems, and is designed to create maximum fear, confusion, and uncertainty. The goal is to shut down critical national infrastructure systems, such as energy, transportation and government operations. Cyber-terrorists have the potential to coerce, or intimidate, a certain government or its people to conform to a particular political, or social, ideology.

Efforts are being made to combat the increasing threat of cyber terrorism. The Federal Bureau of Investigation (FBI) labels terrorism as “the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.” Further to this,

the U.S. Department of State defines terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups, or clandestine agents.”

CYBER INCIDENTS

In recent years, the U.S. Department of Defense and intelligence agencies have become more aware of cyber incidents that involve certain foreign governments. This occurs when attempts are made to retrieve classified information through computer networks. It is believed that China may be involved in these high-level espionage incidents, and they have been code-named “Titan Rain.” Defense officials say that even if the information gained is not of a vital nature, it should raise serious concerns because of the potential threat. They point out that if small bits of information can be pulled together from various sources, it may yield useful intelligence. Although attacks on U.S. systems have never been linked directly to state-sponsored cyber attacks, they point to the incident in 1999 when Chinese hackers disabled three U.S. government sites after NATO bombers had mistakenly attacked the Chinese embassy in Belgrade.

ATTACK IN ESTONIA

A serious incident occurred on May 17, 2007, when a massive three-week wave of cyber attacks began in the small Republic of Estonia, which borders the Baltic Sea. The attack disabled the websites of government ministries, political parties, newspapers, banks, and various businesses. This was the first known cyber-related assault on a particular state, and it caused serious alarm across the

world. At the height of the crisis, Estonian banks were crippled, and people were unable to use their payment cards to buy bread or gas.

Russia and Estonia had been embroiled in a serious dispute that related to Estonia's decision to relocate a Russian military statue that had been previously erected in the capital city of Tallinn during the Soviet era. Tensions over the incident led to rumors of Russian state involvement in the cyber attacks. Investigators said that even if these suppositions can never be corroborated, Estonia's experience may be repeated elsewhere. It indicated the high level of vulnerabilities that have increased as the world becomes more networked. Estonia is one of the most wired countries in the world with their banking, and point-of-sale systems, and government all having moved to the Web. The cyber attacks had a serious effect on the country's total commerce.

WAKE-UP CALL

The United States faces many of the same vulnerabilities as Estonia. Public utilities, such as hydro-electric plants and nuclear power plants, are moving away from their previous and more secure systems, and toward open-standards-based systems that use common Internet protocols to connect to one another. Identifying adversaries in such a system is very difficult and leaves these files subject to cyber attacks. Many believe it is necessary to focus on reducing these vulnerabilities.

Analysts say that these cyber attacks may be compared to the Soviet Union's and China's theft of America's nuclear bomb secrets in the 1940s and

1950s. They say the possibilities of what we can lose in an all-out cyber war, including our individual and national security, is very serious, and to help remedy the situation, the United States needs a cyber force of 20,000 to 30,000 skilled experts to help fight cyber terrorism.

MALWARE

Modern cyber attacks may include the use of malware. The term ‘malware’ is a shortened form of the words ‘malicious software.’ Sometimes it is called scumware. These attacks are perpetrated by individuals, or organizations, and are intended to steal personal information, or to hijack a computer. They secretly access a computer system to perform a wide variety of hostile and intrusive actions. These may include viruses, worms, trojan horses, and other ‘bugs’ that are of a malicious nature. Symantec Corporation named Shaoxing, China as the world’s malware capital on March 29, 2010.

Another way that information may be obtained is by ‘phishing.’ Cyber criminals seek information via the Internet, including personal IDs, passwords, credit card numbers, and PINS. The information may then be sold to other criminals. Online bank accounts may be accessed, and funds transferred to another account owned by one of the criminals.

HIGH TECH BANK HEISTS

In October, 2010, international hackers used computer viruses to steal millions of dollars from bank accounts throughout the United States. Investigators reported that the modern, high-tech bank heist did not require a gun, a mask, a note, or a get-away car. It required only the Internet and

ingenuity, and it was accomplished in the blink of an eye, with just a click on the computer mouse.

Typically an e-mail is sent to computers that are located in homes, businesses, and government offices in the United States. When the e-mail is opened, the virus embeds itself in the victims' computer, recording their keystrokes and capturing user names and passwords as they log into bank accounts. Nearly \$4 million was stolen from victims in the United States. Another \$9 million was taken from accounts in England.

WIKILEAKS

At the time of this writing, the international organization known as WikiLeaks has once again been brought to the attention of the American people. Their website was established in 2006, and they claim to have built up a database of one and a quarter million documents during the first year of their operation. Its founders are various journalists, mathematicians, and dissidents from many locations around the world. In recent months, they have revealed numerous private, secret, and classified documents to the media, which has caused serious concern.

The organization's founder, spokesperson, and editor-in-chief is Julian Paul Assange—a journalist, publisher, and Internet activist from Australia. Assange was an Internet hacker during his youth and has worked as a computer programmer. He has lived in several countries, has published material on many varying subjects, and has received several awards and nominations. These include the Economist's New Media Award in 2008, and in

2009 the Amnesty International Media Award for publishing material concerning the extrajudicial killings in Kenya. In 2010, the *New York City Daily News* listed WikiLeaks as being the first website that could totally change the news. Later in the year, Assange was named the Readers Choice in *Time* magazine's Person-of-the-Year award.

EXPOSED DOCUMENTS

In April, 2010, WikiLeaks posted video from a 2007 incident in which Iraqi civilians and journalists were killed by U.S. forces. In July, 2010, the "Afghan War Diary" was released, a compilation of more than 76,900 documents concerning the war in Afghanistan that had not been previously seen. In October, 2010, the organization released 400,000 documents known as the "Iraq War Logs," and in November, 2010 they began releasing U.S. State Department diplomatic cables.

REACTION

Reaction from around the world in connection with the leaked U.S. embassy documents has ranged from anger and bitterness among some, to extreme indifference among others. Several U.S. government officials were quick to criticize WikiLeaks for exposing secret and classified government information. They point out that such careless actions harm national security and compromise international diplomacy.

In the meantime, Assange was arrested in London, England in December, 2010, and is currently out on bail at the time of this writing, and under house arrest in England pending an extradition hearing. The U.S. government is expected to request

his extradition and prosecute him for espionage. During World War I, the U.S. government enacted the Espionage Act of 1917, which made it a crime to willfully communicate secret government information that could expose national secrets. Many believe that these proceedings could provide a test to decide whether the First Amendment's protection for a free press may be permitted to extend to a worldwide website with an extended audience.

Several human rights organizations have also made contacts with WikiLeaks to inform them that they are not properly editing the names of civilian workers that are associated with international forces. Some journalists have criticized a perceived lack of editorial discretion when releasing thousands of documents at one time, and without providing sufficient analysis. Among negative public reactions in the United States, some people have characterized the organization as being irresponsible, immoral, and illegal.

HACKER'S REVENGE

Media supporters have commended the WikiLeaks organization for exposing state and corporate secrets, therefore increasing transparency, supporting freedom of the press, and enhancing democratic discourse, while challenging powerful institutions.

In what they called "Operation Payback," the network of online activists targeted financial firms including MasterCard and Visa over the recent incident involving the released U.S. diplomatic cables. The group is known as "Anonymous" which is believed to have about 2,000 hackers. They were

able to disrupt the websites of these credit card companies, and that of the Swedish prosecution authority.

Their attack came after the financial giants, along with the online payment firm PayPal, announced they would no longer process donations to the anti-secrecy group. Former U.S. Vice Presidential candidate Sarah Palin reported that her website had also been attacked by “Anonymous” and that personal credit cards belonging to her and her husband had been disrupted. She told *ABC News* that this is what happens when you exercise the First Amendment and speak against these sick un-American espionage efforts, and that Assange should be pursued like al-Qaeda.

The hackers also targeted Amazon, the internet retailer, which provoked their fury by withdrawing server space being used by WikiLeaks to host the government documents. PayPal admitted it had blocked payments to the group which was embarrassing the U.S. government, by steadily releasing a cache of more than 250,000 cables amid pressure from the State department. “Anonymous” distributed denial of service attacks, which have become the standard weapon of cyber warfare, and which temporarily crippled the companies websites. They also brought down the sites of the Swedish prosecutors who are pursuing Julian Assange, founder of WikiLeaks.

The group encouraged volunteers to download a piece of software that would allow them to remotely take control of their computers and harness their power for further attacks on their targeted firms. While the companies sought to play down the potential

impact on consumers, a spokesman for MasterCard said that its customers were experiencing a complete loss of service, and that they were working to restore normal service levels. Hackers have threatened to turn their attention on to Twitter—the microblogging website which it accuses of censoring WikiLeaks. In a statement from the group, they responded by saying, “We will fire at anything or anyone that tries to censor WikiLeaks, including multibillion-dollar companies.”

CYBER COMMAND

The U.S. Department of Defense launched the new Cyber Command (CyberCom) on May 24, 2010, that will synchronize the department’s various networks and cyberspace operations, to better defend them against cyber attacks. This recognizes the need to oversee the nation’s digital infrastructure as a strategic and national asset, and addresses the vulnerabilities of cyber attacks on U.S. military systems.

Defense Secretary Robert Gates approved the birth of Cyber Command that is a unified subdivision of the country’s Strategic Command. It will manage the Defense Department’s resources of 15,000 computer networks across 4,000 military bases in 88 countries. About 1,000 people will work at CyberCom at Fort Meade, Florida, with most of them moving over from existing jobs. Concerns have been raised over the segregation that currently exists among the different cyber networks and information resources across the military. Gates said, “This segregation detracts from natural synergies and ignores our experience in organizing to

operate in the air, land, sea, and space domains. The establishment of U.S. CyberCom will remedy this problem in the cyber domain.”

EVERY IMAGINATION OF EVIL

Jesus compared the trouble of the ‘last days’ to the time of Noah in his great prophecy in Matthew 24. God brought judgment upon the horrendous evil that predominated at the time of Noah’s flood. Concerning this, the Apostle Peter wrote, “Whereby the world that then was, being overflowed with water, perished.” (II Pet. 3:6) We learn from the Scriptures the reason for God’s severe action. “God saw that the wickedness of man was great in the earth, and that every imagination of the thoughts of his heart was only evil continually.”—Gen. 6:5

The time since Adam and Eve disobeyed the divine law, until the establishment of Christ’s future kingdom of righteousness, is termed the dark night of sin and death. “Behold, the darkness shall cover the earth, and gross darkness the people: but the LORD shall arise upon thee, and his glory shall be seen upon thee.”—Isa. 60:2

Satan has been permitted to exercise his powers of darkness and evil. “In whom the god of this world [Satan] hath blinded the minds of them which believe not, lest the light of the glorious gospel of Christ, who is the image of God, should shine unto them.” (II Cor. 4:4) “The great dragon was cast out, that old serpent, called the Devil, and Satan, which deceiveth the whole world: he was cast out into the earth, and his angels were cast out with him.”—Rev. 12:9

THE NIGHT IS FAR SPENT

The Apostle Paul proclaimed, "The night is far spent, the day is at hand: let us therefore cast off the works of darkness, and let us put on the armour of light." (Rom. 13:12) However hopeless the world's present chaotic situation appears, we are assured that the nighttime of sin, death, and darkness is 'far spent,' and that the promised king of righteousness will soon be manifest. "Therefore judge nothing before the time, until the Lord come, who both will bring to light the hidden things of darkness, and will make manifest the counsels of the hearts: and then shall every man have praise of God."—I Cor. 4:5

HOW LONG, O LORD?

Considering the evil hearts of men, we read, "The soul of the wicked desireth evil: his neighbour findeth no favour in his eyes. When the scorner is punished, the simple is made wise: and when the wise is instructed, he receiveth knowledge. The righteous man wisely considereth the house of the wicked: but God overthroweth the wicked for their wickedness."—Prov. 21:10-12

God has promised that this wicked spirit will be taken away, and men's hearts will be cleansed. "Oh let the wickedness of the wicked come to an end; but establish the just: for the righteous God trieth the hearts and reins." (Ps. 7:9) Again, we read, "O LORD God, to whom vengeance belongeth; O God, to whom vengeance belongeth, shew thyself. Lift up thyself, thou judge of the earth: render a reward to the proud. LORD, how long shall the wicked, how long shall the wicked triumph? How long shall they

utter and speak hard things? and all the workers of iniquity boast themselves?”—Ps. 94:1-4

THE DAY OF JUDGMENT

In his second epistle, Peter foretold the great events that would mark the closing features of this present Gospel Age and the approaching day of God’s fiery judgments. “The heavens and the earth, which are now, by the same word are kept in store, reserved unto fire against the day of judgment and perdition of ungodly men.”—II Pet. 3:7

Peter further explained, “The day of the Lord will come as a thief in the night; in the which the heavens shall pass away with a great noise, and the elements shall melt with fervent heat, the earth also and the works that are therein shall be burned up. Seeing then that all these things shall be dissolved, what manner of persons ought ye to be in all holy conversation and godliness, Looking for and hasting unto the coming of the day of God, wherein the heavens being on fire shall be dissolved, and the elements shall melt with fervent heat? Nevertheless we, according to his promise, look for new heavens and a new earth, wherein dwelleth righteousness.”—vss. 10-13

THE KNOWLEDGE OF GOD

The Prophet Isaiah recorded God’s ultimate purpose to bless the poor sin-sick world, and to give them an opportunity to learn of his wonderful knowledge of truth and righteousness. This will take place during Christ’s future kingdom, when men will no longer be allowed to use knowledge to further their own evil or wicked pursuits. Under the leadership of the Christ, every injurious word

or action will be met with an immediate response, and with punishment for their misdeed. “They shall not hurt nor destroy in all my holy mountain: for the earth shall be full of the knowledge of the LORD, as the waters cover the sea.”—Isa. 11:9 ■