

people employed in the financial sector, are either completely overlooking the present vulnerability of the system or are extremely complacent about it. (Just a quick look at Detroit would suffice to expose the vulnerability of a system that is dependent on a high degree of specialisation.) **Nowadays, any meaningful interruption in the international flow of manufactured goods, commodities, or funds (money, oil, and food, in particular)**

**could wreak havoc with the global economy.** Or consider what would happen should a cyber-attack be successful at some future time (which is not exactly on my wish-list, since I depend on the Internet and transportation systems). However, it would be naïve to think that a cyber-attack may never succeed. It is surely more realistic to assume that, at some time in the future, a cyber-attack will succeed in paralysing the world's power, communication, and

transportation systems, as well as the entire mechanism of government. In fact, I am convinced that the day will come when planes will be unable to take off, cards won't work, and funds won't be electronically transferable. (Brink's will be very busy on that day.)

I am extremely grateful to William Leavitt of Leavitt Capital Management for having penned the following thoughts and observations on the threat of a cyber-war.

---

## Cyber Security

William Leavitt, Leavitt Capital Management

3000 Dundee Road, Suite 101, Northbrook, IL 60062, USA

Tel: (847) 205-1300; Fax: (847) 205-1350; E-mail: [wleavitt@leavittcapital.com](mailto:wleavitt@leavittcapital.com); Website: [www.leavittcapital.com](http://www.leavittcapital.com)

**"I am often asked what keeps me up at night. Number One is the cyber threat."**

*Deputy Defense Secretary  
William J. Lynn III,  
January 2010*

When Bosnian Serb Gavrilo Princip assassinated Archduke Franz Ferdinand, in Sarajevo, in June 1914, he set in motion The Great War (before they started numbering them). As with the armies of Napoleon's wars over one hundred years before, and the U.S. Civil War, sixty-five years earlier, millions of personnel and supplies were marched or railed to sites hundreds or thousands of miles away. In 1914, the Germans marched for three weeks, to the Western front, through Belgium, with 84,000 horses.<sup>1</sup> After World War II, the cold war, global civil wars and skirmishes, and expenditures of trillions of dollars on conventional and unconventional weapons, a new threat has emerged, which can be waged from almost any location, by many different participants — cyber

warfare. Current and future wars will largely be fought with computers, rather than armies.

Whether we acquiesce or not, our lives are determined by technology and computer systems. Our electric grids, nuclear systems, water supplies, financial institutions, fuel systems, communication systems, as well as our governments, are directed by technological systems, which are subject to attack or disruption. The recent WikiLeaks disclosures indicate that low-level security clearance can access and cause the dissemination of highly sensitive, classified information. Rogue actors, whether individuals, states, or criminals, have successfully launched many cyber attacks against governments, institutions, corporations, and individuals.

The U.S. Department of Defense classified military computer networks were attacked in 2008. At a military base in the Middle East, an infected flash drive was inserted into a U.S. military laptop, presumably by a foreign intelligence agency.<sup>2</sup> The code uploaded itself to a network run by the U.S. Central Command, spreading undetected in classified and unclassified systems, creating a digital

source from which data could be transferred to computer systems under foreign control. The worst fears of the military (or any institution) had been realized: undetected, a rogue program could deliver operational plans into the intelligence networks of unknown adversaries.

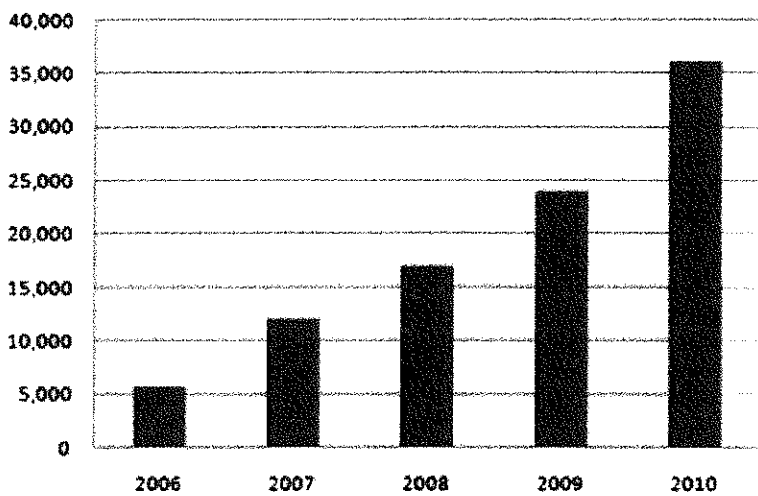
Exponentially, the number and sophistication of intrusions into military, civilian, and financial systems has increased. U.S. Congressional estimates were that U.S. governmental agencies suffered eight million cyber attacks in 2008; by March 2010, the number had risen to an average of 1.8 billion per month.<sup>3</sup> In May 2007, Estonia's government and financial institutions were overwhelmed by cyber communications, causing a shut-down. Coincidentally, the attacks coincided with a dispute with Russian authorities. In August 2008, as combat raged between Georgian and Russian forces, Georgian government internet services were attacked and rendered useless. During the fall of 2008, the height of the presidential campaign, the headquarters of both John McCain and Barack Obama were penetrated by sources attributed

1 Niall Ferguson, *The War of the World* (2006).

2 William J. Lynn III, U.S. Deputy Director of Defense, "The Pentagon's Cyber Strategy", *Foreign Affairs*, Vol. 89, No. 5.

3 "Cyber Attacks Explode in Congress", *Politico*, March 3, 2010.

Figure 1 **Cyber Incidents Reported to US-CERT in 2006–2008, estimates 2009–2010**



Source: "Cyber Security Incidents on Rise", *Cyber Security Market*, May 29, 2009

to China. In July of 2009, South Korean and U.S. government and financial institutions were attacked by cyber perpetrators linked to North Korea (see Figure 1).<sup>4</sup>

The U.K. designated the threat to its "Smart Grid" national infrastructure as a "tier one" threat in a recent study on security. Over the next five years, over 70% of U.K. energy companies are expected to deploy "Smart Grid" applications to defend against cyber attacks, according to an October 2009 report by Oracle Utilities. Even with "Smart Grid", defenders are rushing to keep pace with attackers. During the summer of 2010, Norway discovered computer attacks directed against its electric and water infrastructure, although no damage was reported. A former mathematician at the U.S. National Security Agency calculated that, given \$100 million, 750 people, and two years of preparation, a rogue state or perpetrator could launch a devastating attack on the EU, which could disable electric grids,

communications systems, air, rail, and train systems, as well as stock exchanges, financial institutions, government, and military networks.<sup>5</sup>

Particularly disturbing is the asymmetric nature of cyber war. Nations with little military capability, commercially motivated gangs, and, of course, terrorists and rogue states, can inflict horrific damage on military and economic super-powers, as well as any other nations or institutions. Often, it is difficult to identify the attacker, as an attack can be launched from remote computers and servers, making redress or retaliation problematic. For example, it has been determined that, using a \$26 off-the-shelf software item, Iraqi insurgents have the capability to hack into the live U.S. satellite feeds, providing them information necessary to evade U.S. drone attacks.

Not all attacks are directed against the U.S. or its allies. In 2010, a virus known as Stuxnet, probably the first "cyber missile" or "cyber

super weapon", was inserted into Iran's nuclear facilities, sabotaging them. The computer worm could set back Iran's nuclear efforts for almost two years, according to some estimates. Although no nation or group claimed responsibility, Iran blamed Israel for the attack. Israel has created, within its military forces, an elite intelligence group (Unit 8200), which is trained to develop offensive and defensive cyber warfare capabilities, as well as satellite and communications systems penetration and interception. It should be noted that Russia, China, and North Korea also have extensive cyber capabilities and have been blamed for attacks (see above). Of course, the U.S. has extensive cyber capabilities as well. It is expected that with a cumulative market valued at \$55 billion, the U.S. Federal Cyber Security market will increase at a compounded rate of 9.1% over the next five years.<sup>6</sup> U.S. federal cyber spending is expected to reach \$13.3 billion by 2015, in response to an estimated 445% increase in security incidents over the last four years.<sup>7</sup>

Stuxnet changed the perceptions of cyber security and the responses to it. The virus targets servers and systems which control electric transmission, nuclear and chemical plants, pipelines, communications networks, and other critical infrastructure.<sup>8</sup> In the Iranian attack, Stuxnet sabotaged special power supplies used primarily in nuclear fuel-refining centrifuge systems. Its use, in this instance, was designed to destroy a very specific target.<sup>9</sup> However, variants of the virus could be used to launch a large-scale attack against the U.S. or any other nation, damaging crucial water, power, transportation, financial, and other services, according to a report issued by the U.S. Congressional Service (CRS) on December 9, 2010.<sup>10</sup> A shortage of qualified security

4 Center for Strategic and International Studies, *Significant Cyber Events Since 2006*.

5 *Economist*, August 30, 2010.

6 Market research media, "U.S. Federal Cyber Security Forecast 2010-2015", May 25, 2009.

7 SecurityInfoWatch.com, December 3, 2010.

8 Ibid, November 22, 2010.

9 "How Stunt Cyber Weapon Targeted Iran Nuclear Plant", *Christian Science Monitor*, November 16, 2010.

10 Ibid.

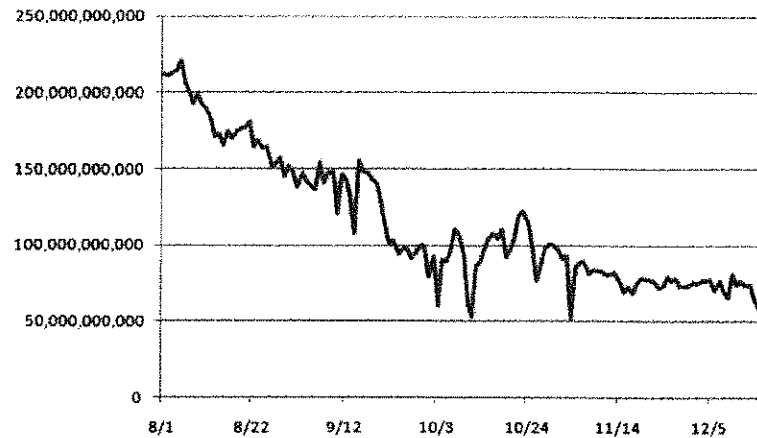
professionals required to staff the increase in cyber security activities presents a problem for the U.S.

Not all cyber activity is directed toward attacks. Many cyber systems are utilized for data gathering and analysis. Banks, airports, hotels, and other institutions not only monitor data for facial and pattern recognition, but also collect data to monitor our purchasing, travel, and other activities. Much of our beloved spam and junk mail is derived from data collection cyber activity. As recently as August 2010, over 200 billion spam messages per day were sent.<sup>11</sup> Approximately 40% of the spam results from the Rustock Botnet. Botnets infect computers belonging to unaware internet users, evading many anti-virus software systems. The computer then comes under the control of cyber rogues, who may direct the computer to perform tasks such as sending out spam messages to other computers (a single computer may be directed to send out as many as 25,000 spam messages per day) or combine with other infected computers to overwhelm websites, causing them to crash. Millions of computers are infected. More effective anti-virus systems have been developed to reduce botnets (down to less than 50 billion per day by Christmas Day of 2010), but there is evidence that spam is again on the rise (see Figure 2).

Of course, government, military, corrections, and police authorities use the data for other purposes. Some airports use eye scanning technology either to expedite the flow of pre-screened passengers, or to detect and intercept unwanted travelers. Virtually every e-mail, fax, instant message, wire transfer, text, and phone call is subject to interception by some group. Think you can remove pictures of an evening doing tequila shots, posted on a social network site? Think again. The virtual world does not erase.

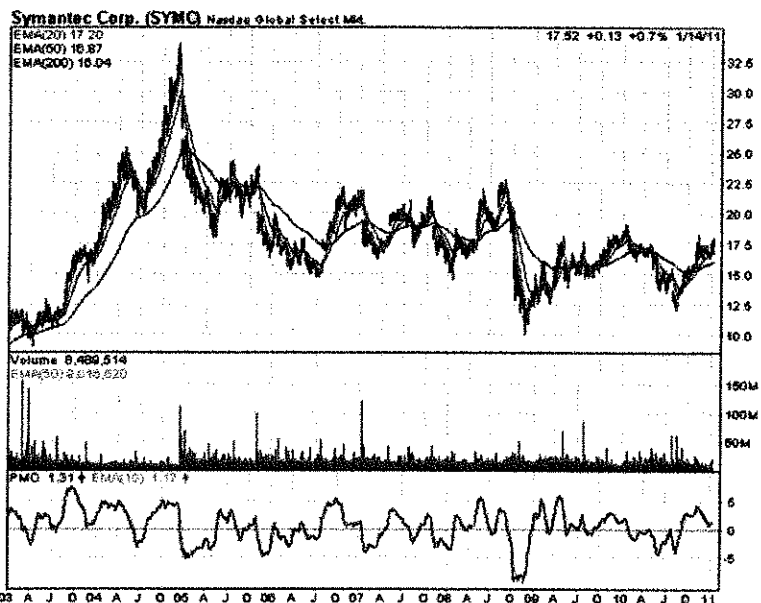
Investors can take advantage of this precarious situation. A few public companies exist which

Figure 2 Spam Volume: Global Projections



Source: Symantec

Figure 3 Symantec, 2003-2011



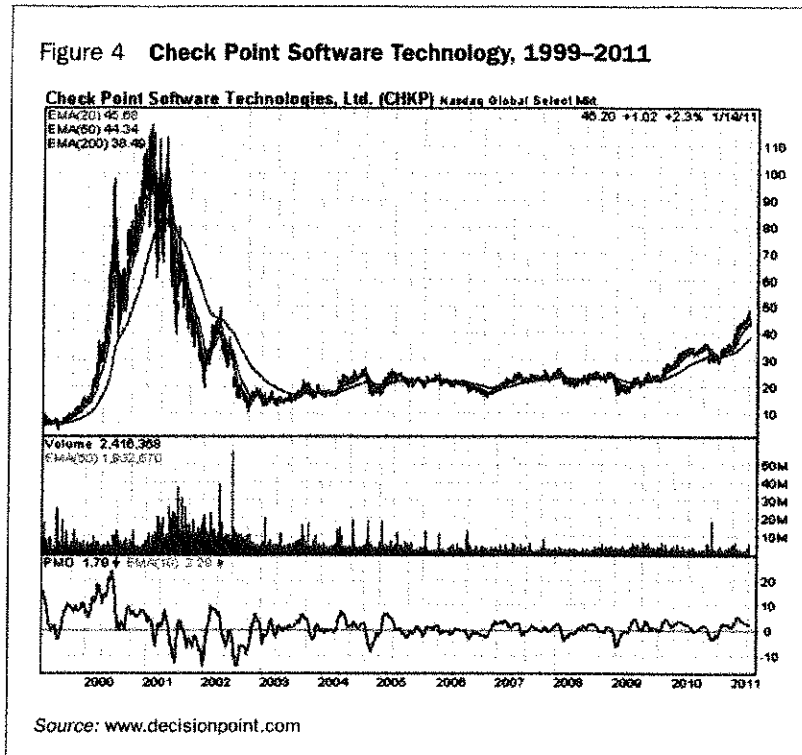
Source: www.decisionpoint.com

specifically focus on cyber threats. Symantec (SYMC: US) (see Figure 3) has developed systems to protect against botnets and other malicious computer viruses. Check Point Software Technologies (NASDAQ: CHKP) (see Figure 4), an Israeli company which recently

acquired Nokia's Security Appliances Division, is one of the premier companies in the field. Most of the cutting-edge companies are private or small public companies which have been acquired by larger groups, eager to gain a foothold in the space or expand their platforms. Fraud

<sup>11</sup> *IT Security & Network News*, January 11, 2011.

Figure 4 Check Point Software Technology, 1999–2011



Sciences, an Israeli company created by former members of Israel's elite intelligence group Unit 8200, was acquired by eBay in 2008; another Israeli company, Riverhead, a provider of cyber protection services, also founded by former members of Unite 8200, was acquired in 2004 by Cisco; and McAfee, the U.S. antivirus software company, was acquired by Intel this past summer.

We continue to search for public and private opportunities in this burgeoning area. The threats posed by cyber attacks will continue to provide involuntary buyers, which is a theme upon which we focus (like water). Technologies which do not exist today, or which are still in the incubation stage, will be on our "radar". Perhaps U.S. Deputy Defense Secretary Lynn is correct in staying up nights worrying about cyber security. While we sleep, someone is indeed watching over us.

## INVESTMENT OBSERVATIONS

I am not suggesting that investors should structure their entire portfolios, and corporate executives should take all their business decisions, based on the possibility (or the likelihood) of some shocks causing major disruptions in global trade, communication, and financial flows. However, since people insure themselves against all kinds of damage arising from adverse events, I strongly suggest that my readers take out some form of insurance against a systemic failure. I am not suggesting that a fully paid house in the countryside, in the mountains, on a remote island, or on a farm will be the best investment people can make. However, under certain adverse conditions, such a piece of property in the middle of nowhere could be one of the very few assets that will provide you with security and the basic commodities for survival, as well as with a relatively comfortable lifestyle. As Professor Ward-Perkins pointed out, we are "wholly dependent for our needs on

thousands, indeed hundreds of thousands, of other people spread around the globe, each doing their own little thing. We would be quite incapable of meeting our needs locally, even in an emergency." This would certainly apply to people living in large urban agglomerations. Conversely, people living in the countryside would be capable and more likely of meeting their needs locally. In a systemic failure, the living standards of the rural population would certainly also decline because people might not get paid (barter will immediately come into play) or they may be unable to ship their produce (energy shortages), or to communicate and get spare parts for their machines, etc. But my point is that they would be in a better position to survive, and under far better living conditions, than city-dwellers whose every necessity needs to be shipped into the city on a daily basis and where looting and crime will inevitably proliferate. Therefore, my first piece of advice is for investors to shift some of their financial assets into rural properties

— not necessarily because of their capital gain potential, but because of security concerns.

In a systemic collapse, countries like the US, Australia, New Zealand, Canada, Brazil, Argentina, Thailand, Russia, Ukraine, etc., would be in a relatively favourable position because these countries could feed themselves. **In fact, I would argue that a global systemic collapse would in relative terms benefit the US.** If an external shock interrupted trade flows, the US trade deficit would shrink and previously outsourced production would come back to the US. Standards of living would decline, but less so than in economies that depend heavily on trade flows or exports. Therefore, in a horror scenario, US equities would likely outperform emerging market equities (see Figure 5). In fact, already in 2011 we could see the US stock market outperforming emerging markets because in the current environment (symptoms of inflation showing up in food and energy prices) money printing is less damaging in high-per-capita-income