GlobalResearch
Center for Research on Globalization

“Conspiracy of Secrecy”: System Failure, Cyber Threats and Corporate Denial

By Greg Guma
Global Research, June 21, 2013
Maverick Media
Region: USA

In August 2010, when *Foreign Policy* posted an article citing credible research and directly warning oil companies worldwide that their offshore oil rigs were highly vulnerable to hacking, few people took notice.

“Computer commands can derail a train or cause a gas pipeline to burst,” warned former Bush administration counter-terrorism chief Richard Clarke in Cyber War, his book on the topic. Until recently, however, such scenarios seemed more like movie plots than foreign policy concerns, and the threat looked more domestic than foreign.

In early 2009, for instance, a 28-year-old contractor in California was charged in federal court with almost disabling an offshore rig. Prosecutors said the culprit, allegedly angry about not being hired full time, hacked into the computerized network of an oil-rig off the coast, specifically the controls that detect leaks. He caused damage, but fortunately not a leak.

After the Deepwater Horizon oil drilling disaster in the Gulf of Mexico the Christian Science Monitor reported that at least three US oil companies had been targets in a series of cyber attacks. The culprit was most likely someone or some group in China, and the incidents, largely un-reported for several years, had involved Marathon Oil, ExxonMobil and ConocoPhillips. But the companies apparently didn’t realize how serious their problem was until the FBI alerted them.

At the time, federal officials said that proprietary information – email passwords, messages, and information linked to executives – had been flowing out to computers overseas. Chinese government involvement could not be confirmed, but some data did end up on a computer in China. One oil company security staffer privately coined the term “China virus.”

The companies generally preferred not to comment, or even admit that the attacks had happened. But the Monitor persisted, interviewing insiders, officials and cyber attack experts, and ultimately confirmed the details. Their overall conclusion was that cyber-burglars, using spyware that is almost undetectable, pose a serious and potentially dangerous threat to private industry.

According to Clarke, many nations conduct Internet espionage and sometimes even cyber attacks. China has been one of the most aggressive, but Russia and North Korea are also among the players. Spying on defense agencies and diplomats has been a major focus, but strategically important businesses and even other countries have also been targeted.

In 2011, Google claimed that it had evidence of at least 20 companies infiltrated from China. According to a report in the Wall Street Journal, logic bombs were being infiltrated into the US electric power grid. If so, they could operate like time bombs.

On oil rigs, the advent of robot-controlled platforms has made a cyber attack possible with a PC anywhere in the world. Control of a rig could be accomplished by hacking into the "integrated operations" that link onshore computer networks to offshore ones. Few experts will speculate that this may already have happened. But there is confirmation of computer viruses causing personnel injuries and production losses on North Sea platforms.

One problem is that even though newer rigs have cutting-edge robotics technology, the software that controls their basic functions can be old school. Most rely on supervisory control and data acquisition (SCADA) software, which was created in an era when "open source" was more important than security,

> "It's underappreciated how vulnerable some of these systems are," said Jeff Vail, a former counterterrorism and intelligence analyst with the US Interior Department who talked with Greg Grant, author of the Foreign Policy article. "It is possible, if you really understood them, to cause catastrophic damage by causing safety systems to fail."

The name of the article, by the way, was "The New Threat to Oil Supplies – Hackers." It sounds a lot like "Bin Laden Determined to Strike Inside the US."

To be fair, the US government's failure to address private-sector vulnerability to cyber attacks goes back decades. Until recently, however, the Obama administration hesitated to challenge the status quo. Given the vulnerability of crucial infrastructure and much of the private sector, surprisingly little was being done to prepare for what sounds inevitable.

The US Cyber Command attempts to protect federal infrastructure, while various branches of the military have developed their own offensive capabilities. But not even the Department of Homeland Security is officially responsible for protecting the private sector. According to DHS Secretary Janet Napolitano, legal and privacy issues get in the way of having the government monitor the Internet or business operations for evidence of potential cyber attacks. As you might expect, business interests are wary of the regulations that might accompany government help.

Though cyber attacks have clearly happened, many leave no obvious trace. As Clarke explains, corporations tend to believe that the "millions of dollars they have spent on computer security systems means they have successfully protected their company's secrets." Unfortunately, they are wrong. Intrusion detection and prevention systems sometimes fail.

As it stands, no federal agency is responsible for defending the banking system, power grids or oil rigs from attacks. The prevailing logic is that businesses should handle their own security. Yet their experts readily admit that they wouldn't know what to do if an attack came from another nation, and assume that defense in such a case would be the government's job.

In 2011, a US Senate bill sponsored by Democrat Jay Rockefeller and Republican Olympia Snowe sought to change that, but became another victim of DC gridlock. It would have required the president to work with the private sector on a comprehensive national cybersecurity strategy, created a joint public-private advisory board, and led to a Senate-confirmed national security adviser position.

Rockefeller said the goal was “unprecedented information sharing between government and the private sector.”

James Fallows argues that the US suffers from “a conspiracy of secrecy about the scale of cyber risk.” His point is that many companies simply won’t admit how easily they can be infiltrated. As a result, changes in the law, the regulatory environment, or personal habits that could increase safety aren’t seriously discussed. Sooner or later, however, “the cyber equivalent of 9/11 will occur—and, if the real 9/11 is a model, we will understandably, but destructively, overreact.”

Articles by: Greg Guma