**John Bumgarner argues that, with the rise of cyber terror, protecting vital infrastructure is no longer just a matter of keeping bombers and armies at bay**

# ELECTRONIC WARFARE

*Power stations are just one target for cyber attacks which could have devestating consequences*

Early in 2007, the world took notice when the highly wired country of Estonia was bombarded using a simple but effective attack method called distributed denial-of-service (DDoS). These attacks were successful in disrupting dozens of the country's political websites, public e-government operations and online banking services, as well as several national online news services.

Many global media outlets have suggested that these attacks represented the first state-sponsored cyber war between countries. In truth, while the attacks were a major inconvenience to the government and people of Estonia, they were actually at the lower-end of the spectrum for cyber warfare attacks.

The Estonia attacks were not the first acts of cyber warfare publicised by the media. For several years, United States officials have reported to the media that they believe China has penetrated numerous sensitive Department of Defence (DoD) and other government systems. Many of the penetrations were aimed at acquiring information, not disabling or destroying computer systems. One of the most successful cyber operations was when an unknown group penetrated multiple US computer networks, including those of Sandia National Laboratories and the National Aeronautics and Space Administration (NASA). These penetrations were used to obtain sensitive data from compromised computers hosted by these organisations.

In a similar incident, individuals in China downloaded approximately 10 to 20 terabytes of unclassified information from the NIPRNet, the DoD's non-classified IP router network. In 2007, many British, French and German government computers were also penetrated by hackers linked to China. While these incidents cause concern, they are fairly common. Such methods are a routine part of the process through which countries gain insight into an adversary's military or economic capabilities. The same techniques used to harvest information from the German government computer systems are also used by global spies to conduct international espionage. A common rule in these types of operations is that any country that is perceived to have a competitive advantage – whether economically, intellectually or militarily – is a potential victim. Prime targets for information gathering operations other than the United States include Brazil, China, France, Germany, India, Japan, Russia and the United Kingdom.

Another way to look at these information gathering operations is as in-depth cyber reconnaissance operations. In the context of cyber warfare attacks, information collection operations are less immediately destructive than most. Still, they are strategically important to the planning and execution of future operations.

A more ominous strategic threat to industrial countries such as the United States, China and Russia is a cyber attack that targets critical infrastructures. Critical infrastructures are items considered vital to national security, economic security, or to the general health and safety of the country and its population. While destroying military targets is extremely important in all kinetic conflicts, destroying or disrupting an opponent's critical infrastructures would usually be more important to the success of the overall conflict. Every adversary needs to fully understand which critical infrastructures will cause the greatest impact on the opponent's rear operations. In most modern conflicts, the rear is considered the army's homeland because in modern warfare there are no longer clearly defined military boundaries. An adversary that exercises a strategic first cyber strike that successfully disrupts an opponent's critical infrastructures prior to battle could potentially reduce the opponent's capacity to wage war, thus influencing the overall war.

Chinese People's Daily online asserts that the cyber systems within the United States' critical infrastructure are extremely vulnerable to surgical cyber attacks that, if successful, could cripple the US economy. The article is correct in pointing out the reliance of the United States' economy on its critical infrastructure, but fails to mention that all industrial nations – including the People's Republic of China – are also susceptible to the same types of attacks. Strategic economic damage to most countries could also cause long-term social and political effects that might hinder a speedy recovery.

Probably the most perplexing national security issue when dealing with critical infrastructure protection is that the governments in most countries do not own these key sectors. Private companies in the United States control at least 85 per cent of these vital infrastructures. Private ownership places the burden for providing security for these key elements on the private owners rather than the government. But even in countries where the critical infrastructures are in government hands, the security risks are high and the threats are similar.

The most commonly cited attack against the critical infrastructures sector is one directed at an electrical power target. The economic and social value produced by electrical power is enormous in any modern economy. The absence of continuous electrical power to a given region for a few days is a reasonable inconvenience for any economy, but long-term absence is totally unreasonable. If electrical power is disrupted in a given region for greater than ten days, more than 70 per cent of all economic activity would stop.

While most other sectors are less economically essential than electrical power, the long-term disruption of several other key infrastructures could also create considerable economic instability. These other sectors include vital oil and gas, telecommunications, banking and finance, and ground transportation. The levels of possible economic loss from an attack on these sectors is potentially devastating to any given region but could potentially be even more catastrophic to a nation, especially if the disruption is to a region with a high economic output.

Quantifying the growing risks to critical infrastructures in cyberspace is a daunting task. The Department of Homeland Security (DHS) reported that cyber incidents rose 152 per cent in 2007. These incidents included an estimated 37,000 attempted breaches of non-military computer systems and more than 80,000 attacks on computer systems of the Pentagon. But the

▶

statistics only take into consideration the reported incidents and therefore do not show the scope of the real threat. The majority of all cyber intrusions are never identified, and those that are discovered rarely get reported. Furthermore, the statistics do not reveal which reported incidents were the work of a common hacker and which occurred at the hands of a highly-trained cyber warrior sponsored by a nation state. The primary reason that these statistics are not more revealing is due to the lack of adequate technical data being reported. The secondary problem with these statistics is inadequate analysis of the incidents and their relationship to other threat factors. Additionally, the reported incidents are almost impossible to accurately attribute directly to an attacker.

One emerging risk that has not received enough attention is that the capacity to wage cyber warfare is not restricted to larger industrial nations. With the rise of globalisation, technology and higher education, smaller countries could already possess – or will soon possess – this capability. The low cost compared to other military expenditures is one of the primary economic reasons for these smaller nations to develop considerable cyber warfare capabilities.

Another problem on the horizon is the emergence of newly independent countries that have the capabilities to develop satisfactory cyber warfare strategies. The majority of these countries gained independent autonomy after the dissolution of the former Soviet Union, and the bulk of them are influenced by ethno-nationalism. Many of them already have the capability of launching limited cyber attacks against those perceived as opposing their nationalism and independence.

*Fatal keystroke: attacks could come from anywhere in the world*

The continued expansion of transnational fundamentalism in the world is another looming threat on the horizon in cyber space. Probably the best example of this ever-increasing threat is the global rise of radical fundamentalism. These extremist groups normally use physical attacks to advance their causes. Some of these groups have shown that they understand the benefits of using advance technology to communicate their fundamentalist message to others that are sympathetic to their cause. A prime example of this understanding is their use of advance encryption to cloak their communications. These fundamentalist groups could greatly advance their technological capabilities by recruiting sympathetic individuals with degrees in computer science, software engineering or another applicable field of study.

Nations must realise that definable strategic boundaries concerning critical infrastructures do not exist in the cyberworld, and may never exist like those in the physical world. This was pointed out in the 1999 book *Unrestricted Warfare* written by two Chinese colonels. The book makes the case that warfare is omnidirectional on the modern battlefield. And that battlefield, the authors explain, includes cyber space.

In short, new technology has produced new threats to a nation's critical infrastructure. All nations must guard against these threats, especially in the era of economic and military manoeuvring among countries for a key position in cyber space. "So in war, the way is to avoid what is strong and to strike at what is weak." - Sun Tzu, *The Art of War*. i

John Bumgarner is Research Director for Security Technology at the US Cyber Consequences Unit

If you have any questions or comments about this article, please email us: comment@intersec.co.uk

Gavin

**Cyber espionage, and the application of national power to launch cyber attacks, is a new colour to the old game of inter-power rivalry, and Bumgarner has addressed this and its implications concisely. Sabotage remains the prevalent aim of politically motivated individuals, which he rightly addresses as a coming concern. UK sources assert that aspirations to cyber attack have frequently been expressed by groups in planning mode. Why the new capability has not been used is an open and oft-repeated question, but leading defenders state it is only in the past year or so that the capability to cause massive disruption has begun to be distributed to those with meagre skills. It is a matter of time.**

**Bumgarner draws on two long-term trends. The first is the distribution of computing power to billions of previously unconnected people – and massive computing power to companies, sub-state actors and nation states where such interconnectedness offers huge reward for growing risks. The second trend is the ever-wider distribution of the know-how to cyber attack.**

**Lower barriers to entry now exist for junior hackers as relevant know-how is shared. Twin cycles of information sharing exist – the hackers boast and the defenders share defences – but the advantage remains with the offensive. Targets proliferate, and among mega-terabytes of data being transmitted, mostly encrypted, advance warning of attack is impossible without specific intelligence. Always and inevitably, we are playing catch-up to the bad guys.**