Are We Heading Towards a 'Digital 9/11'?

By Richard de Silva

A decade on from the Al-Qaeda sponsored terrorist attacks on the US, and the way in which we, as an international community, live our daily lives continues to be shaped by those few fateful hours, whether it be the news we read on our front pages, the movies we watch, or the lengthy – and now second nature – procedures we endure at airport check-in.

In recent years, discussion has turned to the possibility of another brewing disaster, unique to our digitally dependent era; that of the large-scale cyber attack.

What was once referred to as a 'digital Pearl Harbour' has since given way to the notion of a 'digital 9/11', owing not just to the freshness of recent memory, but to an insistence upon accuracy. For it is acknowledged by most involved in the cyber domain that should a large-scale virtual attack take place, it will not be levelled primarily at military systems, but at the more vulnerable, and more vital, civilian networks.

With the feasibility of such an attack barely in question, our thoughts have instead turned to two topics: whether it is likely that such an event will occur, and whether the devastation wrought could really match the dimensions of those attacks we have already suffered.

Whether we are in fact heading towards our digital 9/11 is a big, broad question, an important question, but one that we must also avoid discussing too casually, lest we risk trivialising the very real damage and loss of life incurred ten years ago.

Some will argue that the media has overhyped the threat for sensationalist headlines. If it has, that is not altogether a bad thing. In our recent discussions with key industry figures, publicity of the cyber threat is believed to have been instrumental in the past few months in opening the eyes of the general public to its pivotal role in protecting the nation's interconnected networks.

Meanwhile, it is chilling to hear from other cyber specialists who believe that, to date, the mainstream media is still under-reporting the true scale of a potential catastrophe.

So in terms of looking at the topic properly, with attention to both the potential likelihood and impact, a need for a measured analysis of the threat is clearly needed.

Target acquired

As previously mentioned, the recently scribed Chatham House study (September 2011) detailed the lack of consistent security measures on the part of private companies in charge of the UK's critical national infrastructure. It makes for sobering reading when we consider that international forces are in agreement that CNI is the real bullseye for major and sustained disruption.

Without doubt, this state of affairs is not limited to British shores, but is a fact of life across every other part of the world. For years, we have collectively built our assets – everything from power grids, to health services, and telecommunication networks – on foundations of e-sand. While it is not beyond us to reinforce those foundations, we require a high drive for education and awareness of the need for basic resiliency.

Air Commodore Graham Wright, former deputy director of the UK Office of Cyber Security and now VP of Cyber at Northrop Grumman Information Systems, has expressed some confidence that a cyber attack on this scale will probably not happen, suggesting that people and governments have made, and will continue to make, early preventative measures.

Paul MacGregor, Director of Finmeccanica Cyber Solutions, does not share the same level of comfort. At a recent seminar, he reasoned in plain terms that "there are enough idiots in the world for one of them to do something idiotic," and that he is "almost waiting for the news report to come through."

An important aspect to consider is how we distinguish between the adversaries capable of launching this type of assault. Terrorists, for example, will strike with the purpose of promoting as much panic and disorder as possible. In contrast, organised criminals will hope to profit, thereby attacking the financial systems, or holding CNI to ransom.

Hacktivists, the new breed of protestor seen influencing the likes of the Arab Spring and the Wikileaks fallout, are generally motivated by the need to make a socio-political statement and as yet have offered no real indication that they would have any willingness or reason to do much more than temporarily disrupt websites and servers, or publicise information leaks. However, there are also the simple and more volatile cyber miscreants, often disguising themselves under the hacktivist umbrella. This latter threat has no obvious intention but, spurred by the power of being able to disrupt, decide that they will. Whether that would include a large-scale CNI attack is not something to be left to chance.

A state-on-state attack is of course what most expect as the source of such a disaster. This category, coined the Advanced Persistent Threat (APT), is not concerned with profit or panic, but is purely levelled at neutralising military opponents and expanding its own power base. Hypothetically, conventional warfare could be used in conjunction with this type of attack, disrupting communications and power to expose the target, before launching troops, ships and missiles to take advantage of the chaos.

Aside to this, any of the aforementioned threats may also be state-sponsored, effectively augmenting the adversary with better resources and legal freedoms.

We are therefore presented with a different landscape depending on the motivation behind those hackers able to bypass CNI network security, but it is just as interesting to note that all will use the same methodology, and all will have the same capabilities to wreak havoc at their fingertips.

When disruption becomes destruction

Perhaps the biggest perceived difference between a cyber attack and a traditional weaponised attack is the notion of direct loss of life.

In a recent discussion with Wing Commander Tom Parkhouse, Cyber Policy Staff Officer at the UK MoD, he expressed his view that 'cyber terrorism' is something of a misnomer. While terrorists do make use of the internet, he said, they would not be killing people simply by crashing computers. If, even in theory, a commercial airliner could be brought down with a network attack, the physical impact would then cease to be within the cyber domain and instead exist as standard terrorism, demanding of us the same responses that we have been developing for years.

In contrast, Lieutenant Commander Paul Walker, operations law attorney at US Cyber Command, urged a delegation in Berlin last month to indeed perceive the cyber domain as a direct factor in this wider picture. To do otherwise is to run the risk of devaluing the seriousness of the threat.

Walkerbacked up his position with reference to the 2009 Sayano–Shushenskaya hydroelectric power station accident in which it is speculated that a technician used a computer to restart a turbine generator remotely from 500 miles across the country, not knowing that one of the turbines was under repair. The resulting explosion not only destroyed eight of the nine remaining turbines, created an oil spill, downed power for two days and caused share prices to drop, but directly killed 75 people in the blast vicinity.

His point was that someone with the knowledge, the means, and the intention to kill at the click of a button could do so in just the same manner.

Regardless of which viewpoint you agree with, the real-time effects of such an incident will remain identical. In the long-term, the resulting fallout from a digitally crippled city has been theorised to

include rioting, traffic accidents, and the temporary disappearance of any emergency response service, all of which could quickly spiral into widespread injury or death.

Looking further ahead still, the biggest fear would be in the dissolution of an economic system, which could have similar long-term consequences to a society, and the shifting fortunes of warring nations as the conventional airstrike or land invasion.

Bending rules of engagement

All of which has led to another debate splitting the cyber thinkers down the middle. Where Walker has advised renewed thinking in terms of the impact of the cyber threat, he has also advocated an adherence to old ways of thinking when it comes to dealing with the threat for that very reason.

"The Hague conventions, the Geneva conventions – those are sufficient, in the opinion of the United States, to govern the actions of nation states in cyberspace," he said.

"Whether cyberspace has an adjunct to an actual physical attack changes nothing about the fact that the same rules apply, it's just a different medium. Land, sea, or space, warfare is warfare, and the same rules that have always applied should apply in that medium as well."

This is not a view held by all, including fellow US specialist Michael Boyer, Director of the US Army's Research-CERT (Computer Emergency Response Team), who heads up the protection of the Army's network.

"I think there is a need because while we have a lot of good treaties out there, none of them cover what we can do in cyberspace.

"If we take out the United States financial realm – all of the stock exchange – the US becomes a third world country in a heartbeat. That's how someone from the outside is going to fight a leading country like the US, the UK, or Saudi Arabia."

What a new rulebook would look like in practical terms, Boyer, much like everyone, could not say. As it stands, any notions on a new cyber convention is 'less Hague, more vague'.

Quantum leaping to conclusions

In a recent blog post, Information Operations specialist Joel Harding proposed that nations should consider a threshold percentage by way of ascertaining when enough damage has resulted from a cyber attack to justify any use of the term 'warfare'.

When 10 per cent of the water supply or banking systems goes down, he suggests as an example, national security forces should then be able to declare a 'state of war' and respond appropriately.

While logical, the spider web of problems this presents is also vast. Can you be sure of accurately attributing the attack? What if the attack is comprised of several different attacks, from different sources? If national defence forces shut down other networks to prevent further affliction, will this also comprise part of the same percentage – and what then stops that from being employed as a tool to sway military action? Can we even be sure that we would be able to effectively measure a real-time percentage of disruption while a major attack occurs?

This is not to poke holes in any theory. Indeed, we must champion all efforts to stoke creative debate on the topic before these problems arrive in force. But how close are they?

The idea of whether we are already engaged in a serious cyber conflict can be viewed as something of a Schrödinger's Cat scenario. It does not matter whether anyone is being targeted with large-scale cyber attacks or not. If we exist in a world in which such a thing is even a possibility, our response must be the same as though we are already engaged in conflict – finding ways to defend, to counter, and to, perhaps, pre-emptively neutralise the perceived threat. In other words, we are at once engaged in warfare and not at war.

That is, until someone opens the box.