Cyber-Warfare – The Fifth Dimension

December 2010

DAVID RUBENS ASSOCIATES

DAVID RUBENS
ASSOCIATES

David Rubens Associates

David Rubens Associates is a specialist corporate security consultancy offering strategic security services to individuals and organisations across the world.

DRA has worked with government agencies, NGO's, international conglomerates and major global events, and brings a mixture of strategic vision, operational experience and academic research to all of its projects, however large or small.

David Rubens, DRA's founding director, holds an MSc in Security and Risk Management from Scarman Centre, Leicester University, is a Visiting Lecturer on their Global Security and Policing MSc programme, and is currently a Visiting Fellow at the Security and Resilience Department, Cranfield University at the UK Defence Academy, specialising in Terrorism & Public Policy and Strategic Management & Leadership.

David is widely experienced at developing, delivering and managing large-scale strategic security development programmes, and has worked with government agencies and academic institutions in Asia, Africa, Middle East, Caribbean and Eastern Europe.

For further reports, or to discuss the contents, please contact
David Rubens
david@davidrubens-associates.com

David Rubens Associates
The Arches,
Maygrove Road
London NW6 2EE
post@davidrubens-associates.com

Cyber-Warfare – The Fifth Dimension

As I am writing this article, the world's super-powers are still formatting their responses to the increasingly belligerent rhetoric emanating from Pyongyang and Seoul, following the South Korean air-strikes against North Korean military bases which in turn were a response to North Korean artillery attacks on South Korean targets. Following on from recent reports that North Korea is developing enhanced nuclear facilities and that Iran is also going ahead with its civilian nuclear capability development programme, it seems that the world is heading into a new period of growing uncertainty. However, whilst all these incidents are certainly worrying, the essential problem that they pose is one of increased regional instability rather than actual national existential danger. They are, in short, remnants of what might be called 20th Century threats.

What is much more likely to be at the centre of national security and defence strategy in the 21st Century is the threat of cyber-terrorism, a problem that is still being developed as a concept, and one against which nations and government organisations have little defence.

It is indicative of the seriousness of this new source of national danger that the recent National Security Strategy, which set the framework for the Strategic Defence Review that drew so much attention for its cutting of aircraft carriers and fast jet capability, identified cyber-terrorism as one of the three Tier One priorities, along with international terrorism and natural disasters. (Tier Two threats included use of weapons of mass destruction by another state or its proxy, civil war and an increase in organised crime, and Tier Three attacks would be a conventional large-scale military attack or a large-scale toxic release from a nuclear facility).

In fact, as well as being the ideal tool for non-national actors, given that the only weapon needed is a mouse and access to the internet , it is clear that cyber-terrorism is to a large degree being seen by nations-states as offering a significant opportunity to defeat traditional enemies, albeit in non-traditional ways. China has oficially identified cyber-warfare as being its 'Fifth Military Dimension' (after army, navy, air force and rocket capability), and even the US Ambassador to China has openly admitted that Chinese attacks on US government computers has been an on-going problem for a long time. Russia launched a cyber-attack against Estonia in what was called the Estonia-Russia Cyber War in 2007, and it is also widely believed that it was Israeli cyber-experts who were behind the Stuxnet cyber-attack on Iranian nuclear facilities in September.

Although China has openly practiced using cyber-warfare capabilities in conjunction with its other, more traditional military capabilities, cyber-terrorism applications are limited only by the imagination of the person behind the attacks. What would happen if every account in every ATM in the world showed 00.00? What would happen if every traffic light in every major city turned green at the same time, and then stayed there – within three minutes all of the major cities of the world would come to a standstill. If, as a number of authorities set out, the purpose of national defense has always been based on the defense of trade and associated trade routes, then it is clear that the possibility of cyber-terrorism or cyber-warfare targeted against national economic activity has the potential to impact on the national well-being and the lives of its citizens beyond even the greatest conventional military invasion. (As an example of the scale that these attacks can reach, the Beijing Olympics suffered 12 million attacks *every day* during the 2008 Games).

The lack of clarity concerning what needs to be done in the face of international cyber-attacks is highlighted by the fate of UK hacker Gary McKinnon, who is facing a seventy-year jail term in the US for activity that would have earned him a six-month community sentence in UK. Although called 'the greatest hacker in the world' by US authorities, he claims that what he did was more snooping than an attack, and the fact that he penetrated 81 military and 16 NASA computers is perhaps more damaging to the US reputation for ensuring their own security rather than any national security threat. This follows the similar case of Matthew Bevan in the 1990's who was called 'the greatest threat to US national security since Adolf Hitler'.

Although there is no doubting the ubiquity of cyber-attacks – anyone using a Microsoft Internet Explorer knows how that feels – it is equally possible that just as modern terrorism is based on the ability to shrink the tools of conventional warfare to a scale that can be used by individuals or small groups, so the real threat of cyber-terrorism, as opposed to cyber-warfare, will come from similar individuals armed with little more than a lap-top.

And a final thought….The next time that you go through an airport security scanner, being searched for explosives and other conventional terrorist weapons, look around you and work out what would happen if one hundred people on one hundred planes used a programme built into their mobile phones to jam every bit of electronic equipment on the plane…. Safe travels!

DAVID RUBENS
ASSOCIATES

David Rubens Associates

The Arches,
Maygrove Road
London NW6 2EE
post@davidrubens-associates.com
www.davidrubens-associates.com