By Oliver Jones

Much has been made over recent years of the emerging threat of "cyber-attacks" on Western targets. Governments have become increasingly vocal on these threats, publishing a range of materials and proposing a number of policies. In the United States the government has taken steps which include the establishment of the US "Cyber-Command", alongside the US senate debating a so called "kill switch bill", which proposes to grant the president emergency powers over the internet.  In the UK the cyber threat is also a growing concern. The recent Strategic Defence and Security Review and the UK National Security Strategy have both identified the sphere of "cyber Security" as a "Tier 1" threat or risk . Outside of government circles the issue is also becoming increasingly debated. Recently the popular periodicals "Foreign Affairs" and "The New Yorker" have both released articles detailing and debating the issue.

What however is the threat from this new "cyber domain", does it represent a new paradigm in warfare? Popular perceptions stemming from fictitious sources, such as the 2007 blockbuster Die Hard 4.0 in which the US comes under assault from "cyber-Terrorists" who target key infrastructure to cause a "fire sale" attack with potentially devastating consequences, suggest that cyber-warfare represents a devastating new strategic weapon capable of the kind of destruction only previously threatened by "WMD's". What's more the threat of cyber-attack is also characterised as being an emerging "asymmetric" threat. This idea of cyber-war is also lent credence from sources such as "Unrestricted Warfare," a proposal for Chinese military strategy, written by two Peoples Liberation Army colonels, whereby China seeks to beat a technologically and military superior opponent through the use of imaginative strategies which utilise measures that avoid direct military confrontation and instead attack their adversary through other avenues. Also adding to this perception of the cyber threat are the events like those in Estonia in 2007, where the Government and other sectors came under sustained denial of service attacks during a diplomatic spat with Russia over the relocation of "the Bronze Soldier of Tallinn". This and similar ideas certainly suggest that cyber-war does represent a threat in this way and this idea has been championed by American authorities on cyber-war. Richard A. Clarke, a former White House official with responsibility for the field, this year published "Cyberwar" a proposal for US strategy which prophesizes a particularly apocalyptic vision of a Chinese cyber-attack with mass casualties.

However there is evidence to suggest the contrary, particularly for states such as the US and

UK. For a start, if cyber warfare is so devastating, what is to stop traditional measures of deterrence from being utilised against the state based threat? The perpetrators can still be fought with conventional weapons. Professor John Ferris has likened this new unknown quantity of cyber warfare and the cyber threat to the post-Revolution in Military Affairs (RMA) military to the "downward spiral of C3I over radio, where jamming and the need for security sapped most of its flexibility and power", it does not neutralise conventional weapons, merely makes them harder to use by restricting RMA advantages. If China or some other state launches the kind of devastating attack that is feared, with mass civilian casualties (assuming this is possible), surely the party on the receiving end would resort to a crude and very blunt uranium filled response.

Arguments that suggest that cyber-attack of this nature is "un-attributable" also lack credence. In terms of a state based threat, no state will initiate this kind of offensive just because they can, and if it is initiated planners will be fairly certain who the enemy is. Finally states like China and Russia have little interest in this form of attack, as Hersh points out in his New Yorker article. With their economic interests vested so heavily in the US, why would they hurt themselves unless they were already in a state of war?

So the real threat of cyber-attack is not some form Cold War-esque vision of a cyber-first-strike, a devastating counter-value assault targeting and turning the infrastructure of a state against its government and people. Instead the threat from cyber-space echoes that defining conflict of the twentieth century in a different but no less significant way.  The real threat from state based actors lies in its utility as a tool of intelligence services. Cyber-espionage is a growing danger for developed states, in particular the threat from scientific and technical espionage remains perhaps the most pervasive threat.

Throughout the Cold War the KGB and the GRU, the intelligence services of the USSR, demonstrated an impressive ability at the collection and use of scientific and technical intelligence gathering. The gathering of this form of intelligence remained a significant priority for the intelligence services of the USSR. According to Christopher Andrew, Felix Dzerzhinsky, father of the Cheka (and arguably the Father of the Chinese Ministry of State Security, modelled on and trained by the Soviet services) identified what he called "the achievements of foreign technology" as an intelligence target. In 1949 it was the achievements of Soviet scientific and technical collection that brought the Soviet Union the atomic bomb, with the first soviet bomb to be tested being an almost exact copy of the weapons developed under the MANHATTAN project. Later on the VPK (Military-Industrial Commission)  provided "shopping lists" of acquisition targets. By 1980 successes on the "shopping list" was around one third of items collected within 12 months (1,085 of 3,617).

This hunger for information did not end with the Cold War. The United States National Counterintelligence Executive's "Annual report to Congress on foreign economic collection and industrial espionage" for the Financial Year of 2007 identifies Russia and China as being the primary collectors of scientific and technical intelligence in the United States, whilst the 2008 report clearly specifies the growing prevalence of the use of Cyber technology for this role "Cyber threats are increasingly pervasive and are rapidly becoming a priority means of obtaining economic and technical information. Reports of new cyber-attacks against US Government and business entities proliferated in FY 2008. Several adversaries expanded their computer network operations, and the use of new venues for intrusions increased."

This threat is not limited to the US. Scientific and technical espionage against the UK and other European states has a long history. Speaking recently to the IISS, Iain Lobban, director of GCHQ stated: "It is true that we have seen theft of intellectual property on a massive scale, some of it not just sensitive to the commercial enterprises in question but of national security concern too. As Jonathan Evans said in September, cyberspace lowers the bar for entry to the espionage game, both for states and for criminal actors."

However it is not merely Scientific and Technical collection which can be seen as an identifiable cyber-threat, though it may be the most predominant, also identifiable is the use of cyber technologies and attacks for other forms of intelligence collection. In 2009 attacks, dubbed "Operation AURORA", against Google were blamed upon Chinese authorities. Whilst these attacks did have a focus in part upon technical information, one of the apparent aims was also to gather information on human rights activists and other "subversives" based in China. This kind of COMINT targeting demonstrates that states are well aware of the value of cyber approaches to counter-intelligence and counter-subversion as well as positive collection. Media sources also suggest that PRC organisations have extensively utilised cyber methods for other positive intelligence gathering. In 2009 China again, reportedly, gathered information on over 103 countries through what has been dubbed "GhostNet". Trojan horses apparently compromised systems of a number of embassies and allowed their creators to eventually gain control of some computers remotely.

Cyber techniques have also been utilised as a "force multiplier" for some more traditional espionage techniques. The recent arrest of SVR "deep cover" agents in the US highlighted the use of information technology for passing information between agents and handlers in a form of 21st century "brush pass". It has been reported that Al Qaida and affiliated groups have resorted to virtual "dead drops" utilising unsent e-mails to maintain more secure communications.
Overall it is clear that the cyber-threat is real, and a significant danger to the UK and allies, but this is less about the well-publicised threat of a war-like scenario. Instead this threat is a real

intelligence issue, a counterintelligence threat to western states of significant danger. Combating this threat then should focus on increasing counterintelligence power, especially "offensive counterintelligence". If Western states really wish to secure themselves from the real cyber threat, renewed efforts need to be taken to gain counterintelligence victories, not military ones.