IDSS COMMENTARIES (30/2005)

IDSS Commentaries are intended to provide timely and, where appropriate, policy relevant background and analysis of contemporary developments. The views of the authors are their own and do not represent the official position of IDSS.

National Security Strategy in the Age of Revolutions in Security Affairs

Bernard Loo*

6 June 2005

Strategy, in the words of Grant Hammond of the US Air War College, is the harmonization of purpose and power in tune with the changing strategic environment. That last element of strategy, the strategic landscape, is widely written about, yet often least understood in its impact on how we think about security and strategy. A strategy should deal with objectives, the resources needed to accomplish these objectives, and a plan that allows for these resources to accomplish the desired objectives. But even if these were all present, they could be irrelevant if one misinterprets the strategic environment in which they are to be employed. It sounds facile to argue that a new strategic environment requires us to devise a new strategy for national security, but more often than not, policy-makers tend to cling onto legacy modes of thinking in this most important of issues.

The New Strategic Environment

Some commentators have suggested that 4th generation warfare – the use of insurgency and terrorist tactics against technologically superior military opponents – has been the dominant pattern of conflict and war since the end of World War Two. It is worth noting that all the victors of World War Two have been defeated by insurgency. At the same time, states continue to pose salient security concerns in the international system, as the recent concerns over North Korea's nuclear ambitions and the on-going Sino-Japanese spat attests.

In the military world, new types of weapons technologies are coming on-line – directed energy weapons such as lasers or microwaves or electro-magnetic pulses. Typically, these weapons have two aspects – they can have either precise or volumetric effects, and they can be lethal or non-lethal. However, their impact on warfare remains unknown. How one deals with these emerging weapons technologies is a question that has also challenged the best minds currently available.

Ironically, the very technologies that promise to make military organizations much more efficient at killing – the so-called revolution in military affairs – are equally available to the non-state militant or terrorist. Three key aspects of this revolution stand out. First, many of the technologies that underpin this revolution have to do with the collection and dissemination of information, and sensors of all kinds are becoming increasingly ubiquitous. Second, these technologies have radically increased operating speeds in all areas of work and life. Third, they are small and cheap. There almost seems a law of inverse proportions between exponential increases in computing speed and exponentially decreasing sizes and costs.

What complicates matters further is the ease with which non-military actors can access militarily significant technologies, most of which are dual-use civilian-developed, relatively cheap, and commercially available. Just about anyone can access accurate overhead satellite imagery, night vision devices, micro-satellites, and sophisticated satellite-based secure encrypted communications, as well as conventional and unconventional weapons of all kinds. All it takes is a laptop computer and a credit card, both of which can be stolen. The ability to wage war, or at the very least inflict significant amounts of physical damage is no longer the exclusive domain of states. Al Qaeda (as the prototype of a globally-based, well-educated, organized, trained and financed 'insurgency') may be the harbinger of an even more formidable 5th generation warfare – high-technology insurgencies.

It is bad enough that states have such capabilities. But since states have both territory and a populace, there is at least the theoretical possibility that a deterrent may still be found. All it takes is finding the right 'buttons' – what the other party values above all else, and threatening to destroy that value if the other party acts inappropriately in the first place. However, deterring a non-state actor may not be so straightforward. If we accept the usual argument that suicide terrorism is borne out of poverty, disenfranchisement, disillusionment and despair, how do we deter a terrorist who subscribes to an ideology that promises religious identity, cultural legitimacy, political significance, economic guarantees to one's surviving family, and paradise through suicide?

Responding to the New Strategic Environment

This new strategic environment certainly tempts one to throw up one's hands in despair, as there seems little that states can do to definitively ensure their security and survival. But, as noted, the problem is that while much has been written about this new strategic environment, little has been done to properly understand its actual impact on security and strategy.

Take the idea of deterrence, for instance. The argument that terrorists cannot be deterred stems from poor strategic understanding. Deterrence is essentially about what Edward Luttwak calls 'suasion' – a combination of persuasion and dissuasion. It is about causing a change in the thinking concerning attractive courses of action for another actor – whether state or individual or terrorist organisation. If one actor initially seeks to harm another actor, but suddenly changes his mind, this is deterrence. Deterrence, however, is multi-faceted. It can be active or passive, it can be general or specific, and importantly for the analysis here, it can be expressed through denial or punishment.

Punishment tends to be the dominant paradigm through which we think about deterrence. To some extent, it has to do with the circumstances in which most of us come to know of the term: specifically, in our understanding of the Cold War era, of two nuclear superpowers deterred by the threat of global nuclear holocaust. This is deterrence by punishment – seeking to exact extreme punishment on the opponent for his actions. This is not the way that conventional military powers, however, deter potential aggressors. Conventional military deterrence is essentially about denial - making sure that the opponent is convinced that he cannot realise his objectives - and must thus seek alternative goals.

The same logic applies to the current strategic environment. It is not that deterrence relates only to inter-state aggression; it is equally applicable to aggression that emanates from non-state sources. It all boils down to denial. That said, it is true that deterrence by denial is inherently problematic. First, it lacks the near-absolute certainty that characterised nuclear

deterrence by punishment: there is nothing to guarantee that the aggressor may *still* believe that he can get through to the target, despite all the counter-measures the latter has in place. Nevertheless, the emphasis in this sort of deterrent strategy is ensuring that the deterrent message is internalised by the potential aggressor.

Second, deterrence by denial takes a long time. Conventional military deterrence rests on the credibility of the military organisation, in terms of its material capabilities and its willingness to act as it threatens. This logic is however complicated by aspects of conventional military power that cannot be measured accurately. For example, how does one know that the opponent's military is indeed as well trained as it claims? In the current strategic environment, it means that states have to expect that counter-measures against non-state aggressors will take a long time – both in constructing and perfecting these counter-measures, and in convincing non-state aggressors that these counter-measures will work – thereby deterring them.

The problem with such an approach is that it is essentially passive and generalised. States have to anticipate the likely modes of aggression, and then prepare the necessary counter-measures. The desire to have a deterrent strategy that is both active and specific is understandable, but even in inter-state relations, active and specific deterrence has always been possible only when specific intelligence and forewarning of specific threats have emerged. Failing which the temptation for a more proactive strategy – such as pre-emption – becomes even stronger. In this respect proponents of the revolution in military affairs point to the increasing accuracy of weapons systems, and the ability to precisely destroy targets with minimum collateral damage. But we would do well to remember that accurate weapons require accurate intelligence, and the latter is inherently more problematic than the former. These proponents do not claim moreover the absence of collateral damage, but only the minimum. All it takes is one innocent civilian to become this 'collateral damage', before a nearby journalist or even another civilian with a camera mobile phone, and pictures of this 'collateral damage' will be circulated within minutes round the globe, with serious political repercussions.

Slowly, Slowly

The counsel therefore is patience. This is a long-haul phenomenon, and the plausible solutions are similarly long haul in nature. The construction of a credible defence – whether conventional or nuclear, state or terrorist-oriented – is something that never takes place overnight. It is the cumulative impact of years of capacity building underpinned by long-term investment in capability acquisitions, combined with years of demonstrated willingness to deploy these capabilities. While passive defences against terrorist activities might smack of a 'Maginot mentality' (with all its attendant negative implications) the temptation to seek a strategic quick fix through a policy of pre-emption should be approached with great caution, if only because of possible unintended "blowback" effects. These blowbacks, if anything, can only undermine states' continuing efforts to devise a coherent national security strategy in the face of an ever-changing strategic environment.

---

* Bernard Loo is an Assistant Professor at the Institute of Defence and Strategic Studies, Nanyang Technological University. This is a personal comment.