

The New Strategist Journal

Published by the Changing Character of War Programme,
University of Oxford and the Defence, Concepts,
and Doctrine Centre, UK Ministry of Defence

Volume 1, Issue 1

Contents

1 Editorial Comment	3
2 Soft Power in Theory and Practice GRAEME P. AUTON AND ROBERT J. JACKSON	5
3 Making Sense of Strategy's Relational Nature LUKAS MILEVSKI	9
4 Fighting Complexity With Complexity: Recognising the New Science in NSS WILLIAM RUSHWORTH	20
5 Uncertainty in National Security Strategy: 'What the Old Lady of Thread-needle Street could teach the old men of Whitehall.' JAMES SLADDEN	40
6 Education and the General: Educating Military Executives RANDALL WAKELAM	59
7 Space Security and Strategic Stability JING ZHONG	72
8 Collateral Damage, Covert Operations and American Exceptionalism: An Interview with Chris Woods RODERICK MCKENZIE	85
9 Drones and the RAF: An Interview with Sqn Ldr Keith Dear JAMES FERGUS ROSIE	96
10 On the Ethics of Drone Strikes, Optimism and Obscuring Language: A Conversation with an Anonymous Academic CHRISTIANA SPENS	101
11 Review: Ramsay, Gilbert (2013), Jihadi Culture on the World Wide Web (Bloomsbury: New York) RODERICK MCKENZIE	106
12 Review: Gary J. Bass (2014), The Blood Telegram: Nixon, Kissinger and a Forgotten Genocide (Hurst & Co: London) CHRISTIANA SPENS	108

The New Strategist

The *New Strategist*, the journal of the Development, Concepts and Doctrine Centre,¹ aims to acquaint readers with excellent and innovative interdisciplinary articles in strategic studies that address the pressing concerns of leaders in the fields of defence and security. The journal does not present UK Ministry of Defence policy, opinions or beliefs; every article independently stands or falls on its intellectual merit.

The *New Strategist* is interested in strategic thinking and thinking about strategy, but it is not limited only to debates about theory and decision-making. Instead, it spans a wide field of view. In addition, it aims to combine cutting-edge theoretical advances in defence and security theory with recent findings in empirical and practitioner-focused research. The *New Strategist* encourages innovative analyses across disciplinary boundaries that challenge conventional approaches and promotes critical and creative thinking in matters that impact upon defence and security.

The *New Strategist* welcomes submissions from academics and policymakers across the arts, humanities, and social sciences and including such disciplines as international relations, political science, military history, strategic studies, political sociology, political economy, anthropology, organisational and management studies, and all fields related to defence.

The *New Strategist* aspires to be a forum for ‘disruptive’ thinking, critique, challenge, and innovation.

¹<https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre>

Editorial Comment

What is changing in the character of war?

The last two decades have given some strong indications about the general trends of war, as well as indicating the specific challenges of any stabilisation operations. Yet from a strategic perspective, there has been relatively less change. The United States continued to lead the world in security matters, and its pre-eminent position in global affairs, while challenged, remains more significant than any other state. Even violent non-state actors, although inflicting casualties on Western military personnel in operational theatres in Iraq and Afghanistan and on civilians through acts of terrorism, have not once diverted American foreign policy.

In 2015, there were changes in the strategic landscape in other parts of the globe. China continued its path of economic development without challenging the United States, and Russia, while evidently antagonised enough with the West to overturn international law through its invasion of Ukraine, first in the illegal annexation of Crimea and then through support for separatist elements in Donbass, found itself unable to dissuade Kiev from closer association with Europe. Indeed, its use of force almost certainly drove Ukraine closer to its Western neighbours rather than from it.

An even more significant development in strategic terms was the continued destabilisation of the Middle East and North Africa. Unrest of varying severity continues from northern Nigeria in an arc across to the head of the Gulf. At the epicentre of the violence are the civil war in Syria and its neighbouring conflict in Iraq. These conflicts, and that of Yemen to the south, have become strategic issues in that they no longer concern only government forces trying to suppress infuriated populations, but international terrorist movements, confrontations between major powers and proxy conflicts that stir sectarian sentiments across the Muslim world.

There are also themes that straddle regions of the world and constitute important aspects of the strategic environment. The inexorable expansion of the internet, digitised data traffic and the 'arms race' between protective tools and new viruses have begun to affect the strategic 'real world' and will almost certainly make transformations that contemporary analysts have barely begun to conceive of. Moreover, the unceasing international competition for markets and resources is being transformed by the enabling power of electronic communications. This intensity offers both opportunities and penalties, perhaps even future rivalries and conflicts.

This journal is called the *New Strategist* because there has been a widespread feeling amongst analysts that the Western powers have lost the clarity of purpose, creative thinking and breadth of interest to develop strategies that achieve results. Sir Hew Strachan, the former Chichele Professor in the History of War at Oxford, wondered if strategy had become a 'lost art', and lamented the indulgent ideological

approach to international intervention that characterised the period 2001-14. Others have argued that strategic thinking is the best one can hope for, since making ‘a strategy’ is too nebulous and unreliable to guarantee success. Few can agree even on the definitions of the term, such as the degree of military involvement compared with the other so-called ‘levers of national power’. Many historians insist that strategy can only be understood in the context of its time, which prompts critics to elucidate on the need for entirely new thinking for the parameters of the ‘wired’ (electronically connected) twenty-first century.

Over the coming years, as the New Strategist establishes itself, we hope that authors will assist in assessments of this global strategic context, illustrating how precise, original and empirically grounded research can make a significant difference to our thinking. We also hope it will provide a valuable check on the hasty and often ill-conceived journalistic or ‘op-ed’ approach favoured by busy policy-makers, for we believe there is no substitute for well-argued, reasoned and careful research.

Dr Robert Johnson
Oxford, January 2016

Soft Power in Theory and Practice

GRAEME P. AUTON AND ROBERT J. JACKSON

In this assessment we define, analyze, and evaluate the meaning and especially the utility of ‘soft power’. There is no doubt that this concept has had wide currency in international studies as well as playing a major role on the world stage, at least in American politics.

For two decades, the concept of ‘soft power’ has been associated with Professor Joseph S. Nye, who first mentioned the notion in *Bound to Lead: The Changing Nature of American Power* and then wrote about it in a Foreign Policy article, ‘Soft Power.’ (Nye 1990) In his 2004 book Nye defined ‘soft power’ as co-optive power based on attraction:

[S]oft power is more than just persuasion or the ability to move people by argument, though that is an important part of it. It is also the ability to attract, and attraction often leads to acquiescence. Simply put, in behavioral terms soft power is attractive power. . . Co-optive power – the ability to shape what others want – can rest on the attractiveness of one’s culture and values or the ability to manipulate the agenda of political choices in a manner that makes others fail to express some preferences because they seem to be unrealistic.’ (Nye 2004, pp. 6-7)

Yet, Nye is certainly *not* the originator of the idea of ‘soft power’ in international relations scholarship. When Hans Morgenthau, in his celebrated *Politics among Nations* talks about national character, national morale, and the quality of diplomacy and government as elements of national power, he is talking about ‘soft power.’ Morgenthau argues that ‘the observer of the international scene who attempts to assess the relative strength of different nations must take national character into account, however difficult it may be to assess correctly so elusive and intangible a factor.’ (Morgenthau 1967, p. 128) ‘National morale,’ defined as ‘the degree of determination with which a nation supports the foreign policies of its government in peace or war,’ is fundamentally a form of ‘soft power,’ with at times critically important consequences — as Lyndon Johnson and Richard Nixon learned during their war in Vietnam.

Morgenthau would readily concede that power projection as cultural attraction goes back at least to Thucydides and Pericles’ funeral oration. Yet, Nye makes no mention of Thucydides in *Soft Power*, and in *The Future of Power* simply equates the ancient Greek with ‘the dominant classical approach to international affairs. . . realism.’ (Nye 2011, p. 18) Nye acknowledges the exercise of soft power by

France in the 18th century and Britain during World War I, but makes the odd observation that ‘though the concept of soft power is recent, the behavior it denotes is as old as human history.’ (Nye 2011, p. 81)

In truth, of course, it is the *nomenclature* of ‘soft power’ that is recent; the idea, and invocation of the concept, is very old, as is the wisdom to understand that ‘soft power’ is not the inverse of ‘power politics.’ Even Nye concedes that ‘there is no contradiction between realism and soft power. Soft power is not a form of idealism or liberalism. It is simply a form of power, one way of getting desired outcomes.’ (Nye 2011, p. 82) This concession aside, Nye muddies an already imprecise concept into a ‘baggy’ dualistic typology.

Nye is equally dismissive of constructivism, despite the obvious relevance of the core constructivist argument to his soft power thesis. It seems reasonable to argue that constructivists are ultimately talking about a form of soft power, yet nowhere in either *Soft Power* or *The Future of Power* is constructivism even mentioned. As Alexander Wendt explains ‘The distribution of power may always affect states’ calculations, but how it does so depends on the intersubjective understandings and expectations, on the ‘distribution of knowledge,’ that constitute their conceptions of self and other.’ (Wendt 1992, p. 397)

By the time one finishes Nye’s work it is clear that ‘soft power’ encompasses every application of power other than the application of (or threat of applying) hard military power or tangible economic coercion. ‘Soft power’ embraces not only cultural and political attraction, but also traditional diplomacy, intelligence cooperation, military-to-military contacts, psychological operations (‘psy-ops’), confidence- and security-building measures (CSBMs), public diplomacy, multinational enterprise, and various other kinds of multilateral undertakings.

Nye, however, rejects the criticism that the concept is overly expansive, emblemized in Leslie Gelb’s remark that ‘soft power now seems to mean everything.’ (Gelb 2009, p. 69) Writes Nye:

Many types of *resources* can contribute to soft power, but that does not mean that soft power is any type of *behavior*. The use of force, payment, and some agenda-setting based on them I call hard power. Agenda-setting that is regarded as legitimate by the target, positive attraction, and persuasion are the parts of the spectrum of behaviors I include in soft power. (Nye 2011, p. 20)

This is misleading. Nye exaggerates the distinction between hard and soft power, but more importantly he commits a logical oversight. The major problem, as Nye grudgingly notes, is that the success of ‘soft power’ is inordinately dependent upon the cooperation of its target, or at least on the ease with which the target can be ‘co-opted.’ If the target is not cooperative, if no ‘attraction’ has been consummated, then — according to Nye — no soft power has been exercised. The argument is therefore tautological. ‘Soft power’ is present when it is successful, and absent when it is not.

Lacking a standard for the existence of soft power, Nye provides only a crude definition based on target ‘behavior.’ With soft power, the analyst seldom knows when it has failed, because there are so many other factors that might account for failure. In its dependence on a target state’s (or society’s) behavior, ‘soft power’ is rather like the concept of deterrence. In both cases success or failure rests in the hands of the target state or audience. The difference, of course, is that the tools

of coercion on which deterrence depends are largely in the hands of the state. The tools of soft power, on the other hand, are diffused throughout society and cannot easily be brought to bear in support of state policy. There is no guarantee whatever that their effects will produce strategic advantage. Colin Gray has brilliantly argued that soft power is not (and cannot be) a discretionary tool of policy because its use cannot be regulated, adjusted, calibrated or planned. '[S]oft power is very different indeed as an instrument of policy. In fact, I am tempted to challenge the proposition that soft power can even be regarded as one (or more) among the grand instruments of policy.' (Gray 2011, p. 30)

Nye tries to rescue soft power as *an instrument of policy* and as *a substitute for hard power* by broadening its definition to include virtually all instruments of foreign policy other than the use (or threatened use) of hard military and economic coercion. In *The Future of Power* he attempts to finesse the fuzziness of the distinction between 'command power' and 'co-optive power' by invoking the concept of 'smart power,' which incorporates a combination of both, but which again is an outcomes-based, *ex-post facto* concept. (Nye 2011, pp. 8–9, 11, 16, 22–23) 'Smart power' is present if the policy outcome is successful, and not present if the policy is a failure.

Finally, Nye's analysis is oddly partisan. Like most American liberals and neo-conservatives, he is enamored with the idea of American exceptionalism. He is convinced that 'soft power' is a uniquely American instrument of policy; that the shining 'city upon a hill' remains a reality despite such tawdry adventures as the Vietnam disaster and the 2003 invasion of Iraq. This remains the case despite attempts by Hu Jintao to claim soft power for China, Putin for Russia in Crimea, or the Cameron Government for Britain.

Ultimately, Nye's soft power thesis should be seen as part of his career-long effort to disavow the arguments of political realism. He mechanically equates realist thinking with the use of force. However, no serious scholar of international relations, and no policymaker seeking to advance the interests of a government, would ignore 'attraction' as a component of policy outcomes. Even Clausewitz, the scion of European *Machtpolitik*, identifies the enemy's *will* as the primary target of influence, in an invocation of soft power fully consistent with Nye. The problem is that cultural and political magnetism is an unpredictable tool of policy, unless one hopelessly expands 'soft power' to include diplomacy, alliance building, intelligence cooperation, and the like. No doubt, some realist scholars are too dismissive toward the idea of 'attractiveness,' but that has not been the case for the realist school as a whole.

The bottom line is that 'soft power,' as a concept, presents serious analytical and practical problems. These problems are not addressed in Joseph Nye's recent work, despite his invocation of sloganeering notions such as 'smart power' and other examples void of evidenced-based analysis. Indeed, the only remaining question may be – how 'soft' is 'soft power'?

References

- Clausewitz, Carl von (1976). *On War*. Ed. and trans. by Michael Howard and Peter Paret. Princeton University Press.
- Gelb, Leslie (2009). *Power Rules: How Common Sense Can Rescue American Foreign Policy*. Harper Collins.

- Gray, Colin S. (2011). *Hard Power and Soft Power: The Utility of Military Force as an Instrument of Policy in the 21st Century*. Strategic Studies Institute, U.S. Army War College.
- Morgenthau, Hans J. (1967). *Politics among Nations: The Struggle for Power and Peace*. 4th. Knopf, Alfred A.
- Nye, Joseph S. (1990). "Soft Power". In: *Foreign Policy*. Autumn. Vol. 80.
- (2004). *Soft Power: The Means to Success in World Politics*. Public Affairs.
- (2011). *The Future of Power*. Public Affairs.
- Thucydides (1998). *The Peloponnesian War*. Transl. Walter Blanco. W. W. Norton.
- Wendt, Alexander (1992). "Anarchy is what States Make of it: The Social Construction of Power Politics". In: *International Organization* 46.2, pp. 391–425.

Making Sense of Strategy's Relational Nature

LUKAS MILEVSKI

Relating military means to political ends — that is to say, the crux of strategy — remains the most important question in strategic studies. It is also perhaps the least explicitly studied, due both to the inherent difficulty of accomplishing the task in practice and to the commensurate challenge of reflecting upon it in general theory. Any inquiry is beset by the need to consider myriad variables, each of which may be of decisive importance in one particular context yet insignificant in another. The result tends to be a theoretical morass, inhabited both by undeveloped Clausewitzian truisms and by sloppy thinking. Strategic studies should be able to build upon the solid foundations left by Clausewitz while eschewing undisciplined thought and theory.

General theory has difficulty incorporating strategy's relational nature in detail because so much of that relational nature is context-dependent. This article aims to explore that relational nature without neglecting the importance of contextual details during the actual practice of strategy; instead it seeks balance general theory against the strategist's need to create specific theories of victory in practice.

Reaffirming classical strategy

The meaning of strategy has been lost, and with it much of the actual art of both practical and theoretical strategic thinking. (Strachan 2005, pp. 33-54) This loss is due, in large part, to the unique connotations of the word 'strategy' which make it more desirable than any other related or more appropriate word, such as 'policy' or 'plan.' As Sir Lawrence Freedman aptly notes, 'strategy remains the best word we have for expressing attempts to think about actions in advance, in light of our goals and our capacities. It captures a process for which there are no obvious alternative words, although the meaning has become diluted through promiscuous and often inappropriate use.' (Freedman 2013, p. x) A frequently seen inappropriate usage is one which actually places the concept of strategy above policy — so that policy is meant to serve strategy, and not vice versa! One commentator even suggested, '[t]he natural inclination is to view strategy as supporting policy, rather than the reverse. . . . But strategy is more than this: it is the grand design, the overall mosaic into which the pieces of specific policy fit. It provides the key ingredients of clarity, coherence and consistency over time.' (Foster 1985, p. 14) The relationship between strategy and policy is thus nearly impossible to determine simply due to confusion as to which is the master and which the servant.

This reaffirms the classical conception of strategy as its purest and clearest interpretation. ‘Strategy is the bridge that relates military power to political purpose; it is neither military power per se nor political purpose. By strategy I mean the use that is made of force and the threat of force for the ends of policy.’ (Gray 1999, p. 17) Unlike the promiscuous use of ‘strategy’ prevalent beyond (and occasionally within) strategic studies, classical strategy carries with it a particular focus which informs both its everlasting nature and the central aspects of its varying character. Classical strategy is concerned nearly entirely with war, as both the word and the concept were recovered from the ancient world for the purposes of describing the military conduct of war.

War is at the heart of strategy, whether we use strategy within war the better to direct it, or whether we use it in peace to threaten war in support of our political objectives. . . Part of our current confusion about what is or is not a war, and whether war itself does or does not have utility, derives precisely from our inadequate grasp of strategy. One of the most obvious uses of strategy is to provide us with the tools to understand better the nature of war. (Strachan 2011b, p. 23)

The relationship between strategy and policy is thus caught up in and subsumed by the larger relationship between war and policy. Amongst Clausewitz’s most famous pronouncements is his determination that war is a continuation of policy by other means — specifically, violent means. This appears to be a simple statement, but it must be heavily qualified. As J.C. Wylie has suggested, ‘[w]ar for a nonaggressor nation is actually a nearly complete collapse of policy. Once war comes, then nearly all prewar policy is utterly invalid because the setting in which it was designed to function no longer corresponds with the facts of reality.’ (Wylie 1989, pp. 67-68) Hew Strachan similarly suggests that today we ‘fail to recognize how often states go to war not to continue policy but to change it. The declaration of war, and more immediately the use of violence, alters everything. From that point on, the demands of war tend to shape policy, more than the direction of policy shapes war.’ (Strachan 2011a, p. 508) Clearly, the relationship between war and policy — and therefore between strategy and policy — is highly complex due to the respective natures of both war and policy.

War contains its own escalatory dynamic due to its adversarial nature, as opposing belligerents seek to defeat one another for their own purposes. Clausewitz thoroughly explained this particular facet of the nature of war. ‘So long as I have not overthrown my opponent I am bound to fear that he may overthrow me. Thus I am not in control: he dictates to me as much as I dictate to him. . . If you want to overcome your enemy you must match your effort against his power of resistance. . . But the enemy will do the same’. (Clausewitz 1984, p. 77 This is the main dynamic by which the demands of war may capture the direction of policy as Strachan warns. Strategy thereby, in the face of armed resistance, threatens to become the master of policy rather than its servant and executor.

On the other side of the relationship, policy is always composite. It is never a monolith, but a compound always comprised of at least two parts. This is not a reference to the divide between domestic and foreign policy, although this is one additional complicating factor, nor is it an observation that any polity may have differing foreign policies toward India, Russia, China, etc., which similarly complicates policy-making. Rather, any policy is always comprised of at least two aspects

which together ultimately determine whether the policy has or has not been successful. First, there is the aim of the policy itself: does the West desire to maintain the territorial integrity of Ukraine; does the United Kingdom desire to revitalize its naval power with the construction of two brand new aircraft carriers; etc. Second, at what cost the achievement? This is the condition attached to the policy goal. The West was prepared to support Ukraine's sovereignty short of war. Thus the West was unprepared to employ military force to sustain Ukraine's sovereignty, despite the overall ineffectiveness of its statecraft. Thus if Ukraine does not retain territorial integrity, Western policies will have failed, but also if the West had gone to war over Ukraine, its policies would have failed. The United Kingdom has similarly found the cost of two carriers to be perhaps too high and its policy position awkward. In some cases the condition is judged more important than the goal itself. In other cases the policy goal is determined to be worth more than the condition attached to it; thus Joseph Chamberlain's peace at any price crumbled in the face of the clear need to stop Nazi Germany.

The relationship between strategy and policy is thus dynamic, complex, and often nonlinear. For this reason, strategic studies frequently eschews serious discussion of this relationship beyond endorsing or, sometimes, condemning Clausewitz's well known assertion that war is the continuation of policy by other means. Colin Gray aptly observed that '[t]he trouble is that there is a radical difference in nature, in kind, between violence and political consequence... this dilemma of currency conversion is central to the difficulty of strategy.' (Gray 2010, p. 136) One result of this difficulty is that Western militaries prefer to avoid consideration of this currency conversion (as being well above their professional pay grades) in favor of conceiving of and acting in a politics-free operational level of war where generals must consider only purely military factors. Policy thus de facto maintains its significance only in starting and ending the war. Although frequently such an interpretation is attributed to Clausewitz, it is actually a Moltkean perspective on the relationship between war and politics. Moltke wrote in 1871 that '[p]olicy uses war for the attainment of its goals; it works decisively at the beginning and the end of war, so that indeed policy reserves for itself the right to increase its demands or to be satisfied with a lesser success.' (Hughes 1993, p. 44) It does not or should not, however, affect the course of operations. By contrast, Clausewitz wrote that '[w]e want to make it clear that war in itself does not suspend political intercourse. The main lines along which military events progress and to which they are restricted are political lines that continue throughout the war.' (Clausewitz 1984, p. 605) Politics cannot help but inform the practice of strategy, because strategy is practiced for the sake of political gain. Tension between these two perspectives concerning the relationship between strategy and policy remains rife even today in strategic studies, in academic circles as in actual practice.

Clearly, the relationship between strategy and policy is difficult to master in practice and possibly more difficult to elucidate in the writing of theory. The general theory of strategy, to fulfill the promise implicit in its name, must be at a sufficiently high level to encompass and comprehend the practice of strategy in all of history, from that of the Egyptians and Hittites at Qadesh to the present day. Yet it should not falter in the face of Bernard Brodie's basic questions about the practicality of strategic theory in any given context of practicing strategists.

Strategic thinking, or 'theory' if one prefers, is nothing if not pragmatic. Strategy is a 'how to do it' study, a guide to accomplishing something and

doing it efficiently. As in many other branches of politics, the question that matters in strategy is: Will the idea work? More importantly, will it be likely to work under the special circumstances under which it will next be tested? (Brodie 1973, p. 452)

This underlines the tension between strategy as general theory and strategy in practice as a context-specific theory of victory. How should a strategic theorist go about balancing the general comprehension of strategy in all of history with its necessary context-specific contribution to strategic practice?

Exploring strategy's relational nature

Strategy guides the employment of armed force toward beneficial political utility. A general theory of strategy must, at the least, create and encourage common meaning between two mutually foreign considerations. As with mathematical fractions, undertaking such a unification requires identifying the fundamental common denominator upon which both rest. For strategy and policy, this denominator is power as expressed in politics. Unlike politics, policy is not fundamental. Its position is actually somewhat anomalous; it is both the result of one set of processes (politics) and the guiding light for another (strategy). Politics is continually evolving; policy constantly strives to catch up to politics, therefore strategy is also constantly catching up and changing. The making of strategy and its consequences also loop back to impact the course of politics and so also impact policy.

Policy is a previously agreed-upon course of action determined as a result of political processes, which may be domestic, international, or both. Politics is concerned with fundamental issues, which go by many names despite being approximately the same thing. Harold Lasswell has defined politics as who gets what, when, how. Examples of 'what' include deference, income, and safety. (Lasswell 1972, p. 13) Politics itself is, to repurpose Basil Liddell Hart's definition of strategy, the distribution and employment of power. Power, properly employed, may provide or account for everything else. Any chosen policy therefore only represents the accepted and anticipated changes to that distribution and employment of power.

It is thus arguably more useful to consider not strategy with policy but strategy and *politics*. Politics is not merely the result of choices about power, but also the ebb and flow of power. Policy is just a particular configuration for the use of power to influence its future distribution. Strategy and politics embodies the more fundamental relationship, for, as noted above, the need to practice strategy in war may well represent a failure of policy rather than its continuation.

Power is difficult to measure because it is necessarily relational; it is a meaningless concept without another party against whom to act in competition. Moreover, because it is relational, one's own power may be upset by the actions of others. Thus any policy must assume the requisite freedom of action to enact anticipated changes to the distribution of power by the relevant instruments of political power. This basic insight applies as much to the development and implementation of policy in domestic settings as in international ones. A politician working to improve his polity's future would pursue the enactment of policies which are realistic — that is, are achievable because the freedom of action exists to implement those policies. Freedom of action becomes even more important in conflict. As the French general André Beaufre proposed, '[a]ny dialectical contest is a contest for freedom of action.' (Beaufre 1965,

p. 110) This is especially true in war, which is by definition a highly charged situation which differs greatly from that of relatively peaceful domestic politics.

War is adversarial by nature. Each strategic actor's freedom of action is therefore limited because the mutual introduction of violence changes the efficacy of all non-violent instruments. Non-violent instruments, such as economic or diplomatic pressure, retain some utility and effectiveness in the longer-term or in contexts where the use of force is not an immediate concern. However, such instruments cannot directly resist military force, which has the potential to trump all other forms of power in an immediate situation. Freedom of action in war thus necessarily revolves around the relative capabilities of each belligerent to threaten and use violence. Violence attains such centrality because, in war, the involved parties have each already determined that violence will be the prime instrument of political achievement.

War is also meant to be instrumental. 'On the one hand it is about a purposive activity, geared to the demands of personal, group, and national security. On the other it is about the grim consequences of conflict.' (Freedman 2012, p. 17) This anticipation of instrumentality impinges upon a strategist's freedom of action. The practicing strategist should not act counter to the political interests for which he is striving. Thus tactically plausible actions may be politically — and therefore strategically — undesirable. A strategist's concern with freedom of action is thus not only a concern about his enemy and what that enemy is capable of doing. It is also about how his own choices and actions affect the feasibility of achieving his political goal — the desired redistribution of power between the belligerents in question. As Geoffrey Blainey asserted in a wonderfully minimalistic manner, '[w]ar itself is a dispute about measurement; peace on the other hand marks a rough agreement about measurement. . . Wars usually end when the fighting nations agree on their relative strength, and wars usually begin when fighting nations *disagree* on their relative strength.' (Blainey n.d., p. 122) A strategist should not act in a manner which decreases the power of his polity below that of his enemy. Policy therefore may also restrict a strategist's freedom of action from undertaking actions which, although tactically feasible, may not have desirable strategic or political consequences.

Clausewitz's definition of war remains one of the most clear and concise yet offered: '*War is thus an act of force to compel our enemy to do our will.*' (Clausewitz 1984, p. 75) It is deceptively simple and remains useful, but for the purpose of exploring the bedrock of strategy it is not cast in the most advantageous vocabulary. Wylie more helpfully suggested that '*the aim of war is some measure of control over the enemy.*' (Wylie 1989, p. 66) Indeed, Wylie subtitled his work on military strategy as a general theory of power control. Controlling power is at the heart of both war and, more generally, also politics, both in its purpose and in its conduct, i.e. in strategy. The notion of control stems from naval and maritime strategy, imported by naval historian Herbert Rosinski from that specialized discipline into wider strategic studies. His discussion of control remains among the most lucid.

It is this element of control which is the essence of strategy: Control being the element which differentiates true strategic action from a hap-hazard series of improvisations. . . Comprehensive control of a field of action means a concentration upon those minimum key lines of action or key positions from which the entire field can be positively controlled. . . This concept of strategy as a comprehensive control has the advantage that it applies equally to the offensive and to the defensive. On the offensive, the aim of strategy is to break down the enemy's control while

simultaneously preventing him from interfering with our attack. On the defensive, strategy similarly seeks to constrain the enemy attack to such a form and degree that, while the defense may be forced back, it still maintains control of its actions and avoids collapse. (Cited in Eccles 1965, pp. 46-47)

Power is necessary to implement one's chosen policy, or to prevent an enemy from fulfilling his own policy goals. In wartime, the prime form of power is military power, which achieves effect primarily through battle or the threat of battle. The recourse to war is an acknowledgement that other forms of power besides military power cannot on their own deliver the object desired by policy or politics. Yet military power may be stymied by adversarial military power, and when this happens the halted belligerent is unable to work effectively toward achieving his desired goals, since his main engine of policy fulfillment is being rendered less effective by superior enemy action. Moreover, his opponent may consequently gain greater freedom to pursue his own political ends without having to counter constantly the offensive actions of the defeated. This interaction between opponents does not occur just once, but is repeated throughout the entire war, until one belligerent lacks the power or will to continue.

Strategy may be considered a series of interacting and interdependent choices made by opposing adversaries. Each belligerent seeks continually to limit the freedom of action of his opponents to prevent them from both interfering with his own freedom of action and to lessen their ability to achieve their policy goals. Each belligerent simultaneously also seeks continually to maintain or expand his own freedom of action to restrict his opponent and to achieve his own policy goals. Therefore one may consider strategy to be the distribution and employment of military power to preserve or expand one's own strategic and political options and to restrict and constrain those of one's foe to achieve the desired future distribution of power. Power, control, and freedom of action, woven together, form the fundamental pattern which dominates the currency conversion from military force to political consequence.

The basic consideration of consequence, and particularly of the consequences of employing one's own military power to impinge upon the enemy's freedom and power to act, is thus the bedrock of strategic thinking. Action and its consequences are the foundation of strategy, both in theory and in practice. A focus on power, control, and freedom of action represent an emphasis on the required core competency of strategy. The quality of a strategist and of any chosen strategy is ultimately determined by whether or not political success is achieved through force of arms. Although historical retrospective may be allowed the benefit of doubt, as any practicing strategist may have had the right ideas and the right instruments but have simply faced an even better equipped opponent, this is no comfort to strategists practicing in the present. A strategist either performs well enough to succeed, or he does not. Measures of quality typically follow that which is most fundamental. Nonetheless, power, control, and freedom of action are arguably insufficient to inform strategy in practice as a context-specific theory of victory.

Strategy's relational nature and specific theories of victory

Strategy's relationship with policy is important, and its relationship with politics is even more important, but it also has other relationships which must similarly be

tended, such as its relationship with tactics — the cutting edge of strategy. Moreover, many of the influences within and upon strategy, in theory as in practice, stem from sources which do not directly pertain to strategy's relational nature at all. Fundamentally, a focus only on strategy's relational nature and its connection to politics and policy is inadequate because strategy is necessarily multi-dimensional. To study and understand strategy's relational nature, rather than simply remaining at the general level, one must also delve into the aspects of strategy which impinge upon the challenge of relating military power to political consequences in specific practice in context.

The first aspect of strategy in context is the enemy and the role he plays in strategic practice. Strategy is by definition adversarial in theory and practice, but in strategic studies the enemy is frequently sidelined. This is not limited to the academic sector of the discipline, but is also prevalent in the armed forces. Michael Howard has long noted how 'the complex problem of running an army at all is liable to occupy [a general's] mind and skill so completely that it is very easy to forget what it is being run *for*.' (Howard 1984, p. 194) This negligence may evidence a degree of inevitability. Militaries are created, organized, and maintained so that they may be called upon to inflict violence against a chosen enemy, should the political situation degenerate to that point. Yet '[p]revious to its interaction with the enemy, all strategy is generated with only the introspective view able to be taken.' (Randall 2015)

Detailed consideration of the enemy falls under the purview of control as its vehicle. Each belligerent seeks simultaneously to improve his own control of the pattern of action in the war and erode that of his opponent. Doing this effectively requires consideration of how the enemy's actions influence one's own; of how one's own actions interfere with the enemy's; of what it may or may not be possible to achieve; and of what the enemy may or may not appear capable. The enemy's own choice of means and ways gives clues to inform the strategist. 'If the enemy's actions can reveal his assumptions about what strategic ways he fears or values, the strategist should seek to exploit these in order better to achieve his ends.' (Randall 2015) To control a strategic situation effectively is not only to be reasonably free to act as one desires with the means at one's disposal — a strategist generally cannot, after all, completely erase his enemy's powers of resistance — but also to restrict the adversary's potential options, to prevent him from deploying and employing his own instruments of military power with any great chance of effect.

Control must balance both internal and external considerations. This is important not just for deployment and employment of military power, but also for their political consequences. A strategist in action generally desires either to gain some prize for his polity from his opponent, or to deny his opponent some desired prize. Control may be applied not merely to the interaction of simultaneous and reciprocal military actions, but also to how those actions affect a polity's freedom of action in other fields of power, such as economics. A classic example would be the Napoleonic Wars, when Napoleon's victories on land allowed him largely to deny the continental markets to the economic power of Britain, while simultaneously British success at sea denied overseas markets to French and continental economic power. Territorial occupation similarly prevents a polity from exercising its sovereign power on its own territory. A strategist seeking control may, if successful, escalate his control over the situation to the point where the polity's entire ability to wield power of any sort collapses.

Clausewitz highlighted the importance of *judgment* when he identified the role of theory as educating a strategist's *judgment*. Theory was, for him, 'an analytical investigation leading to a close *acquaintance* with the subject; applied to experience — in our case, to military history — it leads to thorough *familiarity* with it... Theory then becomes a guide to anyone who wants to learn about war from books; it will light his way, ease his progress, train his judgment, and help him to avoid pitfalls.' (Clausewitz 1984, p. 141) The strategist's powers of judgment are the link between strategic theory and strategic practice, as well as being the font of strategic competence or incompetence. Power, control, and freedom of action suffice to explain action and consequences in strategic practice, but a strategist's judgment may require extending his understanding to factors which lay beyond those three fundamental concepts.

One danger of the clarity of power, control, and freedom of action is that it may imply that the practice of strategy is easy, mechanistic, and linear because those three concepts describe strategic consequence in such a straightforward manner. Strategy is not easy, mechanistic, or linear. One belligerent acts to prevent a particular line of operations from being effectively exploited, thereby reducing the enemy's power. In consequence, the inferior belligerent capitulates. As one scholar has powerfully argued,

[t]he overall pattern is clear: war seen as a nonlinear phenomenon — as Clausewitz sees it — is inherently unpredictable by analytical means. Chance and complexity dominate simplicity in the real world. Thus no two wars are ever the same. No war is guaranteed to remain structurally stable. No theory can provide the analytical short-cuts necessary to allow us to skip ahead of the 'running' of an actual war. No realistic assumptions offer a way to bypass these uncomfortable truths. (Beyerchen 1992, p. 90)

Friction sends operations awry in subtle ways. The interaction of adversaries in and of itself generates chance, as do forces extrinsic to the war in question, such as weather. The enemy may not believe himself to be beaten decisively despite battlefield setbacks, or may believe his cause to justify further fighting despite such setbacks. Information is never complete. Indeed, the paucity of information may be so fundamental that Williamson Murray has incorporated it directly into his definition of strategy itself and chided others for proffering definitions which imply clarity in strategy-making. 'In fact, such straightforward definitions go fundamentally astray, for strategy is a process, a constant adaptation to shifting conditions and circumstances in a world where chance, uncertainty, and ambiguity dominate.' (Murray and Grimsley 1994, p. 1) The clarity of strategy's bedrock — power, control, and freedom of action — serves primarily as a beacon around which individual strategists make judgments about the war in which they are involved, as well as a pillar which supports the development of strategic theory in other directions.

Other directions in strategic theory are necessary because the three bedrock concepts exclude myriad dimensions of strategy and strategy-making for the sake of clarity. In 1979 Michael Howard identified four dimensions to strategy which he felt had been neglected by modern strategic studies: the social, logistical, operational, and technological dimensions. (Howard 1979, pp. 976-986) Twenty years later, Colin Gray identified seventeen dimensions which comprise strategy: people, society, culture, politics, ethics, economics and logistics, organization, military administration,

information and intelligence, strategic theory and doctrine, technology, military operations, command, geography, friction, the adversary, and time. Gray 1999, p. 24) Regardless of how many dimensions any strategist personally identifies in the practice of context-specific strategy, general theory must have something to say about all of them so that a strategist may accurately judge when to extend his practical deliberations beyond the three bedrock concepts to consider the functional aspects of strategy's further dimensions in the context surrounding actual practice. Power, control, and freedom of action cannot on their own account for the whole of strategy's relational nature because no theory can account for the impact of individual judgment on strategy and policy-making. Therefore the problem of currency conversion from military force to political ends will continue to plague the achievement of one's own political ends because of the significant role played by the adversary's individual decision-making, particularly with regards to recognizing and acknowledging defeat in war. Strategy's myriad dimensions will ever affect the practice of strategy, although they may not always have equal degrees of influence, and the strategist may not always have to account consciously for each and every one of them in practice.

A general theory of strategy is necessarily a composite of two different theories. The first, which primarily promotes understanding of the bedrock concepts of strategy, is a *theory of strategic effect*. It is a theory which aims to determine how the employment of power leads to control of the enemy's freedom of action. A theory of strategy without a core theory of strategic effect is all but useless; the former requires the latter to have any practical application. Strategic effect must, of necessity, be the central axle of any theory of strategy. The second theory inherent within a general theory of strategy is a *theory of strategy-making*. It details what factors may impinge upon the actual practice and decision-making of strategy, including how the effects of any given strategy are interpreted by its opponents, which are crucial to strategy's relational nature in any particular context. This would not only include many of the dimensions which Gray highlighted, such as culture, ethics, military administration, logistics, and so forth, but also, crucially, civil-military relations. Not only is strategy-making the conduct one's own of civil-military relations, but also intruding upon the adversary's own civil-military relations.

This becomes an issue which may disrupt the making of strategy in societies which attempt starkly to isolate the soldiers from the politics. The United States' model of civil-military relations in particular attempts to render the soldier apolitical, which soldiers frequently find genial. Meanwhile, '[t]he professional soldier's traditional justification for being left to run the war untrammelled by politicians does not reject the idea that war is a political instrument. It just says that the politics can be left to one side until the victory is delivered. When the soldier says that, he implies not only that the politician should stay clear of his business, but also that policy is not part of the soldier's business.' (Strachan 2013, p. 83) This mirrors the flawed Moltkean understanding of war and policy. The making of strategy, and the effort of relating military power to political ends, is an ongoing practice in which both military and civilian personnel must work together despite their different cultures, widely varying experiences and professional concerns, and so on. Different groups involved in the making of strategy will emphasize its different dimensions.

Conclusion

Relating strategy to policy in both theory and practice is difficult as their relationship is complex and may take any number of different forms. Once discussion of strategy reaches this relational aspect, arguments tend to become vague, somewhat unsubstantiated, and circle around the issue without coming to grips with it. This is for good reason — what may work in one instance of strategic history may fail in another, or lead to wholly different results in a third. In strategic history, details pertaining to the myriad dimensions of strategy matter because any or all of these may send the relationship between strategy and policy awry. The general theory of strategy therefore has difficulty wrestling with this relational nature simply because it is general theory, rather than the judgment-driven specific theory of victory a belligerent may believe at any one specific moment in the historical practice of strategy.

This does not mean that strategic studies cannot do better than they already have, at the level of general theory. Strategic theorists should still be able to approach full but generic understanding of strategy's relational nature. With the purpose of making consistent sense of this nature and at the possible cost of eschewing, for clarity, direct concern with many of the other dimensions and considerations of strategy, this may be accomplished by reinterpreting the relationship between strategy and politics in terms of their major common denominators: power, control, and freedom of action.

References

- Beaufre, André (1965). *An Introduction to Strategy*. Trans. by R. H. Barry. Faber and Faber.
- Beyerchen, Alan (1992). "Clausewitz, Nonlinearity, and the Unpredictability of War". In: *International Security* 17 (3).
- Blainey, Geoffrey. *The Causes of War*. The Free Press.
- Brodie, Bernard (1973). *War and Politics*. Macmillan.
- Clausewitz, Carl von (1984). *On War*. Ed. and trans. by Michael Howard and Peter Paret. Princeton University Press.
- Eccles, Henry E. (1965). *Military Concepts and Philosophy*. Rutgers University Press.
- Foster, Gregory D. (1985). "Missing and Wanted: A U.S. Grand Strategy". In: *Strategic Review* 13.14. Autumn.
- Freedman, Lawrence (2012). "Defining War". In: *The Oxford Handbook of War*. Ed. by Julian Lindley-French and Yves Boyer. OUP.
- (2013). *Strategy: A History*. OUP.
- Gray, Colin S. (1999). *Modern Strategy*. OUP.
- (2010). *The Strategy Bridge: Theory for Practice*. OUP.
- Howard, Michael (1979). "The Forgotten Dimensions of Strategy". In: *Foreign Affairs* 57, 976–986.
- (1984). *The Causes of War and Other Essays*. Harvard University Press.
- Hughes, Daniel, ed. (1993). *Moltke on the Art of War: Selected Writings*. Presidio Press.
- Lasswell, Harold D. (1972). *Politics: Who Gets What, When, How*. Meridian.

- Murray, Williamson and Mark Grimsley (1994). "Introduction: On Strategy". In: *The Making of Strategy: Rulers, States, and War*. Ed. by Williamson Murray, MacGregor Knox, and Alvin Bernstein. CUP.
- Randall, Peter (2015). "Strategy and the Role of the Enemy". In: *Infinity Journal* 4 (3), 28–32.
- Strachan, Hew (2005). "The lost meaning of strategy". In: *Survival* 47 (3), 33–54.
- (2011a). "Strategy in the Twenty-First Century". In: *The Changing Character of War*. Ed. by Hew Strachan and Sibylle Scheipers. OUP.
- (2011b). "The Utility of Strategy". In: *International Security and War: Politics and Grand Strategy in the 21st Century*. Ed. by Ralph Rotte and Christoph Schwarz. Nova.
- (2013). *The Direction of War: Contemporary Strategy in Historical Perspective*. CUP.
- Wylie, J. C. (1989). *Military Strategy: A General Theory of Power Control*. Naval Institute Press.

Fighting Complexity With Complexity: Recognising the New Science in NSS

WILLIAM RUSHWORTH

There are known knowns; there are things that we know that we know. . . there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns, the ones we don't know we don't know.

Donald Rumsfeld, US Secretary of Defence (February 2002)

Rumsfeld's comment — while hardly succinct — accurately describes the 'new and unforeseen threats' (Her Majesty's Government 2010a, p. 4) of the international environment midway through the second decade of the twenty-first Century. There are threats that we know and act on, those that we make predictions and plans on and those that we can do nothing about until we know more. Providing security in this ever-expanding threat environment, whilst enduring a share of cross-Governmental funding withdrawals, strategic actors face a monumental task. To overcome this two pronged challenge we must make important efficiency gains, but more critically, we must re-evaluate the role of the British armed forces in the twenty-first century. If we are to maintain the existing capability of our armed forces and fulfil the fiscal duties to the Exchequer, we must explore fundamentally new perspectives on our ends, the means at our disposal and critically, the ways in which we seek to achieve them. Complexity Science offers one such perspective.

This article highlights core principles of complexity science that can be extracted from their origins in natural science and reapplied in the many different realms of the social sciences. It then demonstrates how the implicit adoption of these principles in both doctrine and reform has created substantial improvements in capability and efficiency. Finally, it establishes the potential for effective reform and greater value for money by explicitly recognising complexity science as a policy-generating concept, and through a greater embrace of its principles at an organisational, strategic and operational level in the NSS and the Strategic Defence and Security Review (NSS/SDSR) 2015.

The arguments and recommendations of this paper rest on two assumptions, the first and most fundamental is that security in the global threat environment is directly linked to capability in conflict situations. Consequently, an effective war-fighting force will see a more secure Britain, whether this force is actually engaged or an idle deterrent. The second assumption is based on the work of Antoine Bousquet in *The Scientific Way of War*, that tracks parallel paradigms between science and warfare. Therefore, the increasing evidence of a complexity paradigm in science has

— and will continue to — prompt a shift towards complexity warfare. (Bousquet 2009, pp. 163-215) Based on these assumptions, an early recognition of complexity science as a new paradigm within security will foster strategic innovation in the field of warfare that is likely to develop in the coming decades. Strategic innovation along complexity principles offers a fresh approach to tactical and strategic defence practices and may see us ahead of the game in force development solutions. Of course, being ahead of the game in defence means ensuring greater security in a changing world.

It may seem that the argument of this paper is to embrace a paradigm for strategic thought — and in some ways this is correct. However, to avoid the ‘paradigm scepticism’ of Paul Cornish one can simply describe the complexity paradigm in his own terms: ‘there is no paradigm: anything goes.’ (Cornish and Grouille 2010, pp. 16-18) Complexity science seeks to embrace the unknown, to recognise the limits of our knowledge and act to deal with whatever uncertainties may arise, it seeks — very simply — to generate order from chaos. (Holland 1998)

To establish complexity science as an effective model for security policy, two conditions must be met: first, that the concepts from the science are applicable to defence; and second, that there have been demonstrated benefits from initial adoption of complexity principles — even if this has been done implicitly. The first two sections of this article will address each concern, before the final section will look towards NSS2015 and make recommendations for explicit adoption and further complexity inspired reforms that might help to regenerate British defence to better face the challenges of twenty-first century complexities.

1 Complexity, strategy and complex strategy

1.1 Complexity

Complexity science is a systems-based science that seeks to explain the world through a different set of assumptions and processes to traditional scientific methods. In place of reductionist modelling, complexity theorists embrace the holistic properties of complex systems that defy traditional scientific techniques using various concepts, often developed through new dialects of the ‘language of mathematics.’ (‘Casti 1994, p. 3) This section highlights the key concepts that can be applied to defence and security. Mitchell Waldrop (1992, p. 11) describes something complex as a system where ‘a great many independent agents are interacting with each other in a great many ways.’ Whilst hardly comprehensive, this highlights the fundamental property of complex systems — they revolve around the linkages between many agents, not simply the agents themselves. Complexity science studies this interaction and it is the importance of linkages that renders traditional reductionist science inadequate in dealing with complexity, and that leads to the principle that the whole is greater than the sum of its parts: the concept of emergence.

Emergence describes the second stage of organisation. The interaction of various simple elements simultaneously creates complexity and leads to the emergence of a greater system than the sum of its parts. The same principle applies to amino acids that form proteins, which form cells, which form human organs, which form humans, which form societies. At every stage, the combination of agents creates a greater whole and emergence forms any complex system. Emergence generates complex systems, but complexity science adopts the term complex adaptive systems. This

clarification specifies the nature of the systems as organic, in flux, and thus constantly evolving. These biological terms help to illustrate the active, dynamic properties of complex adaptive systems. Through the dynamic collaboration of many agents, these systems create a self-organised state. Mitchell Waldrop (1992, pp. 11-12) argues that it is this dynamism that separates ‘complex systems’ from merely ‘complicated systems.’

Understanding that the complex systems visible in the world are built from subsidiary systems or ‘clusters’ (Waldrop 1992, p. 171) and the linkages between these clusters, and understanding that the systems and their clusters at every level offer properties greater than their contributing agents, explains the component parts of complex adaptive systems, but doesn’t explain the process of how this self-organisation actually occurs. The concept that does is prediction and positive feedback. The organic system is constantly looking to the future, since each agent within a complex system is affected by interactions going on between other agents as well as those actions it is taking itself. As such, even at a cellular level, agents are making predictions, as John H. Holland emphasised: ‘every living creature has an implicit prediction encoded in its genes.’ (cited in Mitchell Waldrop 1998, 146) Essentially, Holland argues that every creature gambles for survival with its gene pattern. In a complex adaptive system, each agent makes a prediction based on its own assumptions — or models — of how the world is, or is likely to be. Given this, the constantly shifting outside world means constant feedback into these prediction models and thus constant adaptation of the whole system to maintain its position.

The final major principle, that is best known through chaos theory’s ‘butterfly effect’¹ is that of non-linearity: initial inputs into a complex environment can have exponentially large impacts later on. This means that traditional ‘mechanistic,’ (Bousquet 2009, pp. 37-53) Newtonian physics cannot suffice in explanation. New mathematical principles and concepts must be created to account for the almost incomprehensible range of possible outcomes. However, even with mathematical innovation, the limits of science must be recognised and therefore, as Casti (1994, p. 276) highlights: there must be an ‘explicit recognition that system complexity is a subjective, not an objective, property.’ Despite the growing ability of mathematicians, physicists, biologists, computer scientists and the many other applied disciplines to understand and increasingly predict complex systems: chaos is not confounded.²

These concepts of *emergence*, *complex adaptive systems*, *dynamism*, *self-organisation*, *prediction* and *nonlinearity*³ form the basis of complexity science, the systems, prediction and adaptation expressed through them is the basis for application to British defence and security. Before directly applying these to the present threat environment, these principles will be assessed against existing classic and contemporary strategic literature.

¹The first use of this metaphor is attributed to Edward Lorenz on 29th December 1979 at a meeting of the American Association for the Advancement of Science.

²Allusion to Gray, C. S. *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*, 2002, Frank Cass Publishers: London, pp.80-103

³The key principles summarised here will continue to be italicised throughout the paper to make clear their application at all stages.

1.2 Complexity & classical strategy

Clausewitz is a common citation in strategic discussion a thinker of great prestige whose agreement with one's own argument seems to assure its validity. In a sense a very similar tactic is used here, however the wealth of evidence of complexity principles within *On War* justifies this endorsement — and further evidence will be examined to justify the evidence of complexity within current strategic studies.

One might respond to the professed complexity in Clausewitz by emphasising that he builds a polarity between 'yourself' and 'your enemy' built on linear and simplistic premises: what benefits him harms me 'in equal measure' and vice versa. However, the wisdom in Clausewitz's writing lies in his shift to reject this polarity. Further, having established the 'pure concept of war,' (Clausewitz 1984, p. 86) Clausewitz proclaims that 'the probabilities of real life replace the extreme and the absolute required by theory.' (1984, p. 89) As Beyerchen (1993, p. 61) suggests, '[Clausewitz] understands that seeking exact analytical solutions does not fit the nonlinear reality of the problems posed by war.' Clausewitz's contribution to the complexity school can be best represented by three concepts: *friction*, *probability* and *adaptability*.

Friction is the term that explains why the pure concept is insufficient in explaining real war: 'everything in war is very simple, but even the simplest thing is very difficult.' (Clausewitz 1984, p. 138) Clausewitz expresses the countless difficulties that emerge to deny any decision-maker an efficient mobilisation and deployment of force. Friction, in twenty-first century terms, is uncertainty. Clausewitz's recognition of the complexity in war is further evident in the claim: 'no other human activity is so continuously or universally bound up with chance.' (1984, p. 96) Not only do things happen purely by chance, the effects of this are shaped and shape further events depending on other factors that occur by chance — a process both 'continuous' and 'universal.' The ripples of *non-linearity* follow such, that even breaking down all of the first stage of options can never hope to secure an answer for what occurs at the tenth stage. Chance, therefore is nineteenth century terminology for complexity.

Given the fact that total engagement isn't a reality, a commander's strategy must essentially assess threats, risks and probabilities of both the surrounding political and geographic environment and of his enemy. To assist in this process, Clausewitz seeks to provide bounds to the range of probabilities along different scales: 'moral, physical, mathematical, geographical and statistical.' (1984, p. 215) narrowing the extremes of scope but allowing for any outcome within these bounds. Utilising his process of eliminating extremes and examining probability we generate a system of strategic *emergence*, and *self-organisation*. But regardless of the strength of strategy generated, probability is not certainty and 'with uncertainty in one scale, courage and self-confidence must be thrown in the other to correct the balance.' (Clausewitz 1984, p. 97) Strategic *emergence* coupled with the boldness to act on one's intuition comprise the commander's tools to effectively manage the volatile and uncertain environment. Essentially, they generate his *adaptability*.

The uncertain environment cannot be understood through the mechanistic 'pure' concept, and instead must allow for the continual existence of 'known unknowns and . . . unknown unknowns.' (Rumsfeld 2002) The genius in Clausewitz's work was his dismissal of pure war as nothing more than a useful thought experiment; his explanation of chance, probability and adaptability are in context synonymous with several of the complexity principles. Terminology aside, the evidence of his analysis seems to suggest that Clausewitz was a complexity pioneer.

1.3 Complexity in current strategy

Complexity science has increasingly been evident in current strategic discourse — this paper is by no means the first to make the link. Broadly, two arguments have been made: first, the widely accepted claim that the conflict environment is inherently complex and second, the less developed idea that we should adopt complexity principles in our engagement in it. James Moffat (2003, p. 49) offers a concise contribution to both of these ideas via the following table:

Complexity Concept	Information Age Force
<i>Nonlinear Interaction</i>	Combat forces composed of a large number of nonlinearly interacting parts
<i>Decentralised Control</i>	There is no master ‘oracle’ dictating actions of each and every combatant.
<i>Self-Organisation</i>	Local action, which often appears ‘chaotic,’ induces long-range order.
<i>Nonequilibrium Order</i>	Military conflicts, by their nature, proceed far from equilibrium. Correlation of local effects is key.
<i>Adaptation</i>	Combat forces must continually adapt and co-evolve in a changing environment.
<i>Collectivist Dynamics</i>	There is a continual feedback between the behaviour of combatants and the command structure.

This model suggests an ‘Information Age Force’ capable of operating in the complex war environment and — though termed differently — the concepts are interchangeable with the complexity concepts expressed in this paper.

T. Irene Sanders (1998, p. 74) offers a strategic application to prediction in the complex business environment. She claims that ‘the key to foresight is learning to recognise your system’s initial conditions as they are emerging, so that you can see change coming, respond early, or influence it to your advantage.’ This *non-linearity* is developed as Irene Sanders highlights these initial influences — or ‘strange attractors’ (1998, p. 66) — as the force that holds complex systems together, creating boundaries and allowing dynamism within each system. (1998, p. 67) Understanding the strange attractors — or what in security might be termed ‘potential trigger points’ (PTPs) — means a far greater knowledge of the system as a whole. Though not termed as such, these are the principles underpinning ‘Risk Analysis’ — a pre-existing example of complexity science applied in strategy. By seeking to assess likelihoods and create bounds to the area of choice, the strategist seeks to account for uncertainty. Cornish and Dorman (2013, p. 1194) propose a greater shift to a risk-based approach to strategy allowing us to ‘understand strategic challenges... [and] also to improve the quality of our engagement with them.’ Adopting risk embraces the idea of uncertainty and complexity and seeks a strategy to mitigate against it.

With core scientific principles; an expression of the classical strategic relevance; and an understanding of some contemporary literature; the established concept of complexity has sufficient credibility for application to British defence. Thus the concepts of *emergence*, *complex adaptive systems*, *dynamism*, *self-organisation*, *prediction* and *nonlinearity* form the theoretical background for further analysis

2 Britain — complex adaptive strategy or stationary state?

The United Kingdom naturally has a very large strategic bureaucracy crossing several government departments. Rather than assess the many departments contributing to security, this analysis will focus on government-wide and defence strategy.

2.1 A strong Britain in an age of complexity?

The cross-governmental strategy as laid out in the NSS (NSS) and Strategic Defence and Security Review (SDSR) attempted to reconcile the widening threat environment with management of the ten-year £38 billion overspend; matching ever-expanding ends with ever-tightening means. The generated strategy shows clear evidence of complexity principles, implicitly suggesting the concept as one mechanism for solving the dilemma.

Complex Adaptive Systems (CAS) and *emergence* are evident at three strategic levels: through international networks, governmental networks and military networks. Since Military networks are covered in detail in Defence doctrine, focus at this stage will remain with the political levels. The NSS evaluates the United Kingdom's strategic position in the context of the 'increasingly interconnected world,' where uncontrollable 'shocks' could have profound economic or geopolitical effects. (HMG 2010, p. 16) However, alongside this threat is the opportunity for Britain — 'at the heart of many global networks-' (HMG 2010, p. 21) to exploit international economic networks for security purposes and use 'the networks we use to build our prosperity. . . to build our security.' (HMG 2010, p. 9) Highlighting opportunities and threats in the international system demonstrates a clear recognition of our national position within the global *complex adaptive security system*, however, there is also persistent reference to a 'whole of government approach,'⁴ (HMG 2010, p. 10) highlighting the need for policy *emergence* from all areas of the national security bureaucracy. This commitment is embodied in the creation of the National Security Council (NSC) that is meant to offer 'prompt, coherent, coordinated and informed decision-making on all strategic defence and security issues.' (HMG 2010, p. 69) Persistently reinforced by the intention to be 'better connected, (HMG 2010, p. 18) cross-governmental networking on security issues emerges with international networks as two key themes across the NSS and represent a vital adoption of complexity through strategic networks at the national and international level.

Prediction and *non-linearity* in security terms mean the identification of risk and early impacts to control them or what might be termed 'horizon-scanning' and 'upstream threat control.' Recognising the importance of PTPs, the NSS embraces 'horizon scanning' through the adoption of risk analysis through a 'strategic all-source assessment,' (HMG 2010, p. 66) allowing decision makers to 'prioritise the risks which present the most pressing security concerns.' (HMG 2010, p. 26) Just as Clausewitz recognised complexity and sought to eliminate extremes to narrow our range of strategic options, analysing risk generates a mechanism for managing complexity and allocating resources effectively. Building a 'cross-Whitehall approach to horizon scanning' (HMG 2010, p. 67) seeks to enable a better chance of anticipating and responding to threats as they emerge. Just as John H. Holland's genes are implicitly predicting in order to survive, so too are strategists explicitly in order to secure.

⁴Emphasis removed.

Prediction is useless without a commitment to action and — considering *non-linearity* — the best action is to ‘tackle at root the causes of instability.’ (HMG 2010, pp. 11, 33) Upstream threat control commits the UK to engaging in initial conditions (PTPs) to pre-empt and disrupt potential future threats. Again, focussing on a cross-governmental approach, the SDSR points to the NSC as the structure to ‘integrate diplomatic, intelligence, defence and other capabilities on preventing international military crises.’ (HMG 2010, p. 10) A combined recognition of *prediction* and *non-linearity* in the NSS is seen through the dynamic perception of climate change as a ‘risk multiplier,’ compounding unrest and instability in fragile states, with a disproportionate effect on the developing world. (HMG 2010, p. 17) Overall, *non-linear threat prediction and early action* through horizon scanning and upstream engagement with PTPs represents a key asset for the continual development of the UK’s security strategy.

Upstream action though necessary is not sufficient to maintain security, an ever-changing world requires an ever-changing force. *Dynamism* is consistently represented in national doctrine through two terms: adaptability and resilience. On the former, the NSS expresses the strategic imperative of recognising uncertainty and remaining adaptable to manage this. (HMG 2010, p. 15) The SDSR then proposes the actual requirements for providing this adaptability by; diversifying and extending helicopter capabilities, building ‘broad spectrum...capabilities’ and extending the reserves to ‘make the Army more mobile and flexible... better adapted to face current and future threats.’ (HMG 2010, pp. 4, 17 & Independent Commission to Review the United Kingdom’s Reserve Forces 2011) With the latter, the NSS offers a comprehensive explanation of ‘Risk and Resilience’ summarised in the seventh ‘National Security Task’: to ‘Provide Resilience for the UK by being prepared for all kinds of emergencies, able to recover from shocks and to maintain essential services.’ (HMG 2010, p. 33) Seeking adaptability to act effectively in conditions of uncertainty and ensuring resilience to recover and manage shocks demonstrates attempts to ensure a dynamic security provision able to deal with the complex environment.

The NSS demonstrate clear complexity trends at three levels: organisational, strategic and operational. When applied, the complexity principles generated in Section One combine into these areas: organisationally through *multi-level strategic networks*; strategically through *non-linear threat prediction and early action*, and operationally through *dynamic forces*.

2.2 British defence — complex adaptive security system?

Given the apparent doctrinal evidence of complexity principles at a national strategic level, the diffusion of this to defence level doctrine is the first stage in determining the success of its adoption. Since national government decides the budgets for the MoD, it is unsurprising that the MoD will seek to pander to the national strategic priorities, however a genuine adoption of the complexity concept should see expansion from the ideas presented in the NSS and an embrace of the ideas at both service and departmental level. Considering complexity science at the organisational, strategic and operational levels established through the NSS it appears that there is substantial development in the British Defence Doctrine (BDD) and through the process of defence reform since 2010.

Organisational: multi-level strategic networks

The network focus of NSS primarily highlights the international context of the national strategic network emphasising the opportunities to exploit our existing international trade networks for strategic gain. (HMG 2010, p. 21) The BDD affirms the national network through cross-government cohesion in force development for the international threat environment through the ‘Defence Conceptual Framework,’ (Ministry of Defence 2011, pp. 4-6) however — as expected — the primary network focus of BDD is on military networks. The complexity enabled focus ranges from contextual understanding of actions and multiplied impacts on all parties in a crisis, to Network Enabled Capability (NEC), and most prominently through ‘joint action.’ (MoD 2011, pp. 5-7) NEC presents perhaps the most natural embrace of complexity principles by ‘allowing effective decision-making and agile synchronisation of activity’ (MoD 2011, pp. 4-15) through integrated information systems such as Intelligence, Surveillance, Targeting, Acquisition and Reconnaissance (ISTAR) systems. (Defence Reform Steering Group 2011, p. 44) This NEC capability — advocated particularly in the *Royal Air Force’s British Air and Space Power Doctrine* (2009) combines the networked organisational concept with *dynamism* and *self-organisation* and represents an important complexity enabled concept. However, it is the extensive commitment to providing a ‘joint force approach’ (DSRG 2011, p. 7) that represents the major organisational shift towards a military network.

The Defence Reform report published by an independent commission offers details on the creation of a ‘*Joint Forces Command*’ (DSRG 2011, pp. 44-47) to manage cross-service programmes, ‘deliver output focussed capabilities and capitalise on potential synergies to deliver enhanced joint operational effect.’ By allocating certain funds to a joint body, the military will be able to fully fund ‘promising forms of macro-innovation to obtain new capabilities.’ (Luttawak 2012, pp. 85-97) Interestingly, all three services recognise their role in the joint force concept and — in doctrine at least — appear willing to offer capability to joint forces, either nationally (Army 2012a, p. 124) or as part of a ‘joint multi-national and multi-agency force.’ (Royal Navy, p. 3) This organisational shift recognises the uncertainty regarding the roles forces will have to adopt in the future and demonstrates a very significant shift to providing a more organic management process for defence provision

Strategic: non-linear threat prediction and early action

The scope of horizon-scanning and upstream engagement is less prevalent at the MoD doctrinal level since these activities require a cross-governmental approach, somewhat beyond the strategic remit of the MoD. The military is primarily a crisis management tool and is unlikely in their own doctrine to focus on wider measures of economic incentives, aid provision and development investment; however the BDD recognises the military as one component of an ‘integrated approach’ (MoD 2011, pp. 1-11) across government. For example, the Royal Navy highlights its upstream ‘International Engagement’ role through humanitarian operations and disaster relief. (Royal Navy, p. 4) The primary focus in the core defence function is on the non-linearity in conflict — preparing for your ‘known unknowns,’ allowing for ‘unknown unknowns’ and planning for the unplanned. The BDD emphasises that ‘commanders should anticipate the effects of being surprised... [and] make appropriate contingency plans.’ (MoD 2011, pp. 2-6) While defence level doctrine adds little to upstream prediction and action, the MoD’s recognition of the *non-linear* threat

environment stresses the importance of preparing for the unexpected and positioning itself at the ‘global seams,’ (The Royal Marines n.d., p. 4) generating *dynamic* response capability.

Operational: dynamism and self-organisation

Adaptability and *Resilience* were championed characteristics in national strategic doctrine, and are fully embraced in both the BDD and the Defence Reform report:

The British Military are renowned for their ingenuity. The innate ability to make do, and to respond to unexpected circumstances with pragmatism and industry, gives the Armed Forces the capacity to adapt and to overcome both opponents and local difficulties. (MoD 2011, 5A-4)

At the very core of the British forces is *dynamism*, and thus the preservation of a ‘culture that encourages people to think creatively, and to be resourceful and imaginative,’ is a priority for the MoD (2011, pp. 2–7). This is seconded by a similar approach to developing strategy by allowing ‘fresh thinking and innovation, distilled in doctrine’ (MoD 2011, pp. 5–12) and allowing our defence organisation to be ‘lean and agile such that it can continually improve and adapt to changing circumstance.’ (DSRG 2011, p. 11) Clearly, the principles of *dynamism* within the complex systems of defence and government are reflected consistently in both political and military doctrine. Notably, this expressed commitment to the culture of innovation, develops into an integration of the principles of *self-organisation* and *emergence*.

Defence level *dynamism* is clearly represented through service doctrine due to its direct relevance in military strategy and tactical operation. The Royal Marines — for example — regard ‘acute situational analysis, lateral thinking, creativity, nimbleness and incisive independence of mind’ as essential to working in complex ‘hybrid conflicts.’ (2011, p. 4) *Transforming the British Army* (2012, p. 1) expresses the Army’s need to ‘place adaptability and responsiveness at the core of its design.’ Chris Donnelly states this point with even greater emphasis, stating that ‘we should subject any new idea, reform or proposal to a simple test: will it increase our adaptability?’ (Army 2012b, p.192) The Royal Navy’s vision also highlights the requirement to be ‘an agile, learning Navy’ ensuring swift updates in doctrine and strategic practice in response to environmental and political changes. Clearly, there is a wealth of service-level commitment to the provision of a *dynamic* force.

The *self-organising* capacities are generated through increasing commitment to decentralisation of command. Developing from a desire to avoid political intervention at higher decision-making levels, at lower levels is a doctrinal commitment to ‘a style of command that promotes decentralised command, freedom and speed of action and initiative.’ (MoD 2011, pp. 5-4) In the Air Force Doctrine (2009, p. 65) this is developed via NEC, allowing ‘mission command to be extended, with confidence, down through the tiers of command.’ By allowing semi-autonomous elements to *self-organise*, the defence system can utilise these connections to ensure the first point in the Defence Reform report: the emergence of ‘a single Defence framework that ensures the whole is more than the sum of its parts.’ (DSRG 2011, p. 4) Thus *self-organisation* — the final complexity principle — is evident as a key aspect of the *dynamic* force. The doctrine of the Armed forces represents a system that is adaptive, *dynamic* and *self-organising*, but through a prism of organisational structures and techniques.

2.3 Conclusions on the doctrinal adoption of complexity principles

In the application of the complexity principles distilled in Section One, three levels of applied complexity emerged, relating to the three vital levels of strategic decision making: organisational, strategic and operational. There is clear and extensive doctrinal evidence of complexity science within several levels of British strategic bureaucracy. The core, abstracted concepts of complexity have organically produced the themes of *multi-level strategic networks*, *non-linear threat prediction and early action* and *dynamism and self-organisation*. These themes form the framework through which the actual impacts of complexity will be analysed.

3 Embracing complexity and enabling capability

Doctrinal adoption of complexity principles appears widespread at all levels of defence strategy, however the defence bureaucracy is notoriously resistant to major reform. If there is little actual adoption of the advocated principles, then there will be little evidence of their success and the strength of recommendations for further adoption is questionable. Analysis shows that the diffused complexity principles evident in British strategic and military doctrine have — perhaps surprisingly — impacted substantially on defence and security provision, particularly given the extensive reforms since the 2010 NSS/SDSR.

A balanced account of the extent of reform must take into account more than just the Government's own reports since they can tend to overstate the effective implementation of reform proposals and national strategic directives. Departmental reviews are considered alongside Parliamentary committees' own assessments; the independent annual reports of Lord Levene; and an independent report on reserves in the future force, in order to assess the translation of complexity principles from doctrine to practice regarding the three defence complexity themes.

The organisational doctrine of *multi-level strategic networks* has been extensively translated at many levels from international to military. However, certain failures in reform at the national level have called into doubt the full adoption of networking principles. At the international level, the Government's *Annual Report on the NSS and Strategic Defence and Security Review* (ARNSS/SDSR) has recognised that there has been limited progress on 'working in [international] alliances and partnerships' (HMG 2013, p. 8) but also claim that this is often due to international constraints, rather than lack of UK effort or Government failure. On a wider level, embracing international networks appears to have been successful. The ARNSS highlights successes in strengthening our diplomatic network, expanding our influence across the world; (HMG 2013, p. 11) in international cooperation on counter-proliferation; in global counter-terrorism efforts; and in developing an effective response to the growing cyber threat.' (HMG 2013, p. 14) Generally then, international network development — both organisationally and in terms of key security priorities — seems to have been successful — even if only presented in the Government's own review of its progress.

In developing national strategic networks the NSS was most ambitious and — perhaps unsurprisingly — this appears the area where the most difficulty has emerged when implementing change. The House of Commons Joint Committee on the NSS specifies two shortfalls in the role played by the NSC; first and most fundamental in terms of national networking — the NSC is not 'enabling the Government to work

as a coordinated whole.’ (Joint Committee on the NSS 2012, p. 4) Considering the initial purpose of the NSC to bring a ‘tightly coordinated approach across the whole of government,’ (HMG 2010, p. 9) this represents a major weakness in reform implementation and the adoption of complexity principles. Linked to this, the Committee report that they ‘continued to look for evidence of the NSC considering long term and blue skies topics and . . . found little.’ (JCNSS 2012, p. 9) This strategic deficit in the highest governmental security authority is echoed by the Public Administration Select Committee Report, ‘*Who does UK National Strategy?*’ (Public Administration Select Committee 2010, p27-29) They recognise that strategic thought must ‘adapt . . . to changes in our strategic environment,’ but claim that they are ‘yet to see how [the NSS] marks any significant improvement in qualitative strategic thinking from its immediate predecessors.’ Claiming a lack of strategic networking, they argue that ‘different departments discuss and understand strategy in different and incompatible ways.’ Thus, ‘departmental collaboration . . . falls short of what individual departments can do independently,’ a far cry from ensuring that the ‘the whole is more than the sum of its parts.’ (DSRG 2011, p. 4) Overall, the Parliamentary criticism appears damning, however this critique of national strategy development does not reflect the wider developments in the national strategic network that have seen a huge shift in emphasis and adoption of networked collaboration.

The Defence Select Committee’s publication *Towards the next Defence and Security Review: Part One* (2014, p. 76) recognises the success of ‘the comprehensive approach’ during the operations in Afghanistan and Iraq. The key success is represented in the execution of the National Security Tasks as laid out by the SDSR. Their assessments made at six month intervals claim that as of October 2013, 90% of the 220 tasks determined by the SDSR are ‘on track,’ with 28% ‘completed,’ 33% ‘fully on track,’ 30% satisfactory and just ‘6% problematic.’ (Her Majesty’s Government 2013, p. 5) Further, specifically in strategic networking areas — such as supporting bilateral relationships, developing an international diplomatic networks, multi-lateral counter proliferation approaches and a Government-wide commitment to international development programmes — there were no objectives lower than ‘satisfactory.’ The multi-department ‘Conflict pool’ has led to the NSC’s development of the £1 billion Conflict, Stability and Security Fund (CSSF), and demonstrates progressive national collaboration in upstream action. Despite the strategic concerns of the Public Administration Select Committee, the implementation of the SDSR has translated the vast majority of its intended outcomes into reality — meaning that the *multi-level strategic networks* evident in doctrine have progressed in reality.

As established in BDD and Defence Reform, the development of defence level strategic networks lies primarily in the joint force concept and NEC. Lord Levene, in his second annual review on defence reform highlights that the established JFC is a ‘lean and agile organisation [and] . . . a model for other parts of Defence.’ (DRSG 2013, p. 3) It is this joint command centre that develops significant tactical networking capability through funding and development Defence Information Systems such as C4ISTAR⁵ (DRSG 2013, p. 3) capabilities. Finally, military networks are developing in the informational sphere. In the battle-space complex adaptive information network ‘every individual is considered to be a sensor . . . able to contribute to a *Shared Situational Awareness* (SSA) [which allows us] to make better decisions before our adversaries can make theirs. This ‘self synchronisation’ (Cebrowski and Garstka

⁵C4ISTAR — Command, Control, Communication, Computing, Intelligence, Surveillance, Target-Acquisition and Reconnaissance.

1998) — enabled by this multi-nodal, collaborated information system — almost returns to the biological origins of complexity science, but offers a substantial insight into the developing informational networks allowing sensory agents to coordinate and self-organise in complex conflict environments.

Development of non-linear threat prediction comes through risk-based approaches. The publication of a review of ‘horizon scanning’ by John Day in January 2013 looked to form a new ‘cross-government horizon scanning programme [that] joins up existing work and groups within different departments to form ‘communities of interest’ so as to maximise capability.’ (HMG 2013, p. 35) This integrated approach sees horizon scanning come under the remit of the Cabinet Office — allowing an effective flow of conclusions and reports to the NSC through the Minister of the Cabinet Office. A coordinated approach to horizon scanning alongside a new ‘Countries at Risk of Instability Index’ (HMG 2013, p. 10) and the CSSF demonstrates a very clear effort to provide effective *non-linear threat prediction* and is reflected at a lower strategic level through a renewed emphasis on risk management within the MoD as outlined in the *Improvement Plan*. The shift has involved private consultation and sees ‘Chief Risk Officers’ employed at each TLB area with a Defence Board member overseeing them. This structure allows strategic risk to be identified alongside a ‘risk owner,’⁶ resulting in an action plan to be developed in order to allow systematic mitigation and management of risk. In this case, the MoD combines *prediction* and *early action* in order to mitigate the emerging threats.

On a less causal level of ‘risk + action plan,’ the wider Government seeks to act to mitigate risks in the international context. Primarily this upstream engagement is a multi-departmental system based under the ‘Building Stability Overseas Strategy (BSOS). Consisting of ‘Early Warning Analysis’ complimented by an ‘Early Action Facility (EAF) of £20 million per annum,’ (HMG 2013, p. 9) the BSOS programme demonstrates a wider Governmental commitment to embracing non-linearity and attempting early conflict-prevention. The success of the conflict pool programme has meant a development into the previously mentioned £1 billion CSSF. At both the national and defence-wide levels, *non-linear prediction and early action* have been made a high priority, demonstrating financial commitment to a fundamental complexity principle.

Government level *self-organisation* is often difficult given central guidance from Cabinet, however, the Government’s NSSreview highlights the Cabinet Office Briefing Rooms (COBR) as an effective ‘mechanism for coordinating decision-making and emergency response across Government.’ (HMG 2013, p. 34) Lord Levene’s second annual report — the first after the ‘New Operating Model’ became fully operational — praises the genuine adoption of decentralisation, restating that ‘universal support for the concept of greater empowerment and shared top level determination [can] make [decentralisation] work effectively.’ (2013, p. 2) Effective decentralisation of the six Top Level Budgets (TLBs) (MoD 2014, p. 7) allows for a more organic self-organisation process between Head Office, the Defence Infrastructures Organisation, Joint Forces Command and the three service chiefs. Finally, the independent approach saw adaptability generated through adopting a ‘Whole Force Concept’ involving greater integration of specialist reserve troops such as doctors and nurses — in numbers that would be unaffordable as full time regulars. In addition, the GEMS Ideas scheme, created by the MoD draws ideas through an online platform for 270,000 MoD employees fostering innovation into developing capabilities and new

⁶Risk bearer might offer a clearer representation.

ways of cutting bureaucracy. (MoD 2014, p. 11) These creative solutions express elements of innovation that have surpassed Lord Levene's radical defence reform concepts, further developing the importance of specialist agents' role in providing *dynamic* capabilities within the complex adaptive force structure.

Given the perceived nature of Government bureaucracies as a leviathan-like creature, resistant to change and embroiled in political horse-trading, the speed and extent of reforms to defence and security systems since 2010 is remarkable. The result is evident, within the Government's drive to improve the efficiency, capability and cost-effectiveness of our defence provision, *multi-level strategic networks, prediction and action in the non-linear threat environment* and *dynamism* and *self-organisation* emerge as a codification of many different principles proposed by academics and strategic reformers in the last decade. Given its pervasion, and given the now justified assumption that adopting complexity principles can remove inefficiencies no longer acceptable with today's tightening budgets; the final section of the analysis points towards further adoptions that may continue to generate improvements in providing security.

4 The future of complexity in a complex future

4.1 Organisational: multi-level strategic networks

The Multi-Level Strategic Networks concept emerged from complexity principles applied to the political, defence and service level doctrines. However, this concept has potential to clarify organisational understanding of the entire security environment. Embedded in this idea is recognition that the polar distinction between 'Grand Strategy' and 'Military Strategy' (PASC 2010, p. 7) is too simplistic. Instead the developed, multi-departmental security system operates on several strategic planes: the international network; the national network; the defence network. Understanding strategy as the ways to match given *means* to desired *ends*, (Cornish 2012, p. 70) recognises that at each network level, different *means* and more specific or broader *ends* require different strategies. Recognising different network levels helps improve two strategic processes: improved communication with other agents or organisations on the same network level and clear horizontal platforms to establish formal vertical governance structures between higher and lower levels. To understand this improved communication, consider the recent expansion of diplomatic personnel in the international network. Rooted internationally, diplomats can collaborate with DFID civil servants and Secret Intelligence Service Officers, align themselves with embassy defence attaches, and communicate effectively with representatives in multilateral institutions such as the UN, NATO and the IMF — all horizontal communication in the international network. Equally, these international network agents can engage in other network levels through the vertical governance structure of the FCO. The FCO is able to translate international network communication through the Foreign Secretary into Cabinet, and thus into other national level network agencies.

A ready developed opportunity for integrated cross-network governance structure is the NSC, which could provide the crucial link between different security providers operating in their own networks with their own means (Defence, Home Office, security services, FCO etc.). The NSC could provide strategic collaboration through the integration of network-level strategies from these departments into a coordinated security strategy for the UK. Developing the concept of the NSC as a multi-network

coordination structure, there should be a further development of the NSC to address the problem of strategic shortage made by the Joint Committee on the NSS. In order to operate as a more effective strategic coordinator, the NSC should be leading the development of national strategy. To do this, it should have three contributing elements:

First, a *permanent horizon scanning team*: remaining within the cross-government horizon scanning programme under the remit of the Minister for the Cabinet Office — since he also sits on the NSC. National security horizon scanning should be active and reporting routinely — not simply on a commissioned basis — so that the NSC can frequently update strategic objectives. The Joint Intelligence Committee could contribute to this through the provision of real time information that can build a more complete picture of future threats and PTPs.⁷ Whilst developing from the network concept, this constant reevaluation, funded separately from the fiercely guarded budgets of individual agencies and departments seeks to create effective prediction and will ensure that future PTPs are constantly being revisited and reevaluated, and new threats are also highlighted as early as possible.

Second, an *expert panel of strategic planners* able to take the horizon scanning team's results and provide coherent and coordinated threat management plans for emerging PTPs. Consisting of specific agency experts, academics and other less partisan experts this group will generate response plans for all major PTPs and for multiple combinations. Rather than COBRA having to generate crisis management strategy in real time under high pressure, they will be able to refer to and adapt previously considered strategic responses to more efficiently combine security capabilities into bespoke force packages. Thus the network concept also helps to generate *early action*.

Third, *agency representatives* to relay strategy to all strategic bodies. In the event of a developed threat, these central plans, then reconsidered and adapted by the COBR mechanism can be diffused to the relevant security providers with strategic guidance — the developed operational plan can then be formulated at agency level within the remit of the strategic directive provided. These representatives are vital for the functioning of the concept. They must be within the highest levels of their agency in order to ensure an effective diffusion of the strategies generated in the NSC. Without this link, the NSC's influence will be limited and its strategic coordination ineffectual. However, with effective diffusion, the *prediction*, *early action* and efficient coordination generated through the NSC's strategic network will foster an evolving and adaptive strategic narrative and provide a constantly innovating strategic body right at the centre of Government.

Further embracing NEC — arguably the most direct application of complexity science — can enable rapid battlefield coordination, information superiority and potentially decision-making superiority. Utilising the principle of complex adaptive systems and thus understanding each information receiver as an information sensor allows us to adopt a Shared Situational Awareness (SSA) system of information provision. This opportunity to translate technological innovation into capability transforming systems must retain two caveats: first, information security, and second, C2 discipline. With an SSA model, every actor on the battlefield is linked into the network; just one sensor captured by the enemy could mean the elimination of any information advantage. Thus, technology must be used to ensure access is only available to the intended user — whilst retaining its utility in a high-pressure

⁷Potential Trigger Points (See Section One)

conflict environment. Basic fingerprint recognition for example is unhelpful in a high intensity contact situation. The challenge then is to provide an easy-to-use and secure method for unlocking information technology devices — be they visual or audio: security measures must not reduce utility. Secondly, operational command of a SSA system is vital to avoid information overload. Computer systems will be vital in combining different intelligence strands into patterns in the command hub. However, commanders must be wary of issuing tactical directives — NEC systems will not allow command a closer view of the immediate vicinity than the soldier on the ground. Commanders must focus on ensuring that soldiers and officers have maximum information of the wider battle situation, allowing them to make informed tactical decisions. The results of highly trained, well-informed soldiers with a clear strategic direction could emerge into a devastating combination to enemy combatants.

4.2 Strategic: prediction and early action

The recent developments in risk analysis and management through the horizon scanning represent a commitment to accessing quantifiable ‘uncertainty embracing’ techniques. Recognising our limited control in the threat environment, documents such as *Strategic Trends out to 2040* and *Future Character of Conflict* published by the Development, Concepts and Doctrine Centre (DCDC) offer tangible *prediction* on which strategic decision makers can base their risk management plans. Provided the NSC and other decision-makers establish these plans and maintain ‘capability slack’ to account for unpredicted possibilities or the ‘unknown unknowns’, this process of *prediction* and planning offers an effective model. Risks and trends considered, adopting a non-linear approach to threats promotes early engagement to neutralise or influence PTPs. Again, there is a caveat: upstream engagement such as the EAF should always be enacted with caution. Just as successful action to influence PTPs can prevent risks evolving into major threats, poorly considered upstream intervention can cause exponentially large problems down the line. Since non-linearity has no regard for ‘good’ and ‘bad’ intervention, maintaining caution in upstream engagement is essential to avoid exponentially damaging effects.

Successful early engagement in the international threat environment — through upstream engagement — requires an integrated cross-governmental approach, and the UK has had this. The integrated BSOS programme is now a fundamental aspect of *early action* to prevent security crises, but it also represents an improving sociological, anthropological and political understanding of other states in the international network. Establishing this anthropological intelligence can help perceive the specific context in which engagement might be sought. Combining it with the NSC’s PTP management planning can be a vital key in developing an agile, adaptive and appropriate engagement strategy that will not have negative non-linear repercussions. Thus, through a process of early investigation of PTPs — through diplomatic networks, for example — decision makers should generate strategy from the future and the present: *predictive* capabilities emerge from both horizon scanning and the international network.

4.3 Operational: adaptability and self-organising coordination

To maintain the same capabilities under severe budget restrictions and force reductions, there must be an improvement in the adaptability of remaining forces. The

Future Force 2020 model recognised this and formed a brigade force structure reflecting a complex adaptive system model, whilst maintaining the traditional bounds of the system based on hierarchy. An agile, high-readiness reaction force with specialist add-ons provides a swift, but enabled deployment of a tailored force package to suit the specific demands of an operation. The embrace of complexity science has allowed this more efficient use of the limited means available by improving the adaptability of those means.

Justifying self-organisation in a system based on centrally diffused strategy and coordinated operational orders is difficult. However, the British success throughout history is regularly attributed to the adaptability, ‘ingenuity’ and ‘initiative’ of forces personnel. (MoD 2011, p5A-4-5; Farrell 2008, p. 788) Lord Levene recommended the decentralisation of TLBs to the six key defence providers, highlighting the value of a central strategic direction alongside allowing ‘*delivery units... the levers they need to run their business.*’ (DSRG 2011, p. 7) The same logic at the lower level would see strategic objectives diffused from central command, and operational command decentralised to specific capability providers. If the strength of British defence is in the quality and initiative of its people (Army 2012b, p. 182) and decentralised command is an effective management strategy, it follows that a broadly *self-organising* command model should have distinct advantages. There is logic behind the shift to a ‘federal’ management system rather than a strictly ‘hierarchical’ diffusion of command, however the MoD should always conduct systematic evaluation of each decentralisation decision ‘on its own merits.’ (DRSG 2011, p. 7) As with *early action*, poorly managed decentralisation can be dangerous, leading to lack of direction and losing the tight coordination brought about by networks — always centrally diffused strategy must remain paramount.

Further, before any further decentralisation takes place, there must be a complete reevaluation of the education and training given to armed forces. Mungo Melvin’s contribution to *The British Army 2012*, ‘Educating and Training the Army for an Uncertain World’ outlines this need to develop intellectual capital within the service at command level, but also to develop ‘in-service education’ equipping soldiers with the capacity to ‘learn, and successfully relearn, how to successfully employ different forms of military power.’ (2012: 185) In the age of the ‘strategic Corporal,’ (Makay and Tatham 2009, p. 5) embracing the multi-dimensional soldiering of twenty first century conflict — educating our people to fulfil that adaptive role and then empowering them with certain operational freedoms within the broader strategic remit — could provide the sort of *self-organising* command structure that transcends the inefficiencies and communicative problems of the traditional hierarchical force structure and fosters a more dynamic, evolving defence provision. This includes educating soldiers at all levels on the principles of complexity within war and security. The potentially enormous strategic effects of events such as Sergeant Blackman’s murder of an Afghan fighter in September 2011 — if adopted by the Taliban as counter-coalition propaganda — should be used to demonstrate to soldiers the non-linear consequences of mistakes in the field. A full understanding of this, as well as of the organisational, strategic and operational complexity ideas expressed here, can educate soldiers and officers to better understand some features of the current threat environment. The demands are extensive: we require better-educated, more adaptable, agile, effective and empowered troops in the 21st century; but the reason is simple — to maintain our defence capability, we need to provide more with less.

Finally, more important than any specific adoption of specific complexity ideals

is an intellectual recognition and embrace of complexity science's value in security strategy. Paul Cornish's theory of 'paradigm scepticism' (2011) should be heeded — complexity does not have all the answers. However, the fundamental premise of complexity is that we don't know everything. Hence, intellectual engagement with complexity will allow research into further strategic applications of its principles, either through predictive mathematics, or through further network developments. From here an evolving environment of strategic investigation could emerge. This intellectual process may lead to no substantial discovery — the findings may be inconclusive — however, given the evidence already of its initial success, it may also offer the next revolution in understanding and improving our strategic defence and security capability.

4.4 NSS: Embracing the New Science

Core complexity principles from a range of scientific literature were found to be present in traditional strategic theory. When examined against British doctrine at the national, defence and service levels all three adopted complexity ideas and generated three themes of defence and security applications: *multi-level strategic networks*, *non-linear threat prediction and early action* and *dynamism* and *self-organisation*.

There has been real implementation of the doctrine during reform with successful consequences and therefore British defence and security can be beneficially influenced by complexity science. The following represent a summary of the complexity inspired policy recommendations for NSS:

Major reform of the NSC

- a. Emphasis on its core role as a strategic network hub, combining information and strategy from all major levels of strategic governance.
- b. An inbuilt permanent horizon-scanning team to constantly update on the developing threat environment.
- c. A threat management team of expert strategic planners, generating plans for the PTPs that are uncovered by the horizon-scanning team.
- d. An information structure combining evidence from government officials across departments based across the world to inform both horizon-scanning and threat management teams.
- e. Further development of our anthropological knowledge of countries highlighted as or within PTPs.
- f. Agency representatives from all involved parties, significantly senior within their department to ensure effective and complete strategic diffusion at all levels.
- g. Funded through the Cabinet Office in order to remain firmly at the centre of Government strategy.

Further Defence reform

- a. Tangible commitment to employing better educated troops.

- b. Providing further political and strategic education to all forces as part of basic training. This includes an understanding of the complexity principles within security.
- c. Once achieving this, investigate and experiment with different options of decentralised command and generating exercises to test ‘swarming’ as a tactical concept.

Explicit strategic engagement with Complexity Principles

- a. Funding for existing bodies, such as the DCDC, to engage with complexity ideas and mathematical techniques with a view to the strategic and military gains that can be made.
- b. A recognition of complexity as a new way for strategists to approach providing security and departmental management. Focus must further shift towards providing adaptable capabilities.

Of these three areas, two require funding and political leadership. The third, though economically simpler requires a substantial change in mindset — and so may be equally as difficult to achieve. However, the reformed structures above would provide a dynamic, future-orientated strategic bureaucracy. With the NSC generating strategy in the very centre of Government with contact and information from all its limbs, a tightly coordinated and coherent strategy can develop a full spectrum of threat management plans that can assist Cobra in the event of a crisis. More consistent horizon-scanning will enable even greater commitment to upstream intervention. The continuing shift to having a better educated and more adaptable but smaller force will accord with the continuing budget constraints whilst maintaining and potentially even extending our capability.

Finally, this analysis has sought to codify many innovations in security and defence policy through an established scientific construct. Through a broader perception of complexity science as a capability-enabling concept, further research into strategic and defence applications alongside the scientific and mathematical techniques might ensue. Greater strategic investigation of complexity science’s applications could foster even further capability generation and organisational reform. Through an early strategic engagement with complexity science as a discipline, the British strategic decision makers should look to exploit non-linearity and develop exponential development in strategic advantage. An ongoing process of strategic development on complexity lines could at worst explore new avenues and at best contribute to a more secure and prosperous UK.

References

- Army (2012a). *The British Army 2012*. Newsdesk Media.
- (2012b). *Transforming The British Army*.
- Beyerchen, Alan (1993). “Clausewitz, Nonlinearity, and the Unpredictability of War”. In: *International Security* 17 (3).
- Bousquet, A. (2009). *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. Columbia University Press.
- Casti, J. L. (1994). *Complexification: Explaining a Paradoxical World Through the Science of Surprise*. Abacus.

- Cebrowski and Garstka (1998). “Network-Centric Warfare: Its Origin and Future”. In: *Proceedings* 124, p. 1.
- Clausewitz, Carl von (1984). *On War*. Ed. and trans. by Michael Howard and Peter Paret. Princeton University Press.
- Cornish, P. (2012). “National Strategy in the Early 21st Century: Innovating for Uncertainty”. In: *International Symposium on Security Affairs*. Vol. 15. NIDS, pp. 69–83.
- Cornish, P. and A. M. Dorman (2013). “Fifty Shades of Purple? A risk-sharing approach to the 2015 Strategic Defence and Security Review”. In: *International Affairs* 89 (5), pp. 1183–1202.
- Cornish, P. and O. Grouille (2010). “Land Forces Fit for the 21st Century”. In: *International Security Programme*.
- Defence Reform Steering Group (2011). *Defence Reform: An independent report into the structure and management of the Ministry of Defence*.
- (2013). *Second Annual Report*.
- Defence Select Committee (2014). *Towards the Next Defence and Security Review: Part One*.
- Farrell, T. (2008). “The Dynamics of British Military Transformation”. In: *International Affairs* 84 (4), pp. 777–807.
- Gray, C. S. (2002). *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*. Frank Cass Publishers.
- Her Majesty’s Government (2010a). *A Strong Britain in an Age of Uncertainty: The NSS*.
- (2010b). *A Strong Britain in an Age of Uncertainty: The Strategic Defence and Security Review*.
- (2013). *Annual Report on the NSS and the Strategic Defence and Security Review*.
- Holland, J. H. (1998). *Emergence: From Chaos to Order*. Addison Wesley.
- Independent Commission to Review the United Kingdom’s Reserve Forces (2011). *Future Reserves 2020*.
- Joint Committee on the NSS (2012). *Planning for the next NSS: Comments on the Government’s response to the Committee’s First Report of Session 2010–2012*.
- Luttawak, E. N. (2012). “Reinventing Military Innovation”. In: *International Symposium on Security Affairs*. Vol. 15. NIDS, pp. 85–97.
- Makay, A. and S. Tatham (2009). “Behavioural Conflict—From General to Strategic Corporal: Complexity, Adaptation and Influence”. In: *Shrivenham Papers* 9.
- Ministry of Defence. *Strategic Trends Programme: Future Character of Conflict*.
- *Strategic Trends Programme: Strategic Trends — Out to 2040*.
- (2011). *The British Defence Doctrine*. JDP 0–01.
- (2014a). *How Defence Works*. Version 4.01.
- (2014b). *Ministry of Defence Improvement Plan*.
- Moffat, J. (2003). *Complexity Theory and Network Centric Warfare*. CCRP.
- Public Administration Select Committee (2010). *Who does UK National Strategy? First Report of Session 2010–11*.
- Royal Air Force (2009). *British Air and Space Power Doctrine: AP 3000*.
- Royal Navy. *Future Navy Vision: The Royal Navy Today, Tomorrow and Towards 2025*.
- Rumsfeld, D. (2002). *US Department of Defense News Briefing*.
- Sanders, T. Irene (1998). *Strategic Thinking and the New Science*. The Free Press.
- The Royal Marines. *Vision: Think Commando*.

Waldrop, M. Mitchell (1992). *Complexity: The Emerging Science at the Edge of Chaos*. Simon & Schuster Paperbacks.

Uncertainty in National Security Strategy: ‘What the Old Lady of Threadneedle Street could teach the old men of Whitehall.’

JAMES SLADDEN

Abstract

The UK Government’s 2010 National Security Strategy declared that we live in ‘an age of uncertainty’. What was required therefore was a radical transformation in the way we think about national security. However the National Security Strategy did not define what ‘uncertainty’ meant or what the implications of it were. Instead it offered a comprehensive assessment of UK national security based upon risk methodologies. This paper argues that the conventional methodologies of risk are insufficient when assessing or addressing uncertainty. Uncertainty and risk need to be separated as they require to be dealt with in very different ways. Uncertainty will be defined using the conceof ‘Knightian Uncertainty’. This paper will then apply research and insights developed by the Bank of England for dealing with uncertainty to offer an approach to National Security Strategy in ‘an age of uncertainty’. It concludes that uncertainty needs to be separated from risk using the distinction of ‘Knightian Uncertainty’ and dealt with according to the principle of simplicity and that of a ‘good enough’ performance. National Security Strategy and policy therefore needs to be re-orientated to function under uncertainty, as at present they only function under conditions of risk. The paper suggests that there is a case for a multi disciplinary research agenda that better translates the insights of work on uncertainty to security strategy.

1 The ‘Age of Uncertainty’

In 2010 the United Kingdom National Security Strategy declared that the UK was entering the ‘age of uncertainty’ (NSS 2010, 3). It was a marked escalation in rhetoric from the first National Security Strategy in 2008 which said that Britain lived in an interconnected world, albeit a complex and unpredictable one (NSS 2008, 3). In the foreword to the 2010 document, the Prime Minister and Deputy Prime Minister presented a paradox. Britain was now both more secure and more vulnerable than in most of its history (NSS 2010, 3). This duality, in their view, sat in stark contrast to the ‘brutal certainties of the Cold War (NSS 2010, 3).¹ This new strategic

¹Their predecessors might have raised an eyebrow to the notion that they had lived in a world of certainty, even with the concession that it was brutal.

environment called for:

A radical transformation in the way we think about national security and organise ourselves to protect it... This Strategy (sic) is about gearing Britain up for this new age of uncertainty – weighing up the threats we face, and preparing to deal with them. (NSS 2010, 3)

The document claimed that the assessment was based on a ‘hard-headed reappraisal of our foreign policy and security objectives’ (NSS 2010, 9). Taken at face value, the proposition that uncertainty now characterised the contemporary and future strategic environment, was itself a radical transformation in the way National Security was conceived. But what did this ‘radical transformation’, in the way we thought about national security look like? Annex A of the document specified the methodology used:

A.1 Risk assessment involves making judgements about the relative impact and likelihood of each risk in comparison with others. In order to undertake the National Security Risk Assessment (NSRA) we adapted the methodology used to compile the UK’s National Risk Register (which focuses only on domestic civil emergencies). (NSS 2010, 37)

The radical transformation was in fact the same methodology used in the 2008 strategy. Indeed the UK National Risk Register (NRR) methodology has been used for a long time in order to assess domestic civil contingencies (NSS 2010, 37). The use of a ‘likelihood’ versus ‘impact’ framework has been the foundation of most risk-based approaches for a generation and more. In fairness, the NRR was praised by the OECD as, ‘innovative best practice in risk communication to the public’ (cited in Tesh 2013). However its use in 2010 was neither radical nor transformational. Whatever the 2010 NSS claimed, it was in fact a very good but very conventional assessment of the risks to the UK.

The issue of relevance to this paper is that, whilst the assessments of risk are entirely valid, NSS 2010 drew no distinction between risk and uncertainty. No definition of uncertainty was provided. NSS 2010 appeared to imply that they were the same. The document could, by its own methodology and logic, have been titled ‘A strong Britain in an age of risk’. So what had actually changed between 2008 and 2010 in order to proms such a bold statement as ‘an age of uncertainty’? In short, the Government. ‘A strong Britain in an age of uncertainty’ is a catchy title and uncertainty a good hook to grab the readers attention. The new government needed to say similar things in an apparently new way in order to draw a difference with their predecessor. As a hook it worked well in proving a suitably serious and grand package in which to sell well-established ideas. What the document did not do was take its own proposition seriously.

Just as the Cabinet Office and MoD were declaring an age of uncertainty, the Bank of England (BoE) ² was concurrently conducting innovative research into the strategic and policy implications of uncertainty. On the 13th Se2007 a BBC news report revealed that Northern Rock Bank had approached the BoE for liquidity support (Peston 2007). On the morning of the 14th September there was a run on Northern Rock’s retail deposits during which £4.6 billion was withdrawn (HM Treasury 2012, 19). Northern Rock’s collapse was initially believed to be a risk that

²The ‘Old Lady of Threadneedle Street’ is the traditional nickname for the Bank of England.

was important, but isolated. That assumption proved to be wrong. On the 15th September 2008 the US investment bank, Lehman Brothers, filed for bankruptcy and the world's financial markets went into meltdown. The Global Financial Crisis (GFC) had begun. Since then the Bank of England and HM Treasury have been dealing with the worst financial crisis since the Great Depression of 1928.

For over 40 years the concept of risk has been central to the disciplines of finance and economics (Haldane 2012, 2). The use of risk assessment models within finance has been developed to a level of sophistication that makes the use of likelihood vs. impact models commonly used in security strategy literature look pedestrian. Such was the perceived success of financial risk methodologies, that those who ran the purest manifestation of the concept of risk, hedge funds, were referred to as 'Masters of the Universe'. Bankers and economists had believed in their own power and mastery over the financial world and in doing so created markets that they believed they could control through risk.

When the GFC struck, the financial universe collapsed, and the markets were revealed to be a complex monster that challenged that risk was ill equipped to deal with. In response some economists and financiers began to question the fundamental assumptions of their profession. Concepts of risk had proved to be inadequate to explain what had happened, or how to deal with it. Their world had been transformed from one characterised by interconnectedness and risk to one defined by complexity and uncertainty.

In the aftermath of the GFC the US Federal Reserve Bank and the BoE have undertaken research with potentially radical and transformational implications. They have revisited the idea of uncertainty and resurrected an older debate about what risk, ambiguity and uncertainty really are. They drew on a PHD economics thesis written in the 1910's by the economist Frank Knight. Knight argued that risk and uncertainty are substantially different and because of this, they must be addressed in different ways. The Bank of England has developed this research agenda with the Max Planck Institute ³ to produce a body of ideas that has aided them in thinking about uncertainty.

The starting point of this paper is to take seriously the proposition of the NSS; that we live in an 'age of uncertainty'. I will not debate whether this is true, that is another paper in itself. From that starting assumption the intention is to do what the NSS did not, and ask what uncertainty means and what might we do about it? The proposition of uncertainty is highly contentious and it will be interesting to see if, in the promised 2015 revision of the NSS, it is sustained, developed, or quietly dropped.

The argument made here is three fold. Firstly that the use of the term 'uncertainty' in security strategy literature is problematic, poorly defined and of little utility in formulating policy or strategy. Secondly that concepts and research outside of the paradigm of security strategy are more satisfactory in discussing the meaning and implications of uncertainty. Finally that risk and uncertainty should be separated, in order to be addressed properly. I will then consider how one might deal with uncertainty in strategy and policy.

Taking a Government statement seriously is a precarious thing to do. However I contend that the exercise is worthwhile precisely because the Government has not taken its own statement seriously, and has not followed through the logical

³Max Planck Institute for Human Development, <https://www.mpib-berlin.mpg.de/en/institute/profile>.

implication of what it might mean. I do not intend to substantially question or critique risk methodologies. It works well when applied to appropriate problems. The case I will make here is that they do not work well under conditions of uncertainty.

It is easy to throw stones at Government work and make cheap criticisms. The work of the 2010 NSS was laudable and thorough. I will assume, for the purposes of this paper, that the judgments it made concerning risk were correct. This paper will instead attempt to 'fill in the blank' that was left by the title.

I deliberately eschew any one paradigm or methodology. Instead it will deliberately embrace the call by the political scientists Sil & Katzenstein for 'analytic eclecticism' (2011). The essence of which is to make,

Intellectually and practically useful connections amongst clusters of analysis that are substantively related but normally formulated in separate paradigms. It rests on a pragmatic set of assumptions, downplays rigid epistemic commitments, and focuses on the consequences of scholarship for concrete dilemma. (2011, 2)

The focus of the paper will be how to turn uncertainty into something understandable and useful for policy makers and strategists.

The Cabinet Office and MoD in Whitehall sit just two miles from the Bank of England's offices on Threadneedle Street, yet neither department was aware of what the other was doing. This paper will synthesise the Cabinet Office and MoD's strategic quandary with some of the insights from the BoE's research. All three offices of state are all charged with ensuring stability and security for the UK within their respective areas. They might share a common fundamental mission, but are separated by physical department and intellectual discipline. There are other approaches to uncertainty advocated outside of the security strategy paradigm and the alternative BoE approaches offered here. However I am unable to address them all within the space allowed.

For the purposes of this paper strategy is defined as the,

Management of a chain of relationships among means and ends on many levels, it is best not conceived of as an identifiable actor or thing, but as the bridge that fuses them all together. (Porter 2013, 5)

Strategy is about achieving a position of advantage (Freedman 2014). Unlike UK strategy documents, I take Strachan's (2005) definition, which draws a distinction between strategy and policy. Policy is the ends you wish to achieve; strategy is the ways and means of achieving it (Strachan 2005, 52).

Analytical eclecticism draws on and applies ideas from different fields. The danger is doing this superficially. Ideas may appeal on the surface, but like a plant one has to bring the epistemological roots with it. This paper is developed conscious of that. However, whilst the disciplines may be different, the fundamental issues they are tackling are not. Complexity, risk and uncertainty are common themes. When discussed at the fundamental level, insights in one area transfer more readily to another. The BoE is learning lessons from the catastrophic failure of the GFC. Security Strategy has the opportunity to observe these lessons and draw useful conclusions from them without having to go through an equivalent crisis.

2 The use and abuse of uncertainty

Risk is the definitive theme of our age (Coker 2009, viii). Based upon the concept of rationality, it is a simple, flexible and robust framework. It has outperformed all other attempts to capture our fears and hopes about what might happen. Coker (2009) states that the dominance of risk is such that it is no longer just a methodological tool, but a mindset that pervades all areas of modern life (vii-xi). Management of risk became the means and the ends.

That the UK NSS of 2008 and 2010 chose to express strategy and policy in terms of risk is therefore unsurprising. However what can be argued about both documents, and indeed wider security literature from around 2001 onwards is that whilst risk is a necessary tool, it has proved to be an insufficient answer. NSS 2010 appears to hint at this, stating:

The risk picture is likely to become increasingly diverse. No single risk will dominate... Therefore achieving security will become more complex... We no longer face such predictable threats... The adversaries we face will change and diversify... Our ability to remain adaptable for the future will be fundamental, as will our ability to identify risk and opportunities at the earliest possible stage. (2010, 18)

Uncertainty haunts risk. However sophisticated our risk methodologies have become, however good we are at identifying and managing risks, the future remains unpredictable and our present world complex. Where risk once offered the chance to manage the world in which we lived, uncertainty and complexity about the past, present and future means we still struggle with the ‘fog’ of reality. The same was true of the financial world pre GFC. Post GFC it has become apparent that risk methodologies alone are not enough.

The rise of risk methodologies has its roots in mathematics, science and technology (Bremmer 2008, 3-4)⁴. As the dominant paradigm in formulating security strategy, it has influenced the discipline of security strategy towards assumptions of rationality, optimization and the scientific approach to knowledge (Strachan 2011). What if security strategy is more of an art than science, or indeed, if it requires a more sophisticated scientific approach?

Rather than being developed as a distinct concept, uncertainty in security strategy literature has become the policy equivalent of ‘caveat emptor’. Few have meaningfully engaged with what uncertainty really is, separate from risk.

In a special edition of the Cambridge Review of International Studies published in 1999, three leading scholars characterised the period 1989 – 1999 as ‘The Interregnum’,

We might have employed a different word or none at all. But in the end, it was felt that the idea of an interregnum as a space between one era and another at least captured something about the ill-defined and almost impossible-to-define character of the last ten years... while we might know what our modern era is not — it is not a Cold War — we are not at all sure what it is, or where it might be leading to. (Cox, Booth, Dunne 1999, 4)

⁴See Paul K. Davis, (2012) ‘Lessons from RAND’s work on planning under uncertainty for National Security’, as an example of RAND’s scientific approach to risk and uncertainty over 40 years.

‘Interregnum’ was a scholarly way of saying that no one really knew what was happening. Cox, Booth and Dunne warned of the ‘problem of uncertainty and the extent to which we can ever really know what lies round the corner’ (1999, 6). Surveying the events of the past ten years they cautioned that,

History has a rare knack of playing tricks on people, increasingly so in this age of the unexpected where the old rules of the game appear to have been torn up and the new ones are still being written. (1999, 6)

Their invocation of uncertainty was a caution against the hubris of the past ten years. Those who wanted to proclaim the ‘End of History’ (Fukuyama...) or a ‘New World Order’ (Bush 1991), or a ‘Doctrine of the international community’ (Blair 1999) were liable to be made fools of by reality.

The journal edition was a sober and measured volume, which urged intellectual and practical humility, and also spoke of the complexity of the problems we faced (1999, 19).

If we learn no other ‘lesson’ from the last ten years of the twentieth century, it is that we rule out the unlikely at our peril. The past has been full of ‘radical surprises’. (1999, 6)

The argued that uncertainty was a fog, but the right questions and research would diminish it and complexity could be accommodated. The Interregnum edition of the Review of International Studies stands as a useful bookmark in the literature as of 1999, because when compared to more recent assessments, it is clear the interregnum is not over. The recent MoD Global Strategic Trends surveys of 2010 and 2014 take up much of the same research agenda as outlined by Cox et al, and are no closer to sketching out a new order or identifying satisfactory theories. The term interregnum never caught on within the wider literature but it is clear that it encapsulates a large part of what was meant when NSS 2010 talked of an ‘age of uncertainty’.

In the wake of 911, uncertainty moved from being a theme, to center stage (Fitzsimmons 2006, 132). On the 30th September 2001, just 19 days after the attacks on the United States, the US Defence Department published the Quadrennial Defence Review (QDR). The main body of the document, in common with the 1997 QDR, and in a similar vein to Cox, Booth & Dunne (1999), emphasised uncertainty as a characteristic of contemporary international relations. However, in the wake of 911, the front piece to the QDR was redrafted and stated:

We can be clear about trends, but uncertain about events. We can identify threats, but cannot know when or where America or its friends will be attacked. We should try mightily to avoid surprise, but we must also learn to expect it... Even before the attack of September 11, 2001, the senior leaders of the Defense Department set out to establish a new strategy for America’s defense that would embrace uncertainty and contend with surprise. (QDR 2001, iii)

In keeping with the rest of the literature was the idea that uncertainty was more prevalent now than before. It also assumed that uncertainty was surprise, deviance from the norm, a failure of risk and rational thinking, but one that could be dealt with through refinement and improvement to risk approaches. The 2005 National Defence

Strategy went even further, identifying uncertainty ‘as the defining characteristics of today’s strategic environment.’ (Cited in Fitzsimmons 2006, 132).

US Defense Secretary Donald Rumsfeld was to push the idea of uncertainty harder and further than any one, and was in turn to provide the most famous summary,

As we know, there are known knowns; there are things we know we know.
We also know there are known unknowns; that is to say we know there
are some things we do not know. But there are also unknown unknowns
— the ones we don’t know we don’t know.

It was a neat definition, but it was never actually used as anything other than a clever rhetorical device. The increased discussion and use of uncertainty in strategy since 2001 did not arguably produce satisfactory strategy. Fitzsimmons (2006) criticizes the way and the extent, to which uncertainty was used, arguing,

Who can deny that surprise is a fact of life? It is self evident that that
predicting the future is difficult, all the more so when the subject of the
prediction is a network of highly complex, dynamic, human systems, like
international politics. (2006, 133)

Placing uncertainty at the heart of strategic planning is problematic and can be counter productive. Fitzsimmons argued that the notion that today’s future is less certain than yesterday is overdrawn (2006, 134). His main critique of the use of uncertainty, is that it presents a problem without answer. Planning factors and scenarios become too varied to have depth, assumptions too broad, the very tools and fabric of rigorous analysis collapse in muddle indecision and imprecision (2000, 142). Rather than assisting in creating flexibility, uncertainty invites intellectual confusion into the planning process.

A strategist who sees uncertainty as the central fact of his environment
brings upon himself some of the pathologies of crisis decision-making.
(2006, 135)

Summing up his critique Fitzsimmons argues that,

Undue emphasis in planning on uncertainty creates an intellectual temp-
tation to cognitive dissonance on the one hand and confirmatory bias on
the other. And the effect, both insidious and ironic, is that the apprecia-
tion for uncertainty subverts exactly the value that it professes to serve,
flexibility. (2006, 136)

Eight years on that last paragrastill accurately captures the use of uncertainty, which is rife in strategic planning and the wider literature.

However Fitzsimmons’ answer to the problems of using uncertainty was a robust defence of the traditional analysis and planning methodology. Citing common cause with Betts (2000), he argued that,

A risk orientated approach seems to be the only viable model for na-
tional security strategic planning... Unless they (strategists) are willing
to quit and go fishing, then, strategists must sharpen up their tools of
risk assessment. (2006, 143)

In that respect he mirrored the assumptions of officials within the security and strategy establishment and a significant portion of the academic literature. One simply needed to reinvigorated and expanded existing methodologies in order to meet the challenge of uncertainty (for example Edmunds 2014).

Security strategy had still not produced a meaningful appreciation of uncertainty, separated from the risk, in contrast to other academic disciplines. The proposed answer to the shortcomings of risk comes in the form of platitudes, calling for ‘adaptability’, ‘flexibility’ and ‘resilience’ (for example NSS 2010, 18 or QDR 2006, 1–2). But do these statements really tell us how to address uncertainty as a distinct phenomenon? To expose just how vacuous the statements are, one only needs to turn them on their head. Under what circumstances would anyone advocate a rigid, inflexible and delicate security strategy? Has there ever been a time when Governments didn’t advocate flexibility in strategy? At the height of the Cold War US Secretary of Defence Robert McNamara reshaped US nuclear policy under the heading of ‘Flexible Response’.

We don’t know how to respond to uncertainty because we haven’t confronted it in isolation from risk and have yet to define it properly. It is used as a synonym for unclear, changeable, tentative, unreliable and ambiguous. The US placed uncertainty front and center in their security strategy and the UK has followed suit. As such our current strategic disposition favors risk but is unable to address uncertainty. Uncertainty needs to be defined and separated from risk.

3 Separating risk and uncertainty

On one level everything is uncertain. Discussions of uncertainty are therefore problematic and can collapse rapidly into vague circular discussions that have little utility for strategy. The challenge the security strategy community faces is to produce policy recommendations of action or inaction in the face of an issue. It is an answer-orientated community and I believe that this leads to a tendency to conflate risk and uncertainty. It is unsurprising that NSS 2010 neither provided a definition of uncertainty, nor meaningfully used the conceto do anything other than simply imply, ‘we just don’t know’. In a world where every action or inaction, statement and decision by government is forensically scrutinized in hindsight, uncertainty is a sophisticated sounding hedge against anything.

In science and economics the meaning and significance of uncertainty has been has been a subject of intense research and discussion (Peat 2002, xiii–ix). This body of work is potentially transferable across disciplinary boundaries. As explained earlier, uncertainty is often used to make the obvious statement that we cannot predict the future (for example Cox, Booth and Dunne 1999). However Bayesian mathematician Lindley states that real uncertainty is personal; it is not *the* uncertainty but *your* uncertainty about something (2014: 1-2). It expresses a relationship between the person making the statement and the real world about which the statement is made.

In that respect uncertainty is not objective in the sense that it expresses a property that is the same for all of us (2014, 3). The UK Government may well feel that it exists in an age of uncertainty, but other nations could believe the opposite. The use of the term uncertainty in security strategy is often used to refer to the outcome of a policy or future states of the world. In that sense it isn’t saying anything useful, as we are never able to be certain about the future. Taking Lindley’s conception of uncertainty, a statement about a relationshiuncertainty becomes useful. We are never

able to predict future ends but we may be able to alter or influence relationship of the means and ways, and so alter the extent of our uncertainty. Placing the emphasis on the relationship moves dealing with uncertainty into the realm of strategy, the management of relationship (Porter 2013, 5)

Lindley argues that one should admit and highlight uncertainty rather than suppress it (2014: 11). The arguable natural tendency of risk methodologies is to suppress it. Risk is conventionally formulated, as the likelihood of an event occurring, versus impact of the event occurring will have. It therefore attempts to frame a problem by assigning values to the key factors of it. This can be done either quantitatively or qualitatively, making it an incredibly flexible tool. The use of a risk methodology does not require certainty. That is to say, the factors you input do not have to be absolutely precise in order for it to work (Bremmer 2008: 3). It can accommodate a level of uncertainty. Hence the two are often used in the literature interchangeably. The NSS uses uncertainty as a general statement about knowledge of the future and the imperfection of prediction.

What a risk methodology does assume is that one can identify the relevant and important factors, and assign some form of value to these factors. It assumes that the world in which we live in knowable and discernable. Contrary to this position, the economist Hayek, in his 1974 Noble Prize acceptance speech, argued that,

Unlike the position that exists in the physical sciences, in economics and other disciplines that deal with essentially complex phenomena, the aspects of the events to be accounted for about which we can get quantitative data are necessarily limited and may not include the important ones. While in the physical sciences it is generally assumed... that any important factor which determines the observed events will itself be directly observable and measurable. (1974)

Hayek's speech, 'The Pretense of Knowledge', was a continuation of his long running critique of an excessively scientific approach to economics and social sciences. Thinkers such as Hayek (1974) and recently Taleb (2010 & 2012) take the imperfections of knowledge as their foundational assumption. The problem with risk is that it sits within an epistemology that seeks to know all that we can and then hedge against it. What if the world which security strategist's deal with is one in which important factors are not observable or measurable, and therefore subvert risk assessment?

The US Federal Reserve and the Bank of England faced this problem in the wake of the GFC. Their risk methodologies proved to be inadequate. The issue as Haldane, Executive Director of Financial Stability at the BoE, states, is that models of decision-making under risk assume that future states of the world are known by agents and so are able to be priced and hedged (2012, 2-3). Combined with this, is the assumption of rational expectations, that information collection is close to costless and that agents have sufficient cognitive facilities to weight probabilistically all future outcomes (2012, 1-2). The pursuit of stability and security pre GFC was the pursuit of further perfecting knowledge and refining the risk models. Post GFC the two central banks began to wonder if the world in which they lived was not one of known knowns and known unknowns but rather of complex unknown unknowns.

The response of both organisations was to resurrect a concept of uncertainty that had largely disappeared from mainstream economics due to the success of risk methodologies, that of 'Knightian Uncertainty' (Haldane 2012, 2 and Pritsker 2010).

Frank Knight, later professor of Economics at Chicago University, published his 1916 PhD thesis in economics in 1921, as the text *Risk, Uncertainty and Profit*. In it he attempted to explain the role and contribution of entrepreneurs in a capitalist system. The most enduring idea was his definition of risk and uncertainty. Knight drew a distinction, which is worth quoting at length, as it is central to this argument,

Uncertainty must be taken in a sense radically distinct from the familiar notion of Risk, from which it has never been properly separated. The term “risk” as loosely used in everyday speech and in economic discussion, really covers two things which, functionally at least, in their causal relations to the phenomena of economic organisation are categorically different. The essential fact is that ‘risk’ means in some cases a quantity susceptible of measurement, while at other times it is something distinctly not of this character; and there are far-reaching and crucial differences in the bearings of the phenomena depending on which of the two is really present and operating... It will appear that a measurable uncertainty, or ‘risk’ proper, as we shall use the term, is so far different from an *unmeasurable* one that it is not in effect an uncertainty at all. (1921, 19)

For Knight, true risk could be quantified in some form and real uncertainty could not (1921, 233). Knight belonged to the school of economics that placed the imperfection of knowledge at the heart of theory and used it to explain the world (1921, 206–210). The distinction became known as ‘Knightian Uncertainty’, but as a theory it was overtaken by the rise and apparent success of probabilistic risk methodologies.

There are two basic critiques of ‘Knightian Uncertainty’. Firstly, that it presents a false dichotomy. Taleb argues that one never ever knows the odds of any situation but has to discover them (2010, 128). In his view Knight is wrong to say that there is no such a thing as true risk, known knowns, as differentiated from unknown uncertainty.

The second criticism of ‘Knightian Uncertainty’ is that uncertainty is already accounted for in the conventional risk models. Uncertainty is a component of likelihood. This could account for the lack of a distinction or definition in the risk models used. Uncertainty is ubiquitous and risk approaches do not claim, or require, absolute certainty, in order to work.

One can argue that ‘Knightian Uncertainty’ is a false dichotomy and still find value in it as a tool. All tools are, to an extent, over simplifications in order to aid in thinking about difficult problems. Even if a false dichotomy, provides a useful vehicle to surface and accentuate the extent uncertainty in security strategy problems. Uncoupling uncertainty allows risk methodologies to play to their methodological strength. Conflating the two subverts the overall product and has the tendency to hide uncertainty or at least undervalue it. This is the weakness of the NSS 2010. ‘Knightian Uncertainty’ addresses these issues whilst also respecting and allowing for the methodological strengths of risk approaches.

4 Adapting security strategy to the ‘Age of Uncertainty’

Gigerenzer (2014) states that in dealing with uncertainty, ‘You will fail if you use the tools of risk’. I will draw on the body of research by Gigerenzer and the BoE

(principally Haldane) and translate the strategy and policy ideas they have developed to security strategy. The main conclusion of this body of work is that the answer to ‘Knightian Uncertainty’ is simplicity. As Haldane states,

Under risk, policy should be fine respond to every raindroit is fine tuned.
Under uncertainty, that logic is revered. Complex environments often call for simple decision rules. That is because these rules are more robust to ignorance. Under uncertainty, policy may only respond to every thunderstorm, it is coarse tuned. (2012, 3)

The proposition of simplicity in the face of complexity and uncertainty may at first appear a somewhat glib response. However it is based on accepting the limits of knowledge and understanding the true nature of uncertainty. It supposes, as Hayek argued, that our knowledge of the world is limited and incomplete. Complexity can create uncertainty because the variables are too great to calculate and because what is important might not be observable or measurable. You are in the realms of unknown unknowns by virtue of complexity and it requires an appropriate response.

The conventional response within literature is to meet complexity with complexity. ‘Complex Adaptive Systems’ or ‘wicked problems’ require an equally complex solutions or an adaptive strategy. These approaches share a fundamental assumption with risk methodologies. It is that we are able to eventually find out all that we need to know about a problem, and so convert unknown unknowns into known knowns, or at the very least known unknowns. It also assumes that we have the cognitive capacity to process this information and act upon it.

The approach to uncertainty advocated by Knight (1922), Taleb (2010), Gigerenzer (2014) and Haldane (2012) all reject this conclusion and instead assume the opposite. Rather than trying to fight complexity and uncertainty they advocate accepting the limits of our knowledge and working within it to produce satisfactory rather than optimal results. Harford (2011) highlights the applicability of this approach in a number of different fields. From engineering to business to biology, attempts to meet complexity with complexity, or apply rational optimization approaches, don’t just result in a worse performance relative to simple approaches under uncertainty, but rather catastrophic results. Bremmer calls optimization under uncertainty a ‘false idol’ (2013, 213).

The first and most important task of strategists therefore, is to determine whether the nature of the problem one is dealing with is a risk or an uncertainty. To use techniques appropriate to uncertainty to address problems of risk would be just as mistaken. Applying the Knightian distinction, or the Rumsfeld short hand, aids in the correct diagnosis. Using Lindley’s conception of uncertainty helorientate strategists to the fact it is the relationship that matter, not the outcome, which is always uncertain.

Gigerenzer (2010) Haldane (2012) argues that one should use simple heuristic rules to make decisions under uncertainty,

As you do not fight fire with fire, you do not fight complexity with complexity. Because complexity generates uncertainty, not risk, it requires your regulatory response to be grounded in simplicity not complexity. (Haldane 2012, 24)

Simple heuristic rules are those that look at only a few parameters and try to be robust (Gigerenzer 2014). Accepting the limits of knowledge and the difficulty of

acting under uncertainty, the most appropriate aim, according to Gigerenzer is to be 'good enough', as opposed to risk-based approaches that seek to tailor and rationally optimise actions. The Bank of England's research bases their concept of simple heuristic rules approach on five ideas.

First, information gathering is not cost free and the cost of cognition is detrimental. Unfortunately the founding models of risk assumed that it was cost free (Haldane 2012: 2). In that respect they made neat models but fall foul of Taleb's (2010: 128) critique that they were elegant in the laboratory but are less useful in the real world. If one accepts Hayek's argument about the limit of knowledge and adopts Knightian Uncertainty, then gathering more information is a cost that does not yield results. Information can exceed our cognitive capacity or becomes too costly to gather. At a certain point a decision has to be made and compromise reached. Risk approaches in contrast place a premium on rational optimization and maximization of information. Here the distinction between risk and uncertainty is highly useful because it would allow a decision maker to recognise that less information is actually more useful. Simons (1956) called this 'bounded rationality' and 'satisficing', getting just enough information but no more. The aim is to be 'good enough' in general, rather than ideal in particular.

Secondly disregarding information can produce not only cognitively cheaper but better decisions (Haldane 2012, 4). Too much information can oversensitise decision-making models. Historical data can be misleading, it is deductive about the past but is not necessarily inductive about the future. Haldane points to research that demonstrate that 'decision rules based on one, or a few, good reasons can trump more sophisticated models' (2012, 5). Risk responses based upon past information will not just underperform relative to simple rules; they may actually be catastrophic. Talib states that learning from the past is 'negative knowledge' that may prove to be at best irrelevant, or at worst, viciously misleading (2010, 40-41). Risk methodologies can be so finely tuned that when they fail, they fail completely, particularly in tightly woven complex problems as shown by the GFC (Harford 2011). They are ideal responses for specific circumstances but not good enough for a broad range of possibilities. It is what is known in the military as preparing perfectly for the last war.

Thirdly, giving equal weighting to all options available can outperform more sophisticated weighting models used in risk. This is the 1/N rule, where all options (N) are weighted equally as 1. Rather than weighting each option by differentiating between them on likelihood and impact, you assume all possibilities are equal. You therefore do not try to discriminate between possible outcomes; instead you adopt a broad capability based approach that allows for you to deal with as many of them as occurring as possible. Done properly this means that performance will be average (good enough). You will not perform to the optimum level, but you will not catastrophically fail by preparing for what turns out to be the wrong event. Gigerenzer (2014) notes that the economist Markowitz, famous for developing the risk weighting strategies used in financial investment, adopted the 1/N approach in investing for his retirement.

Fourth, the small samples on which so many assessments are made are deeply problematic, they simply cannot support the weight of assumptions placed upon them. Smaller samples increase the sensitivity of estimates to past information (Haldane 2012, 6). Bigger samples taken over longer periods of time can support complex and detailed decisions in depth. One must realize just how big a sample

needs to be and indeed how small so many of our supposedly 'big' samples really are. Haldane cites the evidence of De Miguel et al (cited in Haldane 2012, 6) whose study of investment strategies showed that the sample threshold at which complex rules outperform simple rules (such as 1/N) was when there was in excess of 250 years worth of data. How many security strategy risk models have data sets that large?

Finally, simple rules are easy to understand by all actors and therefore encourage the correct behavior (2012, 7). Because as Lindley states, our relationships with the real world are personal, and so statements of certainty or uncertainty are personal, interpretations of the world can vary dramatically. Therefore sophisticated or complex responses to problems can easily be misunderstood both in meaning and intent. Simple heuristic rules are easier to understand and harder to get wrong. They are pejorative, but again this is acceptable under conditions of uncertainty because the aim is good enough performance, not ideal. Haldane (2012, 7) also points to the fact that people are less able 'game' simple heuristic rules. Gigerenzer (2014) calls this tendency to 'game' risk based rules 'defensive behavior'. Risk approaches encourage optimum responses and so under conditions of uncertainty actors seek to minimize their liability and reduce the risks they take, in short 'covering your ass'. Risk methodologies are all about minimizing risk. This can lead, under uncertainty, to the wrong behavior or indeed bad behavior. Simple rules, correctly aligned to the issue, keep people focused on the bigger picture, rather than the small print. I will illustrate this point later with regard to NATO Article 5.

In the part 2 it was shown how the response within both US and UK security strategy to uncertainty was to advocate 'flexibility' and 'adaptability'. They were largely hollow phrases because they were not based upon a rigorous methodology. The responses advocated here, simplicity in response correctly diagnosed uncertainty, provides a meaningful basis on which to base a flexible and adaptable strategy under uncertainty.

A strategy based upon flexibility and adaptability doesn't really tell you what not to do. One would never advocate being inflexible. However one could argue against 'satisficing' and or adopting a 1/N approach. The opposite of both would be optimization and discriminatory risk weighting. Unlike in so much of security strategy, the research identified here offers both what to do, and also makes clear what not to do, because the arguments can be falsified. Much of the above would provide a rigorous definition of flexibility and adaptability. The body of literature may well label it 'simplicity' but one could, to put anxious minds at ease, re-label it within security strategy. It would back fill an otherwise intellectually empty vessel.

NSS 2010 called for a radical transformation of the way we conceive of strategy in response to the age of uncertainty (2010, 3). The research and strategy developed by the BoE does exactly that, and the ideas would have been regarded as heresy pre GFC. I will now offer some brief examples of how, using Knightian Uncertainty, the principle of simplicity in response to complexity, and the aim of a good enough performance, might better orientate security strategy under uncertainty. I use the term 'orientate' deliberately. By its very nature you cannot directly counter uncertainty in the concrete terms you would under risk. Instead you re-orientate strategy and policy so that it is able to perform under conditions of uncertainty. It should be seen as complementary to the NSS assessment of risk, not in competition. Security strategy should be divided between risk and on uncertainty and then these areas addressed in separate and appropriate ways.

The most far-reaching conclusion of the study of uncertainty, compared to risk, is that risk approaches do not just under perform relative to simple, uncertainty orientated approaches, they can fail catastrophically. Has the security strategy discipline constructed a falsely reassuring world of risk, as the financial markets did pre GFC?

The evidence that risk approaches perform worse under uncertainty can be addressed using the 1/N equal weighting methodology. Balanced, flexible and adaptable forces have been the aspiration of defence planners for years; yet have been undermined by the demands of the day and the prejudices of yesterday. The appropriate intellectual arguments have never quite been made because it lacked a persuasive evidence base, which tentatively now exists. Separating risk and uncertainty would allow for some force elements to be calibrated towards optimisation against identified risks and other elements to adopt a 1/N approach against uncertainty. One area this is already applied, but is under renewed debate, is the UK's nuclear deterrence. Trident is an example of a 1/N approach to the threat of interstate war. It is however the only 1/N tool we have for a multitude of uncertainties.

Explicitly adopting a procurement policy that aimed for 'good enough' performance in some areas, and optimized equipment in others, could ease the requirement on procurement. Davis (cited in Bremmer 2008, 209) argues for a capability based upon, modularity, adaptiveness and robustness over optimization. As an example of the policy relevance of this approach, the Royal Navy decided against the building of a new class of modular, economical and multi role corvette, because the RN still prefers hyper optimized platforms.⁵ The research advocated here could have provided the intellectual justification, that has been either absent or found wanting, in making the case for what a flexible and adaptive forces would actually be based on.

Simple heuristic rules may well operate well under uncertainty but their performance will be directly linked to the people exercising judgment. Haldane (2012) states,

Simple rules are not costless. They place a heavy emphasis on the judgment of the decision maker, on picking appropriate heuristics. (7)

This is especially true when one defines strategy as one of managing relative relationship between ends ways and means; it is always in flux and relies on judgment. Gigerenzer (2014) places huge emphasis on the value of experience and intuition in dealing with uncertainty. However exactly who and what type and nature of experience is deeply problematic. How do we develop the right people in the right way? It is in a sense an appeal to reinstate 'wisdom' as a formal requirement in security strategy apparatus.

If the UK is uncertain about the world then it needs to develop experience and retain it. Currently the departments of Government do not develop deep experience, instead placing greater emphasis on generic skills and a modularized approach education. The House of Commons Foreign Affairs Select Committee recently took up this debate with the Foreign Office stating that:

Our concern, which persists, is that certain strengths, such as depth of understanding of a country or a highly developed ability to communicate in a local language, appear not to carry significant weight in comparison

⁵See UK MOD DCDC, (2012) Future 'Black Swan' Class Sloop-Of-War: A Group System, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33686/20120503JCN112_Black_SwanU.pdf, accessed 1st Sep 2014.

to more generic skills... which make up the core competencies. (House of Commons 2013, para 54-61)

The Foreign Secretary had previously stated a desire to place a premium on languages and regional experience in the selection and deployment of diplomats, saying that,

Our diplomats need to have an unrivalled knowledge among diplomats of the history, culture, geography and politics of the countries they are posted to, and to speak the local languages. (Ibid, para 57)

However, in the committee's opinion, little action was taken.

Gigerenzer's research confirms what people (ironically) intuitively believe anyway, experience matters. People are inclined to defer and refer to those who they perceived to have it. Field Marshall Lord Wavell maintained that the most important quality of a strategist was,

What the French call *le sens du praticable*, and we call common sense, knowledge of what is and is not possible. (cited in Gray 1999, 32)

Hayek (1976) made a similar appeal in his Nobel Prize lecture,

If man is not to do more harm than good in his efforts to improve the social order, he will have to learn that in this, as in all other fields where essential complexity of an organized kind prevails, he cannot acquire the full knowledge which would make mastery of the events possible. He will therefore have to use what knowledge he can achieve, not to shathe results as the craftsman shapes his handiwork, but rather to cultivate a growth by providing the appropriate environment, in the manner in which the gardener does this for his plants. (Hayek 1976)

In order to deal with uncertainty we need to develop and retain and reward real experience, over time. It is a policy recommendation that should be explicitly linked to the National Security Strategy and justified as an effective means of developing strategy under uncertainty. It is by no means a quick or easy task, and requires further substantive research and implementation, but it is an example of a recommendation missed by NSS 2010 because it did not follow through its own proposition. The BoE meanwhile is reforming structures to ensure institutional wisdom through its people.

Another example of reassessing and re-orientating strategy for uncertainty is the application of simple rules that are robust in the face of complexity. NATO Article 5 is an excellent example. It states that an attack on one is an attack on all (NATO 2014). The response to an attack therefore is war with the NATO alliance. Rather than being able to manipulate alliances or pick off individual countries, the simplicity and robustness of this rule means that the adversaries have to weigh all actions on the basis that it could provoke an overwhelming response. Likewise NATO had to be mindful that its actions did not undermine the rule. Actions were orientated towards their bigger implications, not the small print. Gigerenzer (2014) provides a fresh basis on which to reinvigorate an old idea.

Appreciating the value of simple heuristic rules under uncertainty could assist in appreciating rules and international norms. You could seek to orientate your activity to uphold the integrity of rules you valued under uncertainty. Rather than match

complex threats and continually try to optimize the response, the actual goal would be to minimize the extent to which adversaries can find asymmetric means to subvert the integrity of a rule. One only has to look to see the very real threat of this in Ukraine now. In Crimea, Russia reportedly employed asymmetric tactics to create doubt and maximize complexity. They successfully subverted basic international rules such as borders and sovereignty, and in doing so achieved their aim.

If one applies the insight of Gigerenzer et al, one would understand that the real threat that NATO faces is not necessarily how to match and defeat Russian asymmetric tactics, but how to preserve the integrity of robust simple rules such as Article 5, in the face of subversion. One could also apply this approach to thinking about how to uphold international rules and clarify thinking about what it is in those rules that matter most, a priority of the NSS 2010 (33). The BoE is currently exploring simplifying financial regulations in order to ensure the correct response from the financial services and not asymmetric assault by armies of bankers and lawyers. Robustness trumps sophistication under uncertainty.

Defensive behaviors, as promoted by risk, stands in contrast to the offensive, or 'positive', behavior advocated under uncertainty. By solely adopting a risk approach we have adopted a defensive approach that undermines performance under uncertainty. Knight used his distinction to draw a difference between business people, who were comfortable operating under risk (defensive) and entrepreneurs who performed well under uncertainty (offensive) (1921, Chap X). The UK may be a nation that has decided that it operates under risk, but other nations in the world, currently Russia, have clearly decided to embrace uncertainty. Russia is, in a Knightian sense, a 'strategic entrepreneur'. Risk orientates us to the consequences of our actions and so we are likely to miss opportunities. Strategic entrepreneurs such as Russia will face consequences for its actions, but are exploiting and sowing uncertainty in order to shatter their overall strategic environment. We may well choose to continue risk averse policies, but it is useful to understand the nature of such a choice. The end goal of other nations might be global uncertainty itself, where they are comfortable operating and we are not. As Coker states,

At the heart of the paradox... is the fact that other societies are willing to take very great risks indeed. It is their predisposition for risk-taking that may force us to confront or overcome our own predisposition to be risk averse. (2009, x)

We are going to have to deal with a world of uncertainty and strategic entrepreneurs.

Finally the issue of the cost of cognition, that less information can lead to better decisions, and the danger of small samples sizes; all contribute towards putting the wider issue of information and decision making in a different context. Rather than believing that the more we know about something, the less uncertain it will be, we would understand that less is more. Identifying and knowing a few key things, and understanding them very well, would aid in prioritizing information requirements. The BoE has reduced the number and type of indicators it requires banks to submit (Gigerenzer 2014) and so freed BoE capacity for other tasks. Governments often decide not to find something out, not out of choice, but lack of capacity.

Conclusion

What this eclectic approach to uncertainty has attempted to do is part of what Bremmer has called 'shifting from solutions based approach to one of a management approach' in strategy (2008, 302). This matches Lindley's conception of uncertainty as a statement about a relationship rather than objective fact. Bremmer's argument is in favor of adopting a broader range of approaches to strategic risk, ambiguity and uncertainty. Gigerenzer's and the BoE's research doesn't solve the problem, but reconstitutes the problem in a useful way. Even those who might dispute conceiving of uncertainty separately within strategy cannot deny that traditional risk based approaches have proved insufficient, and in other fields catastrophic. Attempts to improve them through greater refinement or increased sophistication do not address the fundamental methodological problems. At the very least this paper offers a number of areas that would warrant an interdisciplinary research agenda, as there appears to be a gap in the literature when it comes to uncertainty.

The UK NSS led with uncertainty because the US had made it a main theme in the 2000's. The 2014 US Department of Defence QDR has quietly dropped uncertainty when compared to the 2006 QDR. Instead it uses terms such as volatility and change. It will be interesting to see what use the 2015 UK NSS makes of uncertainty.

Risk is susceptible to measurement in some form. Uncertainty by the definition employed here, is not. Uncertainty therefore requires a substantially different approach, one that seeks satisfactory performance based on a principle of simplicity. Paradoxically, simplicity under uncertainty is the optimum approach. The Global Financial Crisis showed what happens when exclusively risk-based approaches fail. Global financial systems have been incredibly fortunate to survive the crash, but it has exacted a heavy cost. It has exposed us to a weakness that had been overlooked and also provides the possibility of insight and lessons to be learnt. It is a shame therefore that the lessons have not been carried across to security strategy. Gigerenzer's research has been used in medicine, finance, business and technology. Because he has focused on general principles and their relevance and application to real life, the ideas are readily transferable. Security Strategy needs to approach uncertainty in a more intellectually rigorous and multidisciplinary way. Uncertainty needs to be freed it from risk methodology, thereby allowing risk methodologies to perform to their optimum, and for uncertainty to be addressed in the appropriate ways.

References

- Anderson, R. (2011), 'Masters of the Universe, meet the world's best-paid men', BBC News, 2nd Feb, <http://www.bbc.co.uk/news/business-11942117>, accessed 28th August 2014
- Blair, T. (1999) 'Doctrine of the International Community', 24th April, National Archive, Official Site of the Prime Minister, <http://webarchive.nationalarchives.gov.uk/+www.number10.gov.uk/Page1297>, accessed 23rd August, 2014
- Bremmer, I. ed. (2008) *Managing Strategic Surprise*. Cambridge University Press
- Bush, G. (1991) 'Address Before a Joint Session of the Congress on the State of the Union', January 29, <http://www.presidency.ucsb.edu/ws/?pid=19253>, accessed 24th August 2014
- Coker, C. (2009) *War in an Age of Risk*. Polity Press

- (2009) *Rebooting the West*. RUSI Whitehall Paper, London
- Cox, M. Boothe, K and Dunne, T. (1999) 'Introduction: The Interregnum controversies in world politics, 1989–99', *Review of International Studies*, 25, pp. 3–19
- Edmunds, T. (2014) 'Complexity, Strategy and the National Interest', *International Affairs*, 90:3, pp. 525–539
- Fitzsimmons, M. (2006) 'The Problem of Uncertainty in Strategic Planning', *Survival*, 48(4), pp. 131–146
- Freedman, L. (2014) 'Stop looking for the Centre of Gravity', War on the Rocks Blog, 24th June, <http://warontherocks.com/2014/06/stop-looking-for-the-center-of-gravity/>, accessed 25th August 2014
- Fukuyama, F. (1989) 'The End of History', *The National Interest*, Summer 1989, <http://www.kropfpolisci.com/exceptionalism.fukuyama.pdf>, accessed 29th August 2014
- Gigerenzer, G. (2014) *Risk Savvy*, LSE Lectures, 2014
- Goldin, I. & Mariathasan, M. (2014) *The Butterfly Defence*, Princeton University Press
- Graham, D. A. 'Rumsfeld's Knowns and Unknowns: The Intellectual History of a Quip', *The Atlantic*, March 27, 2014, <http://www.theatlantic.com/politics/archive/2014/03/rumsfelds-knowns-and-unknowns-the-intellectual-history-of-a-quip/359719/>, accessed 11th Aug 2014
- Gray, C. S. (1999) *Modern Strategy*. Oxford University Press
- (2002) 'Thinking Asymmetrically in Times of Terror', *Parameters*, Spring 2002, pp. 5–14
- Haldane, A. G. (2012) 'The Dog and the Frisbee', Speech given at the Federal Reserve Bank of Kansas City's 36th economic policy symposium, 'The Changing Policy Landscape', Wyoming
- Harford, T. (2011) 'What we can learn from a nuclear reactor', *The Financial Times*, Jan 14th, <http://www.ft.com/cms/s/2/cea7b256-1def-11e0-badd-00144feab49a.html#axzz3Bz6Z5NZq>, accessed 2th Sep. 2014
- Hayek, F. A. V. (1974) 'The Pretense of Knowledge', Available from: http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/1974/hayek-lecture.html, accessed 28th August 2014
- HM Treasury (2012) 'Review of HM Treasury's management response to the financial crisis', HMSO, London, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220506/review_fin_crisis_response_290312.pdf, accessed 28th August 2014
- House of Commons (2013), Foreign Affairs Select Committee, Fifth Report, FCO performance and finances 2011-12, HMSO, London, 2013 <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmfaaff/690/69009.htm#a7>, accessed 1st Sep. 2014
- Clauswitz, C. von (2007) *On War*; Ed. and trans. by Howard. H, and Paret, P. Oxford University Press
- Knight, F. H. (1921) *Risk, Uncertainty and Profit*, LSE Reprint (1946)
- Lindley, D. V. (2014) *Understanding Uncertainty*. Wiley
- NATO (2014) 'What is Article 5?', <http://www.nato.int/terrorism/five.htm>, accessed 1st Sep. 2014
- Peat, F. D. (2002) *From Certainty to Uncertainty*. Joseph Henry Press

- Peston, R. (2007) 'Northern Rock gets bank bail out' BBC News, 13th Sept, <http://news.bbc.co.uk/1/hi/business/6994099.stm>, accessed 1st Sep. 2014
- Porter, P. (2013) *Sharing Power? Prospects for a US Concert-Balance Strategy*. US Army War College Press
- Pritsker, M. (2010) 'Knightian Uncertainty and Interbank Lending', http://www.chicagofed.org/digital_assets/others/events/2010/bsc/Matt%20Pritsker.pdf, accessed on 1st Sep. 2014
- Sil, R. & Katzenstein, P. J. (2010) *Beyond Paradigms, Analytic Eclecticism in the Study of World Politics*. Palgrave Macmillan
- Simons, H. A. (1956) 'Rational Choice and the Structure of the Environment', *Psychology Review*, 63(2), pp. 129–138
- Strachan, H. (2005) 'The Lost Meaning of Strategy', *Survival*, 47:3, Autumn 2005, pp. 33–54
- Strachan, H. (2011) 'How is War directed? The Problem of Strategy' <https://www.youtube.com/watch?v=FHWyffZn5-c>, accessed 1st Sep. 2014
- Strachan, H. (2013) *The Direction of War*. Cambridge University Press
- Taleb, N. M. (2010) *The Black Swan*. Penguin
- (2012) *Antifragility*; Penguin
- Tesh, J. (2013) 'The National Risk Register's Value to Business and Communities', RUSI Analysis, https://www.rusi.org/analysis/commentary/ref:C51F254011BB92/#.U_dHAeX_1o, accessed 19th August 2014
- UK Cabinet Office (2008) 'The National Security Strategy of the United Kingdom, Security in an Interdependent world.', HMSO, London
- (2010) 'A Strong Britain in an Age of Uncertainty, The National Security Strategy of the United Kingdom', HMSO, London
- United States Department of Defence (2001), Quadrennial Defense Review Report, 30th September, Washington.
- (2006), Quadrennial Defense Review Report, 6th February, Washington

Education and the General: Educating Military Executives

RANDALL WAKELAM

“Hawke is a very good sea officer but no Minister” said Pitt on one occasion, when he thought that that distinguished Admiral was opposing a scheme designed to help the general situation in Europe in order to further another that could have only a local effect. (Doyle 1931)

Any officer who attains a certain standing is liable to be called into council, either with the Government at home, in the Dominions or in the colonies, with diplomatic or consular officers, British or foreign, and with business and shipping interests. In council, however, his views will carry no weight if it is found that he knows little beyond what he should do with his forces should he happen to meet the enemy. We want at all times, but particularly when at war, to ensure that the military view shall be given full attention, and an officer who shows that when formulating his opinions he has given the necessary consideration to all the various factors-political, economic, etc. is far more likely to get his ideas accepted than one who has obviously failed to give these matters due weight. (Slim 1947)

“What got you here won’t get you there.” (Jans, Mugford et al. 2013)

The conundrum of the general officer which Pitt commented over 250 years ago and Slim more recently is summed up neatly by the pithy observation from the Australian Defence Forces in our times. What they all say, fairly clearly, is that the warfighting capabilities of the officer, even at senior ranks, will not necessarily be the same competencies that he, and now she, needs to lead a Service, or the Services, in making good the security of the nation.

This article looks at the concepts and practices used in the ABCA nations for preparing their most senior officer cadre. It begins by defining concepts of education and identifying the competencies required of general officers. It then looks at the educational structures in place and suggests what might be changed, or kept, to make good on the ultimate goal of ensuring that senior leaders have the competencies to steer their services through the challenges of security and defence in the 21st century. Before continuing, it should be noted that we will not in most cases look at specific courses or programmes but more broadly at the sorts of learning and education that go on.

When civilians think of military education they may envisage a field of soldiers doing calisthenics early in the morning or firing earnestly at targets on the rifle range. A more modern version of this might see a pilot in a flight simulator or a team around a plotting display in a virtual ship's ops room. All of these activities tend towards training and so they qualify under the broad rubric of learning, but they do not capture the half of that latter concept. What they do reflect is the necessity for service personnel, both non-commissioned and commissioned, to be able to respond in a standard fashion to predicted circumstances — this is training. What they reflect less is the need for more senior personnel to develop and implement effective responses to unpredicted circumstances. This largely intellectual action requires more liberal education than it does training.

Before focussing uniquely on this aspect of learning, it would be useful to parse out a learning lexicon. Should one speak of education, training, learning, skills acquisition or something else? Does it really matter what terms are used so long as we can observe the preparation, cognitively, morally or practically, of personnel to allow them to discharge the functions of a military service? It is perhaps significant that when some of the terms discussed in the following paragraphs were presented in 2014 at a conference for historians of education some in the audience were not familiar with them. One might conclude that a common understanding of basic concepts must never be taken for granted.

In the *Concise Oxford Dictionary* (Soanes, Stevenson 2008) one finds the following three terms which are to some degree interrelated:

- to educate: to give intellectual, moral and social instruction;
- to train: to teach a skill or type of behaviour through regular practice or instruction.
- to learn: to gain knowledge of or skill in (something) through study or experience or being taught.

Recent pedagogical research (McNeir 1993, Manno 1994) links these actions with the concept of the 'learning outcome': what one expects the learner to be capable of at the completion of the learning activity. Generally, although not always, it should be possible to confirm the achievement of the learning outcome through some form of assessment. A slightly older construct, Bloom's Taxonomy of Learning, allows us to discern between cognitive, psycho-motor (physical skills) and affective (values and morals) capacities, which taken together seem to capture the range of capabilities and capacities which humans demonstrate. Assessment is somewhat easier to do when dealing with psycho-motor learning and somewhat, perhaps much, harder to do when looking at affective learning. (Bloom 1976, Anderson 2001) Indeed, how does one confirm that the learner has accepted and will employ, for example, a culture-sensitive approach when dealing with people from other nations, religions or cultures?

In further defining the context of this research we come to more recent ideas of 'learning organizations' and 'life long learning'. Learning organizations, as described by American researcher Peter Senge (Senge 2006), are evidenced by the presence of five characteristics.

The first of these is "personal mastery" which involves "personal growth and learning". It requires us to discern where we are and compare it to where we want to be. The difference between the two generates a "creative tension" which spurs us to

action. There are however, organizations which do not want personal mastery; their managers and leaders prefer their workers to simply remain stagnant intellectually. (2006, 131–2)

A second characteristic of learning organizations is the ability to challenge and where necessary transform or replace deeply held ‘mental models’; i.e. ways of doing business. Senge sees the requirement for openness when thinking about these models; do they work in changing circumstances or not? One of the biggest challenges is dealing with the reality that the mental model whether or not the hierarchy of the organization is open to change or is determined to control and direct. (2006, 171)

The third characteristic of the learning organization is the shared vision. Senge says that at its simplest it comes from answering the question “What do we want to create. . .” He says the belief or vision becomes “palpable” and that it “creates a sense of commonality that permeates the organization and gives coherence to diverse activities. Senge points to various corporations that experienced phenomenal growth, Apple for example, as manifesting shared vision. (2006, 192-3) He might well have looked at militaries in general, which on the face of them have an ethos and bond which unites members regardless of their function within the whole.

The fourth characteristic is what Senge calls team learning. About this he says: “Team learning is the process of aligning and developing the capacity of a team to create the results its members truly desire.” It builds on shared vision and personal mastery. (2006, 218) Team learning as three characteristics. First, the thinking and learning must be insightful. Next there must be “innovative and coordinated action” where trust exists between learners that the whole team is moving towards the same goals, but with some freedom of action. Finally, team learning may involve coordinated and sympathetic interaction with other teams. (2006, 219)

Pulling all these together, “. . . systems thinking is the fifth discipline. It is the discipline that integrates the disciplines, fusing them into a coherent body of theory and practice. It keeps them from being separate gimmicks or the latest organization change fads. Without a systemic orientation, there is no motivation to look at how the disciplines interrelate. . . . it continually reminds us that the whole can exceed the sum of its parts.” (2006, 11–2)

A second recent addition to learning lexicon is the idea of life long learning which is generally linked to rapid advances in knowledge and technology. In the *Oxford Handbook of Lifelong Learning* Manuel London (London 2011) argues that lifelong learning in the workplace can occur where the organization sets up a “learning environment” including policies, practices and activities to encourage learning. (2011, 5) In the same volume Paul Hager (Hager 2011) reviews the nuances of the term since its first use in the 1970s. Importantly for this paper, he points out that lifelong learning is not an individual activity, but that it can equally apply to organizations. (2011, 24)

If these concepts can be seen in the experience of society as a whole then are they also to be found in professional education and in military professional education and learning? Do they applying in preparing the general? And if so how? Before attempting to answer these questions we are best to define the key characteristics of a profession and professional learning.

In his work, *Professionalism: The Third Logic*, Eliot Freidson (Freidson 2001) argues that “professionalism” exists when “an organized occupation gains the power to determine who is qualified to perform a defined set of tasks, . . . and to control the criteria by which to evaluate performance.” (2001, 12) While all occupations

contain some blend of skills and knowledge, professions, he says, involve a “special kind of knowledge . . . believed to require the exercise of discretionary judgment and a grounding in abstract theory and concepts.” (2001, 13) All training, whether for craft, technical or professional work involves some degree of vocational training, but professions benefit from the broadening experience normally associated with a university milieu and approach to learning. (2001, 90) It is this liberal education that both enables specialist practitioners to later serve in managerial positions and also establishes a societally recognized legitimacy. (2001, 121) Moreover, a professional is better prepared by having a broad knowledge of theories which can be a “guide [to] discretionary judgment” rather than a narrow ability in only some of the practical applications of the profession. (2001, 95)

Professors Rod Gidney and Wyn Millar have found similar themes in the evolution of professional education in nineteenth century Canada. In their monograph *Professional Gentlemen* (1994) they explore the three traditional professions – divinity, medicine and law, concluding that technical proficiency had to be accompanied by a liberal education which remained “the touchstone of the educated man: it constituted a training in character and culture, the necessary prerequisite to framing technical expertise within ‘scientia’ . . .” (1994, 355) This scientia – knowledge – was thus a fundamental component of the individual’s formation, giving the professional the ability, in theory at least, to see the bigger picture while at the same time conferring a certain social status both on the individual and the profession.

While Friedson, Gidney, Millar and others do not discuss the military, there are researchers who do and who see it as a profession. Samuel Huntington’s *The Soldier and the State* (Huntington 1957) is a cornerstone of that thinking. In it he argued that twentieth century professional officers were much more than full time practitioners in that they met three essential criteria of professions: expertise, responsibility and corporateness. (1957, 8–10)

Huntington identified that while officers held a variety of qualifications (pilot, intelligence analyst, submariner, etc.) there was, however, a common underpinning that could be identified by the phrase, “the management of violence.” An officer’s associated duties included preparing the force, planning its missions, and directing its actions. An officer’s skill was neither “craft” nor “art”. “It is instead an extraordinarily complex intellectual skill requiring comprehensive study and training.” In Huntington’s view, acquiring this intellect required about one third of an officer’s career. Mastery came not simply through “learning existing techniques. [The management of violence] is in a continuous process of development, and it is necessary for the officer to understand this development and to be aware of its main tendencies and trends.” These statements surely suggest the requirement for life long learning. But even this was not enough, for Huntington posited that the officer must be in tune with the culture in which he operated. This required an understanding of society, of the characteristics of other professions and of human beings themselves. (1957, 11–14) More evidence, one can argue, of the place of scientia.

So it would seem that there is a ‘doctrine’, perhaps a /mental model, or at least a set of concepts that one can apply to military learning, but we also need to define who or what the general officer is and what specific skills and knowledge s/he might need before speculating on how these might be acquired.

In the 1939 Lees Knowles Lectures at Cambridge University the General Sir Archibald Wavell (Wavell 1941) focussed on three aspects of generalship: the general and his personal qualities; the general and his subordinates; and the general and

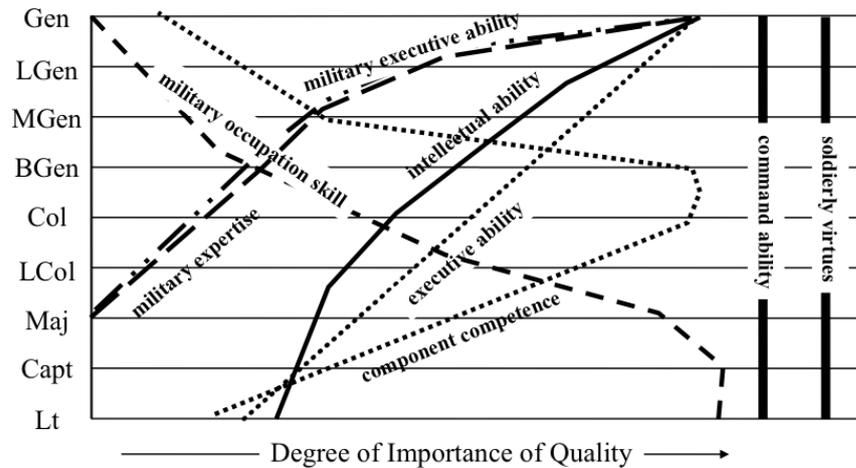
his political masters. Before discussing these relationships he quoted from Socrates who had said “the general must know how to get his men their rations and every other kind of stores needed for war.” Planning, energy and tactical knowledge were also critical to this Socratic model for success. (1941, 14–5) Wavell agreed that effective administration was the “real crux of generalship,” and went on to say that administering – providing for an army’s needs – was critically important. (1941, 15) Nonetheless, Wavell continued, generals also needed a range of personal attributes: mental and physical robustness, physical courage, health and youth, courage of convictions, knowledge of humanity and fighting spirit. (1941, 15–23) These things gave the general the strength of character to be effective when working with subordinates where it was necessary for him to “keep strict, though not necessarily stern discipline,” “give [ungrudging] praise where praise is due,” be visible to the troops, avoid sarcasm and keep the soldiers informed. (1941, 46–7) These things, he said, were hard to do given that generals were far less visible to their soldiers than in times past. Finally, and central to the present discussion, Wavell, reminded his audience of the problems of the Great War and how it was vital that the general and the politician worked in unique yet overlapping spheres and that cooperation was of vital importance for the successful conduct of the war. (1941, 57–62) All things considered Wavell painted the picture of a complex and demanding role where the general was required to exercise a mastery of a broad range of skills and knowledge, drawing on each as the situation demanded to ensure the success of the fighting troops.

If Wavell’s model, not to mention Slim’s and Pitt’s ideas, is still pertinent today the general needs both the competencies to administer within the organization and the savvy to deal with government, both politicians and high functionaries.

Before going further, however, it is worth reminding ourselves that generals are not, as is often the case with business executives, recruited from another organization, or even different types of businesses. Rather they normally advance within one national system and service so that by the time they reach the executive cadre they have a deep sense of the purpose and functioning of their service. Part of that advancement includes professional learning, both training and education, both appointment specific and general, and so we should be cognizant of this prior learning.

But not all prior learning will help in executing the functions of the general. A 1960s Canadian military study (Wakelam, Coombs 2010) of the then newly unified officer corps concluded that the importance of various sets of competencies and knowledge ebbed and flowed during a career. Technical and tactical expertise, what the study called “military occupation skill”, became relatively less important as an officer advanced in rank. Knowing how to conduct a fighting patrol would be of little utility to the general responsible for procurement or his/her counterpart working in international policy formulation. For those officers, knowing how the military fit within government, that is “military expertise”, was the focus of their competency. All of this and the supporting intellectual and personal values were captured in the diagram shown here: “Variation in Importance of Qualities with Rank”. (2010, 45) Executive ability it should be noted was “the ability to make decisions . . . and live with problems which defy solution”, a notion we attempt to capture today by referring to chaos, ambiguity and wicked problems.

The *Report of the Officer Development Board* concluded that to be constantly ready for new challenges as they progressed in rank meant that officers required continual education; the report suggested that 20 percent of a career should be devoted to professional learning activities, including where appropriate a civilian



graduate degree. (Wakelam 2004) This final statement was a bold one in an era when a high school diploma was often the norm for winning a commission. The military political security and military challenges of the last decade make the notion of problems which defy solution seem a commonplace. In 2014 we are witness to renewed East-West tensions and conflict in Ukraine, the Ebola crisis and instability in Iraq and Syria as a result of ISIS to name just three major concerns. How to deal with issues like these while also juggling shrinking resources are the daily stuff of a general’s diary.

To this point we have established that there is a doctrine of learning concepts, and that the military like other professions values knowledge as a vehicle to staying connected with and meeting the needs of parent societies. We have also seen that generals must be able to work with their operational forces, but that they must also work across government and society in dealing with incredible challenges. What sort of education or learning can possibly prepare these individuals for the most senior appointments? We now turn to four documents written in the ABCA nations, most quite recent, each of which attempts to lay out some general principles or intents for officer professional education either specifically for or including the executive cadre. Once we have looked at some key points we will perhaps be able to discern what an optimal learning experience looks like.

The earliest of the studies is the UK *Modernising Defence Training: Report of the Defence Training Review* completed in 2001 (Great Britain Ministry of Defence 2001) These are extracts from the document and its supporting essays:

There are three main stages in officer training: initial officer, command and staff, and senior officer training. Despite obvious gaps and exceptions, initial officer training and initial staff training probably correspond to the tactical level; Advanced staff training to the operational; and senior officer training to the strategic level. (2001, Supporting Essays, 9)

Training should reflect the different demands of each level of an officer’s career. The initial requirement is primarily to prepare an officer to operate at the tactical level and in a mainly single service environment, including all the required specialist skills. Thereafter we need progressively

to prepare officers for a wider and more senior range of appointments, which, at the operational and strategic levels are increasingly likely to be in the joint/multinational/inter-agency environment, in the integrated MOD HQ or its supporting defence businesses. (2001, Supporting Es-says, 9)

Most officers attend some form of Initial Officer Training and the great majority Initial Command and Staff Training; thereafter training becomes more selective. Officers will find themselves increasingly working in a joint environment. But joint expertise takes time to develop. Building on the changes already implemented in recent years, we propose a progressive increase throughout an officer’s career in exposure to joint as well as multinational, inter-agency and wider defence issues. This will begin with the introduction of short common modules during Initial Of-ficer Training, which will continue to be conducted in a predominantly single Service environment, given the importance of instilling individual Service ethos. Thereafter, while the focus of Initial Command and Staff training will similarly continue to be primarily single Service, we propose further common defence modules and an increase in joint activity, taking advantage of the collocation of staff training at the Joint Services Command and Staff College at Shrivenham. (2001, 15)

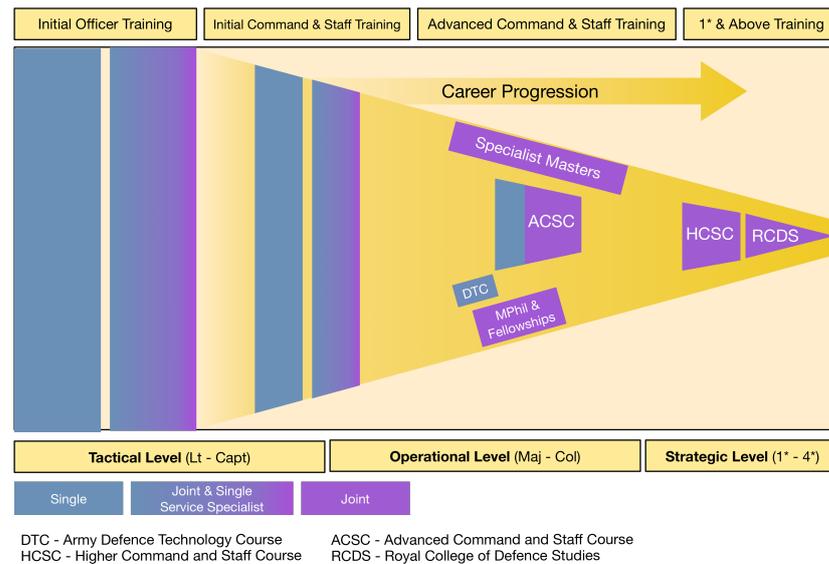


Figure 6.1: Recreated from *Modernising Defence Training: Report of the Defence Training Review* (2001)

There are gaps in training for senior officers ... in business leadership and management skills.(2001, 14)

... we will establish a small Defence Leadership Centre to design an overarching policy framework and strategies for managerial and leadership development. The centre will: provide a more focused and coherent

approach throughout an individual's career to leadership training, particularly for those likely to reach the corporate/strategic level... (2001, 24)

There is virtually no formal training in Joint Warfare for officer above 1-star at the operational level. We propose to meet the training requirements for commanders of joint and multinational operations through a mixture of very short modular courses, interactive gaming, and the development of a Joint Training for Operations Centre. ... Inter-agency training will be enhanced through the development of an annual politico-military game [replicating joined up government]. (2001, 16)

Overall it would seem that the concepts espoused at the time reflected the various levels of employment of officers and recognized the complexities awaiting those who would work in the highest offices. The range of courses and programmes available includes 'specialist masters' MPhils and fellowships in addition to the HCSC and the RCDS programmes. Unfortunately the DTR was only partially implemented. It could be said that conflicts in IRAQ and Afghanistan, as well as in other regions, took away the flexibility of MOD to provide these learning venues. But surely these operational demands and their strategic and political branches called for this very sort of learning.

Two reports were published in 2013. In the United States an independent think tank report Building Better Generals (Barno, Bensahel et al. 2013) stated:

The U.S. military needs an adaptive and creative officer corps in order to address the complex challenges of the 21st century — where the demands of managing an increasingly volatile international security environment and massive defense enterprise will rapidly collide with the realities of declining defense budgets and constrained U.S. global military capabilities. Yet 12 years at war in the unconventional conflicts of Iraq and Afghanistan have distorted the skills of the officer corps and much reduced the time that has been available for professional military education and broadening assignments. Additionally, over a decade of irregular warfare may poorly prepare officers for what lies ahead. For this reason, the United States must redouble efforts to strengthen its current and future military leaders, starting with its corps of generals and admirals, and extending to all those rising to fill these positions. These officers will be responsible for leading a smaller, more austere force charged with fulfilling the nation's global security responsibilities. Improving flag officer assignment, education, selection and evaluation is a wise and necessary investment to ensure the nation maintains the senior leadership capable of preventing, and if necessary, winning the next war.

Several initiatives would significantly improve flag officer development and accountability in the years ahead. Tomorrow's flag officers would benefit from an assignment system that tracks them into one of two specialties: warfighting ("operational") and institutional ("enterprise") billets. Coding all two-, three- and four-star billets as either operational or enterprise, and assigning flag officers selected for two-star rank to one of these tracks, would enable officers to optimize their development and education for the responsibilities of their assignment. Flag officers will also

need robust, tailored education to support their assigned track. Officers on the operational track should attend a new U.S. Higher Command and Staff Course that emphasizes strategic and political-military skills; enterprise officers should attend business schools and corporate and executive leadership programs, supplemented by military-specific courses.

Finally, officers will need a selection and evaluation process that establishes clear expectations for performance and enhances accountability throughout their careers, particularly at the three- and four-star level. This process should include performance reviews and written evaluations for all officers, which will additionally promote mentorship and continuous self development. Today, this system abruptly stops when an officer is promoted to three-star rank. (2013, 5–6)

This last paragraph contains a significant point: education is for specific people and the profession must identify those people who have ‘the legs’ and the brains to operate effectively at the highest levels. But readers will see that the entire system proposed by the study would demand a great deal of foresight to pick the right people, this followed by highly focused and individualized education for those identified.

Also in 2013, Australia reviewed its senior officer learning strategy. The following are extracts from *The Chiefs A Study of Strategic Leadership* (Jans, Mugford et al. 2013)

The report reaches three major conclusions, relating respectively to individual development, organisational development and leadership style. These conclusions are that:

- for the ambitious officer, “what got you here won’t get you there”;
- for the military institution, “what got us here won’t get us there”;
- and
- the principle that “leadership is a team sport” is just as valid at the senior level as it is lower in the organisation. (2013, 111)

It is recommended that:

- the core JPME effort (or at least that from mid-career onwards) be oriented around the four strategic leadership roles of Strategic Leader, Strategic Builder, Strategic Director and Steward of the Profession.
- such JPME be focused on preparing officers for future roles in both leadership and support for senior leaders.
- officers from mid-career onwards periodically be exposed to and engage with contemporary and evolving issues at the strategic level, with exercises that require them to examine the responsibilities and skills needed for the Director-Leader-Manager-Steward forms within their own current and immediate-future career roles. (For example, as part of preparation for ship/unit command, O4 and O5 could examine the application of these four roles to that level of command and the level of command immediately above it.)

- such engagement use active rather than passive modes of learner behaviour.
- each Service continue with the current encouraging trend of introducing career models that enable selected officers to develop in-depth specialisations within relevant fields – not just within “personnel management” and “project management/technology” but also within economics, politics and military sociology. (2013, 113)

Notions of ‘got here... get there’ seem awfully like personal mastery and perhaps mental models. There are striking similarities with Senge’s model throughout the Australian document. There are also striking similarities with the recommendations of the US study’s recommendation to group officers either for operations or enterprise assignments. Perhaps most centrally we can see the wisdom of Wavell and Slim in the recognition that strategic leadership is not the same as operational and tactical acumen.

A third document from 2013 captures the main themes from a pan NATO conference on military education and learning. Extracts from the report of “Connected Forces, Educated Minds: Transformation and Professional Military Education” follow. (Wilton Park 2013) From the conference report:

The aim of this two day conference is to help lead the way towards a new NATO Standard for professional military education (PME). Specifically, the conference will consider PME in the light of the lessons learned from over a decade of Alliance-led operations and how best the corporate memory gained can be captured before becoming lost so that PME takes its rightful place as part of enhanced training, exercising and education in the creation of NATO Forces 2020. (2013, 3)

Education will vary according to level and capability and be tailored to support careers that specialise in many security domains. For example, at the mid-level education will produce “brilliant mechanics”, whereas at the higher-level it will reinforce “strategic level intuition”. The PME system must be agile enough to recognise early and support “the likes of a Petraeus or Stavridis” as well as more modest mortals. Critically, central to PME will be a tailored, career-long learning relationship that can identify early talent and foster an elite of officer-scholars, some of whom are sent off for a time into the civilian education sector with no suggestion that their careers will be blighted as a result. (2013, 1)

On a related blog site principal conference contributor Julian Lindley French wrote:

To my mind education, the knowledge it is built upon and the connectivity it breeds is the missing link between NATO nations that will help the Alliance close the strategy-austerity-capability gap.

NATO 2020 pre-supposes defence modernisation at a time of acute defence austerity. NATO have created both Smart Defence and the Connected Forces Initiative both of which further pre-suppose much greater synergies between capabilities and capacities. Today, value for money in defence strategy is as much about ‘human software’ as hard capability.

Therefore, critical to NATO 2020 must be a model of professional military education that aims to promote comparative advantage of NATO personnel both on and off the battlefield. In other words, NATO must become as much knowledge nexus as military nexus. (Lindley–French 2013)

The report talks more about the career process perhaps, but the Lindley French comments illuminate the central value of education in giving senior leaders the advantage they need to provide security and defence effectively when the problems seem never to abate.

In Canada a review of the entire officer development system is currently under way, but details are not available. At this time the Canadian Forces College offers the National Security Program (NSP) for officers of the colonel/naval captain and civilian equivalent; it is designed to prepare leaders to operate at the strategic level. All students take the same curriculum, those taking an extra course in economics are able to complete a Masters in Public Administration. Courses focus on national security policy and instruments of national power as well as the workings of government. There is one course dealing with operations but here the context is set at a very broad level and deals more with defence and security policy than the conduct of operations. Several ‘wargames’ and simulations are used with facilitators drawn from active and retired government executives and former politicians. The intent is to replicate the complexity and chaos of political decisions.¹

The genesis of the NSP was the result of meeting between the CDS and the Commander of the Canadian Defence Academy in 2007 at which the author was present. In addition to establishing the NSP, the CDS and his Vice Chief felt that there was a need for graduate education and fellowships for selected officers. Their intent was to create the necessary tailored learning to generate a pool of one and two star officers with the knowledge and intellectual skills to replace them. Follow-on work led to a study by a retired commander of the army in which it was noted that roughly 70 percent of Canadian general officer positions were not in operations, but rather in institutional leadership and management in areas such as personnel or defence policy, procurement and finance — those ‘enterprise’ billets in the US and UK studies. His conclusion was that to be effective in these sorts of functions the general needed to have served in lower level appointments within these specialized areas, normally at the major/ lieutenant colonel rank. Other recommendations included a mentoring programme for all general officers, particularly for those moving into the national headquarters and having to work across government for perhaps the first time.

The Canadian experience like those of the other ABCA nations is founded on identifying those with the potential to go on to the most senior ranks, and then giving them the experience and learning opportunities necessary to do just that.

While earlier it was stated that the paper would not look at specific courses and programmes the review of the NSP above has opened the door to such an examination. But for the purposes of this paper it is sufficient to say that each of the ABCA nations has its own programme or programmes which, over the span of about 10 months, expose selected senior officers to the range of issues they will face when working at the strategic and even political levels of government. To these are

¹The syllabus of the program is available on line at <http://www.cfc.forces.gc.ca/119/187/312/331-eng.pdf>

added, or at least envisaged, additional ‘bespoke’ learning events from short courses to graduate degrees, intended to provide that extra something to actually catalyze the officer’s potential.

We are left with the question: Are these programmes enough? If nations stick with their existing in-house programmes then arguably not. Selection for one a year of learning assumes that the officer has both the intellect to learn and advance as well as the intrinsic desire to learn. If however there is a streak of hubris in that individual, or if she or he accepts a year of schooling simply because it seems the right thing to do for career advancement, then the learning experience and the further service may not be equal to the investment.

Moreover, while we as professionals race about attempting to deal with the wicked problems we tend to lose sight of the fact that we need to be on top of our game. Would we, for example, want to visit a physician who eschewed learning and using the latest diagnostic practices in keeping us healthy? Why then would anyone want to put trust in the general would only grudgingly accept a learning billet or who ignored professional self development being too busy with operations?

Finally, can we say that war and defence college programmes are ‘the answer’ to preparing the general. As good as they may be they are generally limited in allowing the student to be curious and to risk adventuring into unknown issues. And yet this adventuring and risk taking are exactly what the operating environment of the most senior leaders often looks like. Just perhaps, we need to consider the use of civilian graduate programmes and fellowships – where students can be put in ‘unmoderated contact with knowledge’, where there is no school solution and no rules of engagement about where the discussion can go – as closer to the norm, and this perhaps in addition to the war or defence college. We need to invest in the next generations of executive leaders; the return on that investment could be well worth the effort.

Acknowledgements

This paper was prepared with support from Defence Research and Development Canada and from the Changing Character of War Programme at Oxford University. The author wishes in particular to thank the Visiting Fellows of 2014/5 for their input and comments.

References

- Anderson, L. W., ed (2001) *A Taxonomy for Learning, Teaching, and Assessing: a Revision of Bloom’s Taxonomy of Educational Objectives*. Complete ed. edn.. Longman
- Barno, D., Bensahal, N., Kidder, K. and Sayler, K. (2013) *Building Better Generals* (Washington D.C.: Center for a New American Security)
- Bloom, B. S. (1976) *Human Characteristics and School Learning*. McGraw–Hill
- Doyle, W.H.D. (1931) ‘The Higher Study of War in the Services’, *Royal United Services Institution Journal*, 76(502), pp. 356–376
- Freidson, E. (2001) *Professionalism: the third logic* (Cambridge: Polity)
- Gidney, R. and Millar, W. (1994) *Professional Gentlemen: The Professions in Nineteenth-Century Ontario* (Toronto: University of Toronto Press)

- Great Britain Ministry of Defence (2001) *Modernising Defence Training : Report of the Defence Training Review* (London: Ministry of Defence)
- Hager, P.J. (2011) 'Concepts and Definitions of Lifelong Learning' in M. London (ed) *The Oxford Handbook of Lifelong Learning* Oxford University Press, pp. 12–25
- Huntingdon, S.P. (1957) *The Soldier and the State: the Theory and Politics of Civil-Military Relations*. Belknap Press of Harvard University Press
- Jans, N., Mugford, S., Cullens, J. and Frazer–Jans, J. (2013) *The Chiefs: A Study of Strategic Leadership*. Australian Defence College
- Lindley–French, J. (2013) *Connecting NATO Forces... And Minds*
- London, M. (2011) 'Lifelong Learning: Introduction' in M. London (ed) *The Oxford Handbook of Lifelong Learning* Oxford University Press
- Manno, B.V. (1994) *Outcome-Based Education: has it become more affliction than cure?*. Center of the American Experiment
- McNeir, G. (1993) *Outcomes-Based Education: Tool for Restructuring*. Oregon School Study Council
- Senge, P.M. (2006) *The Fifth Discipline: the Art and Practice of the Learning Organization*. Rev. and updated edn. Random House Business Books)
- Slim, W. (1947) 'Higher Training for Combined Command' *Royal United Services Institution Journal*, 92(568), pp. 507–516.
- Soanes, C. and Stevenson, A., eds (2008) *Concise Oxford English Dictionary*. Eleventh Edition, revised edn. Oxford University Press
- Wakelam, R. (2004) 'Officer Professional Education in the Canadian Forces and the Rowley Report, 1969', *Historical Studies in Education/Revue d'histoire de l'éducation*, 16(2), pp. 287–314.
- Wakelam, R. and Coombs, H.G., eds (2010) *The Report of the Officer Development Board: Maj-Gen Roger Rowley and the Education of the Canadian Forces*. Wilfrid Laurier University Press
- Wavell, A.J. (1941) *Generals and Generalship: the Lees Knowles Lectures delivered at Trinity College, Cambridge in 1939*. Penguin Books
- Wilton Park (2013) *Connected Forces, Educated Minds: Transformation and Professional Military Education (WP1225)*. Wilton Park

Space Security and Strategic Stability

JING ZHONG

Translation assisted by Dr Robert Johnson

In recent US-led wars, space power invariably played a very important role. Space power, a core component of war fighting capability, enabled coalition forces to integrate all their assets into a joint operations concept in the true sense of the term. Today, the United States considers space as its strategic ‘highlight’ and the most significant interest in the information era, not least as part of its missile defense project. It is against this backdrop, that this article seeks to depict the new emerging challenges of space security and analyze their impact on future global strategic stability and arms control.

Over the past half-century, mankind has taken great strides in space exploitation and achieved considerable progress. As a result, human society and space are becoming increasingly inseparable. However, the situation in terms of space security is not one that generates much optimism. Although there are no weapons deployed in space today, it is undeniable that situation is serious and the trend in the weaponization of space is conspicuous.

Recent changes in the security of space stem mainly from current international relations, developments in global economics, and the related scientific-technological environment. The end of the Cold War and the collapse of the Soviet Union left the United States as the only superpower and it has displayed increasing strength and ambition in space. Meanwhile, as a new territory for human exploration and the last frontier for human existence, space is regarded both as a reflection of a country’s technological prowess and as a key to its future economic development. In addition, since the most obvious characteristic of high technology in the information era is its rapid diffusion, it is impossible for any country or organization to monopolize space technology for long. In the early twenty-first century, more countries are looking to enter space. Until now, eleven countries have a space launch capability and over sixty countries own and operate approximately 1100 active satellites. Against this backdrop, many observers and analysts have claimed that an era of space competition has arrived.

Emerging challenges to space security

Those wishing to ensure space security are confronted with unprecedented challenges that are different from those of the past. If these are neglected and mishandled, the resulting fallout could lead to acute vulnerabilities, and even to conflicts.

Four major future challenges have emerged, which will be discussed in detail below. First, the space policy and doctrine of some space-faring countries which focus on space deterrence and the military use of this domain are possibly creating a serious risk of reigniting a new round of great power competition thereby generating new vulnerabilities. At present, the most important factor resulting in instability in space is American policy. Although the latest U.S. National Space Policy (NSP), released in October of 2010, has obviously shifted away from the Bush administration's emphasis on the military freedom of action in space, over all other requirements, to a multi-layered approach to ensure space security, the U.S. still emphasizes deterrence with a clear ambition to monopolize space. Space deterrence reminds us of the Cold War. It is established on basis of confrontation with a perceived enemy. The U.S. space deterrence idea has clearly upset other countries. It stresses that deterrence of hostile acts in space, as with nuclear deterrence, rests on secure retaliatory capabilities sufficient to deny advantages to an attacker, as well as effective command and control mechanisms (Krepon 2014). To achieve space deterrence, the U.S. puts forward a multi-layered strategy that can help deter hostile actions against American space capabilities. It includes the ability to respond appropriately to attacks on American space assets, greater resilience and redundancy, better space situational awareness, improved command, control, and intelligence capabilities, and sound diplomatic initiatives (Krepon 2014).

Under the guidance of space deterrence, the United States is vigorously pushing its missile defense system. It is a *de facto* step that will lead inevitably to space weaponization. The U.S. military holds the notion that its missile defense system is a purely defensive weapon system. However, it may not be. On the one hand, any defensive technology can easily be changed into offensive one or used in offensive operations, not least because the border between offensive technology and defensive technology is blurring. As we all know, it is very easy for anti-missile technology to be used for anti-satellite purposes. That said, not all missile defense systems have latent ASAT capabilities. Missile defense systems are generally categorized into three types based on which phase of ballistic missile flight they target: namely their boost phase, terminal phase and midcourse missile defense phase. As one U.S. scholar pointed out these midcourse missile defense systems are very similar in capability to ASAT functions as they are designed to target objects moving through space in the same altitude regime as LEO satellites (Weeden 2014). What's particularly noteworthy is that there is no meaningful difference between midcourse ballistic missile defense and 'hit-to-kill' ASAT capabilities. Midcourse ballistic missile systems are intended to destroy warheads travelling at speeds and altitudes comparable to those of satellites; typically the only difference between the two systems is the software and control algorithms used to detect, track, and home in on a satellite compared with a warhead (Weeden 2014). In fact, midcourse ballistic missile systems are likely to be more complex than that of an ASAT weapon since most satellites are easier to detect, track, and target than warheads with often a penetrating capability moving through the earth's upper atmosphere and subject to a range of interfering factors. On the other hand, if a country's defensive capability against missiles increases, then its

offensive capability with its own missiles will be accordingly raised to a new level. This will inevitably undermine strategy stability. When the U.S. deployed the base elements of an anti-missile system in Poland and the Czech Republic, it provoked corresponding reactions from Russia, including demands that it move from a global approach back to a regional one. Some experts have deduced that the U.S. could test capabilities for space weapons via missile defense tests. The Bush administration's proposal for missile defense therefore went a long way towards preparing for the deployment of space-based weapons.

Japan is another case example where enhancing the potential military dimension of current and future use of space. Many space programs have obvious military purposes. Japan's four IGS systems (two satellites have optical sensors and two others have imaging radar capabilities), which make it possible to gathering information by scouting any point on the Earth at least once every day, were completed in 2007, and its new-generation IGS were scheduled to be launched between 2009 and 2014 (Sawako 2009). Furthermore, Japan was keen on participating in the U.S. MD program from 2003 and made efforts to expand further its technological cooperation of MD. The MD system is a major step toward Japan's militarization of space. Even more worrisome, in 2008, Japan enacted the basic space law, ending a several-decades-long decree against the development of military space capabilities and instead permitted the development of non-offensive military space capabilities. The new space law further lifted the ban on the use of space technology for military purposes. In particular, the revision raised a serious conflict with the second paragraph of Article 9 of the Japanese Constitution, which declares that 'land, sea, and air forces, as well as other war potential will never be maintained'. Some experts are worried about this tendency and have a sense that 'It is not just in terms of Japan's position on the legitimate uses of outer space, but also in terms of its potential broader 'remilitarization' (Hughes 2009). As a result of the approval of the Basic Law on Space, Japan's space budget is weighted even more heavily toward military purposes and inevitably will lead to the integration and reframing of its space industry.

U.S. space defence and Japan's move toward a more militarily-oriented policy will have a far-reaching impact on other countries. Faced with the United States' policy of seeking absolute security and a monopoly over the use of space at the expense of the security of all other countries, it is almost certain that other countries will make corresponding plans to counter the ascendant U.S. monopoly of power in space. It is reported that Russia, the European Union, China, India and other space-faring powers have major plans for space exploration. Therefore, the U.S. desire for monopoly is triggering a new round of competition in space. As Kenneth N. Waltz has argued, the aspiration for dominance, coupled with the immoderate behaviour of one country, causes others to look for ways to protect their interests (Sagan and Waltz 2003, 149). Many examples in history illustrate how uncontrolled competition in developing advanced technology can lead to escalation and generate action-reaction escalation. Space competition could become a case in point.

Second, with the rapid development of space technology, space power has become closely linked with land power. It has become the most important component of the future integrated battlefield. Since the end of the Cold War, four major military conflicts have taken place, all of which could be characterized as high-tech wars, namely the Gulf War in 1991, the Kosovo War in 1999, the Afghanistan War in 2001, and the Iraq War in 2003. In all of these wars, space power had played a very

important role. Furthermore, its significance is increasing with each new war, given rise to the rapid development of space technology.

Space capabilities were integrated into operations at all levels in the Iraq war and represent an indispensable component of the warfighting package of the United States. Because of the progress of integrated operations, the combat effectiveness of American formations were increased significantly. For example, U.S. military forces required more than two days to detect and then attack a Scud missile in the first Gulf War, a relatively slow operational process called observe–orient–decide–act (OODA) loop. In the Kosovo War, the time for this OODA process was reduced to 1–2 hours. In the war in Afghanistan, it was further reduced to only 19 minutes. In the Iraq War, the time was again shortened to no less than 10 minutes. According to a report from *USA Today*, it will take only 7 seconds to finish this cycle in a future war since the attacking missile will be able to acquire and adjust the information from the data link even during its flight course. It is therefore inevitable that there will be an increasing demand for, and reliance upon, space–based force enhancement capability.

According to an estimate from a war–game simulation, it is believed that combat effectiveness can increase at least 50 to 100% with the application of space power. One U.S. military expert even commented that if space war was only an infant in the first Gulf War, then it now is growing up at light speed. In the Iraq War, for the first time, space power enabled the coalition forces to integrate all their assets into joint operations to such an extent that many observers thought that the Iraq War was indeed the first real Space War in human history. Space warfare, as a new pattern of future war, is divided into two phases by this U.S. expert: the first phase of Space War features a compact linkage between space and earth operations. The establishment of new concepts of space operations, space weapons, and space forces will be the indicators of the second phase of space warfare.

According to these theories and given the benefits of space power in recent wars, the United States has taken great pains to adopt a policy of developing space technologies to enhance and integrate its military power. Based on the understanding that the center of gravity of the future battlefield is an effective system of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), the most critical part of which are all kinds of satellites, the U.S. military is trying hard to establish an integrated battlefield, by further engaging space power into global military deployments at every level: from strategy to tactics. Since the effective use of space assets has become a determinative factor in wars, it has now become highly likely that satellites and other space assets could become targets subject to attack or deception during a major conflict. Even primarily civilian satellites will likely be attacked, as they play a significant supplementary and substitute role for military satellites. Thus, due to an integrated battlefield and the strategic significance of space assets, space conflict will almost certainly lead to escalation of such wars.

From a long–term perspective, with a tighter linkage between space and earth in the future, the possibility of space conflict among the great powers will increase if there are no effective measures to prevent it. Even an accident or misjudgment in space could possibly escalate into a conflict.

The third point, linked to the previous one, is that space weapons might be hidden in civil space assets, given the dual–use nature of space technology. At present, the borderline between emerging military and civilian technologies is becoming increasingly blurred. This fuzziness is reflected not only in the overlap of key technologies

in the military and civilian fields, but also in the synergy of future development trends for key technologies. It is sometimes difficult to tell the difference between military and civil uses in space technology. For example, Japan's use of solid propellant in certain rocket boosters is puzzling. The development and production costs for such fuel, as well as launch expenses, are so high that they are hard to justify on commercial grounds. However, solid boosters may be used in ICBMs. It has also been reported that the American X-37B has the potential capability of attacking and destroying hostile satellites. Therefore, many civil space items have shadows of military purposes. As Joan Johnson-Freese has pointed out, there is no distinction between space technology for civil or military use, since 95% of space technology is dual-use. How to regulate space items to both ensure equal rights to peaceful uses of space while guaranteeing that no military intentions are involved has become a real challenge.

The fourth point is that, with space power overlapping with cyber power and nuclear power, it will almost increase possibility that space power will be dragged into future conflict. With the development of integrated systems, the borderline between different technologies is being increasingly blurred. This development tendency of the high-tech sector will lead to the overlap and penetration of different domains. Firstly, the field of space and nuclear missiles are becoming more closely entwined. The command and control systems of nuclear missiles require satellites in outer space. The intertwining of space and nuclear weapons is inevitably stronger with an increased dependency on space-based assets for all operational activities. Meanwhile, full-scale missile defense systems (using space assets) will undermine the existing strategic deterrence capability of nuclear missiles. Secondly, cyber power has illustrated incredible synchronisation with space power due to its ability to penetrate and enabling a range of other operations. Cyber power and space power are both generally considered an enabler and penetrator of other domains, and could integrate with the other domains to the point that all these domains are dependent on them. There are two phenomena that display such tendencies of tighter synchronization between space power and cyber power. One phenomenon is that Global Information Grid (GIG) as the basis of cyber operations, whose main component is the transfer of operations from land to space. The other phenomenon is that future satellites are being allocated of IP addresses and operated by a universal network. As a result, the linkage between nuclear missile C2 and cyber power is obviously increasing. As we all know, cyber power has penetrated into all aspects of human society in the information era. Consequently, even a small incident or misjudgment occurring in any domain will possibly lead to a series of reactions in other domains. This must evoke the strong possibility, if not inevitability of space power being dragged into future conflict.

Implications of space weaponization on strategic stability and arms control mechanisms

Faced with these serious challenges, it is undeniable that the situation for space has become serious in recent years. Space weaponization will surely have deep implication for strategic stability due to its strategic nature not least as a countermeasure against nuclear weapons. Moreover, it will almost certainly change the arms control regime in the future.

Firstly, space weaponization will possibly lead to a power unbalance. Strategic

stability in essence refers to the notion of a balance of power among the leading nations, and a sustained stability through certain international mechanisms. Strategic stability can also be defined therefore as an enduring situation, in which various strategic forces in the world are able to establish and sustain a framework for the fundamental relations with each other, giving them, in turn, an adequate sense of security. Strategic stability thus is closely related to the existing world order, through established international mechanisms and norms of behavior in international relations.

During the Cold War, the nuclear weapon was the pillar of strategic stability. The nuclear balance between the United States and the Soviet Union became the central theme for that stability. The equilibrium of MAD (Mutually Assured Destruction) was believed to be effective in preventing nuclear war as neither side would not dare launch a preventive nuclear strike lest the attack would lead to the automatic retaliation by the other side and bring about a guaranteed self-destruction. MAD thus was not only a practice, but also the basis of a theory, which constituted the conceptual basis for the strategy of deterrence that both these two Superpowers were believed to embrace. According to deterrence strategy, the focus was on the prevention rather than the actual fighting of a nuclear war. Thus, a nuclear balance was achieved in terms of the identical nuclear doctrine as well as the nuclear force structure between the two Superpowers. And it was based on this nuclear balance that strategic stability was ultimately established. It was indeed a balance of terror, codified by the ABM Treaty and other related nuclear agreements.

At the same time, strategic stability went beyond the manipulation by the two superpowers even in the Cold War years. With the development of the world campaign for peace, nuclear disarmament and nonproliferation, tension between the nuclear weapons states (NWS) and non-nuclear weapons states (NNWS) increased. This situation had led the conclusion of a number of important multilateral treaties like the Partial Test Ban Treaty (PTBT) in 1963 and the Nonproliferation Treaty (NPT) in 1967. Strategic stability in the Cold War years was therefore further consolidated as it became institutionalized through the gradual establishment of a series of arms control and disarmament agreements, and regional security arrangements both at bilateral and multilateral levels.

Yet nuclear weapons, as a core of strategic stability during the Cold War, was challenged with the development of a revolution in military affairs (RMA) and new types of strategic technology such as space power and cyber power. In particular, with the development of space power and its extensive use in military operations, space power has become a significant component of strategic power. Compared to the ordinary conventional weapon, the use of a space weapon, projected onto the surface of the earth, would have unimaginable shock effects on the populace and lead to the escalation of a war due to the inevitable reaction from an adversary. Although a space weapon could not perhaps cause the massive damage of a nuclear weapon, it would become even more important than nuclear weapons in the future frame of global strategic stability because of its special effects on a country's politics, economics and security. We might also anticipate an amazingly rapid development by different nations.

Space weaponization could therefore have grave and perhaps unknown negative implications for the world strategic stability and arms control mechanisms. On one hand, space weaponization would undermine strategic stability. Full-scale missile defense, as one step of space weaponization, will lead to the nuclear unbalance due

to its counteraction to nuclear weapons. This is a typical case where the search for absolute security at the expense of the stability can affect the whole world. As a result, space weaponization will perhaps further stimulate the horizontal and vertical proliferation of nuclear and conventional missiles.

Furthermore, space weaponization would destroy arms control and disarmament mechanisms. As noted above, strategic stability in the Cold War years was consolidated with a series of arms control and disarmament treaties. These legal documents reflected the convergence of interests of the majority members of the world, as well as their willingness to accept certain constraints on their own actions in the international arena. However, space weaponization will completely overturn all these efforts by the international community. An un-limited missile defense system (via space) will undermine the nuclear balance, the very basis of these arms control treaties. It will thus block directly the progress towards nuclear disarmament and that will surely spread to related field of nuclear nonproliferation. Of course, some hold different views on this issue. In the 2011 London Summit known as 'Global nuclear zero', the 'Global nuclear zero initiative' was committed to support to development of the proposed Missile Defense cooperatively. Ultimately, it was seen as a benefit for strategic stability by advancing the case for 'nuclear zero'. However, as far as I am concerned, future cooperative development of full-scale MD will create ambiguity because of the sharing of sensitive technology and the absence of trust amongst those outside the MD system. Meanwhile, as long as full-scale MD exists, it is difficult to continue to cut nuclear weapons. Therefore, full-scale MD will directly and seriously impede disarmament. Space weaponization will be a huge challenge to a series of arms control and disarmament agreements.

A second point is that, with space deterrence overlapping with nuclear deterrence and cyber deterrence, it will make the institution of strategy stability more complicated. This will require the reframing of the architecture of arms control entirely. Nuclear deterrence was supposedly critical for strategic stability due to perceptions that if not deterred, an opponent will attack. For nuclear deterrence to be successful it relied mainly on the size of the nuclear arsenal. It was only with sufficient scale that states would moderate their aggression and accept political stability.

Space deterrence is depicted by the Pentagon planners of the United States as 'control of space' in order to 'conduct defensive and offensive counter-space operations as directed to protect space and terrestrial forces'. Its core can be categorized in three categories: deterrence by denying benefit to an adversary; deterrence by cost imposition; and deterrence by inducing an adversary action. Space deterrence is more complex than nuclear deterrence because of the rapid development of space technology and the vulnerability of space environment. As Michael Krepon argued: 'successful space deterrence depends on a multi-layered approach which includes the ability to respond appropriately to attacks on US space assets, greater resilience and redundancy, better space situational awareness, improved command, control, and intelligence capabilities, and sound diplomatic initiatives.' (Krepon 2014)

Cyber deterrence has instinctive characteristics different from nuclear deterrence and space deterrence. First, cyber deterrence has strong operational potential. The United States has attempted to develop cyber deterrence as a strategic instrument since 1990 (Stevens 2012). In recent years, there has been a series of published works, such as 'International Strategy for Cyberspace' in May 2011, 'Department of defense cyberspace policy report' in December 2011 and 'sustaining the U.S. global leadership: priorities for 21st century defense' in Jan 2012, and each have proposed

‘positive defense’ as the strategy of cyberspace security on the basis of deterrence. And the U.S. military will further launch a new type of cyber deterrence strategy on the basis of combining ‘integrated operation of strategy deterrence’ with a ‘new trinity strategy deterrence’. Under the guidance of the cyber deterrence concept, the U.S. Department of Defense (DOD) treats cyberspace as an operational domain where it will organize, train, and equip troops so that it can take full advantage of cyberspace’s potential. Accompanying the creation of its cyberspace command system, there have been a host of new U.S. initiatives and cyber deterrence doctrines clearly targeting state actors, including leaving open the option for escalation to traditional military means in the physical realm if the U.S. ever felt it suffered too dearly in the cyber realm.

Cyber deterrence could be understood as a form of complex deterrence. As Knopt argues, cyber deterrence may only be ‘partially effective’ and ‘less than ideal’, but it is better than no deterrence at all; the important consideration is ‘whether deterrence can make positive contribution at the margins (Knopt 2010)’. Tim Stevens also thought cyberspace forms one of a suite of ‘complex deterrence measure in a post-cold war world, whose outcomes and objectives are less absolute and more pragmatic than those of preceding era of nuclear bipolarity.’ (Stevens 2012) Successful cyber deterrence depends on not only cyber weapon but also the development of regulatory norms for the use of cyberspace, which can lead to a form of soft-power deterrence (Stone 2012).

As space power overlaps with cyber power and nuclear power, it is almost certain that space deterrence will affect deeply both nuclear deterrence and cyber deterrence. The development of full-scale missile defense will counteract nuclear deterrence. The main component of missile defense lies in space and missile defense rely heavily on a space awareness capability. For this reason, NATO leaders have agreed on how to establish better space awareness and, more importantly, space situational understanding through the establishment of a missile defense system that covers all eventualities (Hansson 2011). On the other hand, space deterrence overlaps cyber deterrence. To achieve successful space deterrence relies on not only countermeasures against attacks on US space assets but also a better space situational awareness capability and advanced command, control, and intelligence network, and that is closely linked with cyberspace. Furthermore, cyber deterrence depends mainly on the basic infrastructure of cyberspace, whose critical components have been deployed in space.

With the background of this complex mixture of nuclear, cyber and space deterrence, what is its implication on strategic stability and how we should reframe strategic stability? In the Cold War, nuclear power was the only pole of strategic stability. With the development and extensive uses of space technology and cyberspace technology, there will be multipolarity in future strategic stability. Although space power and cyber power cannot yet be considered to be new poles of strategic stability, current strategic stability is already de facto a complex posture that is based on nuclear deterrence against the background of space deterrence and cyber deterrence. Taking a long term perspective, future strategic stability will be evenly balanced on three poles — nuclear power, space power and cyber power and form a new type of integrated deterrence. This will be the result of the three kinds of strategic powers and the further rapid development of space and cyber technology. The establishment of future strategy stability that relies on this new integrated deterrence will certainly readjust the world balance, and change norms of behavior in international relations.

What is particularly noteworthy here is that the interpenetration of the strategy of deterrence in different domains will have a profound impact on future arms control mechanisms. In general, the articles and codes of the arms control treaties are designed to regulate the behaviors of one special domain. For example, the design of the nuclear nonproliferation treaty only focuses on nuclear weapons and there is little consideration of other related domains. Moreover, the conceived notions of the space codes of conduct is only focused on the space domain and has less linkage with cyber and nuclear issues. However, it is my concern that the whole arms control system has some significant loopholes and inherent flaws. It is difficult for these treaties to be effective even where they have been ratified without much difficulty in the past. With the interdependent nature of different strategic domains, it is now necessary to design a comprehensive framework of future arms control mechanisms from holistic perspective rather than from narrow approach to each domain in isolation.

Approaches to Space Security

Space security is at a crucial crossroads. How is one to protect space security in the future? The international community should take effective measures to contain the tendency toward the weaponization of space and divert space activities onto the right track of peaceful uses in order to serve all humankind.

The solution must be to establish a new security concept. This is a key point for ensuring space security. We should learn lessons from the nuclear era. Seeking a monopoly of weapons superiority and absolute security is mad and unwise. If we keep the old model of conceiving of a rival as the main enemy, progress in space will be a zero-sum game in which any advance made by either side is harmful to the security of the other. Therefore, it is important for states to give up the Cold War concept that is based on ideology and establish instead a new concept of cooperative security. More and more countries have acknowledged that individual nations cannot achieve space security only by depending only on themselves and that a military advantage in space only can ensure space security for a short period of time, yielding to greater insecurity in the long run. Cooperative security is the only wise and realistic approach to ensuring space security. The concept of cooperative security ensures each and every country in the world enjoys equal rights to freely explore, develop and utilize outer space and its celestial bodies, and that all countries' outer space activities should be beneficial to economic development, the social progress of nations, and to the security, survival and development of mankind.

Our solutions must be built on sustained constructive cooperation. A very effective approach for the international community would be to call for space cooperation in order to reduce mutual suspicion and achieve common benefits in future space security. Given the world's rapidly growing reliance on satellites, coupled with advances in space technology, the development of wider and deeper cooperation to enhance mutual understanding and trust may be demanded to provide adequate space security for all who depend on the ability to access and use the space environment. Fruitful cooperation will promote international exchanges, technical assistance, and cooperation for peaceful purposes so that all countries can share in the economic and technological benefits of scientific advances in outer space.

China has been persistent in strengthening exchanges and cooperation in this field, with other countries, on the basis of the principles of equality, mutual benefit,

peaceful utilization of outer space and common development.¹ China has developed bilateral space cooperation with a host of countries and propelled multilateral cooperation in space technology and its application in the Asia-Pacific region. China has signed a number of cooperation agreements and memoranda on the peaceful utilization of outer space with a many countries, space agencies and international organizations. For instance, China and the European Space Agency (ESA) have signed the 'Status Quo of China-Europe Space Cooperation and the Cooperation Plan Protocol' under the mechanism of the China-Europe Joint Commission on Space Cooperation. The two sides cooperated closely during the lunar exploration missions of Chang'e-1 and Chang'e-2, and signed the 'Agreement on Mutual Support for the TT&C Network and Operation' in September 2011.² China and Great Britain have established a joint laboratory on space science and technology, jointly organized a seminar on space science and technology, and conducted exchanges on lunar exploration, earth observation, space science research and experimentation, as well as personnel training and other areas.³ Meanwhile China has taken part in relevant activities sponsored by the United Nations and other international organizations and supported international space commercial cooperation. The Chinese government actively participates in the cooperation and study of various projects of the Asia-Pacific Space Cooperation Organization (APSCO), including the development of a space data-sharing platform, its demonstration and application; an earth-based optic space target observation network; compatible navigation terminals, particularly in the formulation and release of its policy on small satellite data in the Asia-Pacific.

The solution must also involve the further strengthening of arms control measures. To ensure the peaceful use of outer space, prevent the weaponization of that domain, and avoid an arms race in space, it is now urgent for the international community to begin the negotiation of a treaty on space non-weaponization. The experience of humanity's conquering of space is the same as that of conquering the sea and the sky. When mankind enters a new environment, chaos ensues, because more and more entities seek to acquire their assets for their own interests. Given this scarcely tolerable confusion, which we might regard as a latent crisis, new regulations need to be made by the international community on the basis of the consensus of many nations. Nowadays, space security is at a turning point, which may be the last opportunity for humanity to regulate space technologies and enhance space management for avoiding space weaponization and the protection of the vulnerable space environment. That is why the international community should enhance the sense of urgency of calls for immediate action to put the arms control efforts on the right track.

Since the 1980s, China, Russia, and other countries have been initiating and supporting the idea of keeping space free of weaponization.⁴ Outer space belongs to all mankind and should be used exclusively for peaceful purposes to benefit human-

¹See the full text of China's Space Activities in 2011 at the website of The Information Office of the State Council of China: <http://www.scio.gov.cn>.

²ibid

³ibid

⁴As early as 1985, China submitted to the UN Conference on Disarmament (CD) a working paper entitled 'The Basic Standpoint on Preventing the Arms Race in Outer Space' (CD/579). In February 2000, in another working paper (CD/1606) put forward to the CD, China expounded on its position and proposals on how the CD should deal with the issue of the prevention of an arms race in outer space, including some tentative ideas about the basic elements of the envisaged legal instrument. In June 2001, China submitted further proposals (CD/1645) on the possible main elements of the proposed legal instrument.

ity. China has consistently maintained that the UN Conference on Disarmament in Geneva should negotiate and conclude an international legal instrument on preventing the weaponization of outer space. In order to adapt to the new space security situation, China and Russia proposed the draft 'Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects' (PPWT)⁵ on February 2008 as an international legally-binding treaty that would outlaw the weaponization of space. In fact, this draft goes further than the 1967 Outer Space Treaty, which forbids placing nuclear weapons and other weapons of mass destruction in space.

Meanwhile, considering lack of effective monitoring and norms in outer space, it is also necessary for the international community to establish confidence building measures (CBM) and a Code of Conduct for activities in outer space. The EU has issued a draft code of conduct for outer space activities,⁶ after revising two versions in 2008 and 2012, it calls for states, subscribing voluntarily, to 'minimize the possibility of accidents in space... or any form of harmful interference' and to 'refrain from any action which will or might bring about, directly or indirectly, the damage or destruction of outer space objects.' However, the draft code omits or bypasses the key problems of ensuring space security. The draft does not provide the definition of weapons in outer space nor prohibits their placement in space. In addition, it also does not express the desire for limiting full-scale missile defense systems in space.

There is one vivid analogy that illustrates its shortcomings in protecting space security. The red-green light system is designed for avoiding traffic accidents but it is as if we have permitted tanks to wander about the streets. It is thus urgent to negotiate the treaty that forbids the placement of weapons in space and the threat or use of force against outer space objects than a code of conduct which only focusing on the regulation of behavior in space by working out norms.

The solution must take into consideration the establishment of a mechanism of crisis management. Considering the increasingly congested space environment and more frequent occurrence of troubling 'incidents' in space, it is pressing for the human community to establish confidence-building measures and a crisis management system that avoids space incidents, including conflicts and the protection of space assets. First, the enhancement of mutual exchanges and understanding is an important strategic measure for space crisis management. Official channels, especially track-two exchanges, are proven confidence-building measures. It is through strategic-level talks and academic exchanges with different forums that the international community can convey a clear and consistent message, improve dialogue, and lay a foundation of moving toward greater cooperation. Second, elaborate pre-crisis planning and an effective organizational structure coupled with clear decision-making procedures are essential ingredients for collaborative space crisis management. Third, timely situational awareness and crisis response capability should be enhanced as the technical basis for reducing the possibility of satellite collisions.

⁵Available online at: <http://www.cfr.org/space/treaty-prevention-placement-weapons-outer-space-threat-use-force-against-outer-space-objects-ppwt/p26678>; accessed on 15 March 2016.

⁶Available online at: http://eeas.europa.eu/non-proliferation-and-disarmament/pdf/space_code_conduct_draft_vers_16_sept_2013_en.pdf; accessed on 15 March 2016.

Conclusion

Space, as a territory that is still unconquered by mankind, is increasingly related with the security of the world's nations. Greater complexity, uncertainty and unpredictability have become hallmarks of the world space security situation in the new century. The rapid development of advanced space technologies and the extensive use of space in high technology warfare suggests that space weaponization, space security and its relationship to global strategic stability has become a major topic of debate in the international community.

It is clear that space weaponization will lead inevitably to a power unbalance due to its counteraction of nuclear weapons and the associated effects in undermining strategy stability and international arms control mechanisms. In particular, with space deterrence overlapping with nuclear deterrence and cyber deterrence, strategic stability in the future will become more complicated and based on a new type integrated deterrence. The establishment and continuity of strategic stability in the future will rely on integrated deterrence and change the world order, international mechanisms and norms of behavior in international relations. There will be corresponding changes take place in arms control territory. Due to the interdependence of different strategic powers, it is necessary to shape the framework of future arms control mechanisms from a holistic perspective rather than from a narrow approach that only considers each domain in isolation. Faced with these new challenges and their implications for space security and strategic stability, the most important point is that it is now urgent for states to begin negotiations on treaty of space non-weaponization, to prevent an arms race, and to reduce rising tension in outer space. The international community cannot wait any longer.

References

- Hansson, Anders (2011) 'Refocusing European missile defense', *Space Policy*, 27, 116–117
- Hughes, Christopher W. (2009) *Japan's Remilitarization* (London: Routledge)
- Knopt, Jeffrey W. (2010) 'The fourth wave in deterrence research', *Contemporary Security Policy*, 31(1), p. 4
- Krepon, Michael (2014) 'Responding to China's counter-space capabilities', previously available from the Stimson Center. This item was no longer available on the Stimson Center website, <http://www.stimson.org/> on 15th March 2016.
- Sagan, Scott D. and Waltz, Kenneth N. (2003) *The Spread of Nuclear Weapons: A Debate Renewed*. W.W. Norton
- Sawako, Maeda (2009) 'Transformation of Japanese Space Policy: From the "Peaceful Use of Space" to "the Basic Law on Space"', *The Asia-Pacific Journal, Japan Focus*, 7(44), Number 1; available online at <http://apjff.org/-Maeda-Sawako/3243/article.pdf>; accessed on 14th March 2016
- Stevens, Tim (2012) 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, 33(1), pp. 148–170
- Stone, John (2012) 'The Future of Deterrence: Introduction', *Contemporary Security Policy*, 33(1), pp. 82–84
- Weeden, Brian (2014) 'Through a Glass, Darkly: Chinese, American, and Russian Anti-satellite Testing in Space', Secure World Foundation, <http://www.swfound.org/>

[org/media/167224/Through_a_Glass_Darkly_March2014.pdf](#), accessed on 15th
March 2016

Collateral Damage, Covert Operations and American Exceptionalism: An Interview with Chris Woods

RODERICK MCKENZIE

Chris Woods is the author of *Sudden Justice: America's Secret Drone Wars* (Hurst & Co., February 2015), which investigates drone warfare through interviews and insights of the pilots, analysts, Special Forces and intelligence officials who have been involved in recent action. Exploring the use of drones (or RPAs, remotely-piloted aircraft) by the CIA in Afghanistan, Iraq and Libya as part of the Global War on Terror, as well as more covert operations in Pakistan, Yemen and Somalia, Woods records an up-to-date and thorough history of drone warfare, confronting the often hidden consequences of their use.

RM: What is it about RPAs (Remotely-Piloted Aircraft) that make them so controversial in the eyes of the public? Is it a worry about the manner in which they are used, or is it something about the technology itself that is a cause for concern?

CW: It's both. From the public's perspective — and you can partly blame Hollywood and an overexcited media for this — unmanned or remotely piloted/remotely controlled vehicles of all sorts are novel and they're going to become increasingly dominant. We just had data through from the Royal Air Force saying that 4 out of 5 British air strikes in Afghanistan now are by RPA. That is a phenomenal shift in warfare and I think the public picks up on that and I think they are nervous around some issues. The problem with RPAs is that all sorts of other issues that get dragged in. Whether it's the assassination programme run by the CIA or concerns around automation and autonomy, which are often confused in the public's mind. They are kind of a lightning rod for lots of concerns around modern warfare, but in and of their own right they warrant significant interest, I think. They're a revolutionary approach to warfare and I think they need to be thought of as that, at least for the time being.

RM: A key aspect is accountability. How much transparency is there around who is directing the US's armed drone usage? What kind of accountability and oversight is there beyond trusting these organisations to self-regulate?

CW: The Americans have three separate but interlinked and intermeshed drone

campaigns: the conventional air force, special forces' drone use, and the CIA's programme. That gets complicated with the Americans when it comes to transparency and accountability. Because it's so tightly bundled up with elements that the United States doesn't want to publicly discuss, their approach has been to classify everything. Interestingly, we have seen a significant gulf open up now between the British and the Americans in the way that they view transparency. For example, the British now regularly release data on the number of missiles released, from which platform, whether British crews were using their own Reapers or were borrowing American ones, and they give tallies of civilian casualties. The Americans presently classify that data as top secret on grounds of national security. So it's a problem for the Americans – less so for the British at the moment.

The Americans, for example, measure RPAs in terms of combat air patrols (CAPs) — that's the ability to field continuous operations by RPAs over a 24-hour period. They can do that 63 times, so they have 63 CAPs, into which everything is bundled. So you've got your CIA strikes, your Air Force Special Operations Command strikes and your conventional air force strikes. They just can't unbundle it — it's like those kids' games where you pull out the straw and the whole thing falls down. So they don't pull out the straw. Of course, the problem in terms of public perception is it makes them look terrible. They refuse to discuss even the most basic facts about the armed drone programme with journalists, generally, although I did get some levels of cooperation for my book. And when it comes to assessing data, we know from the British that they're being open about it. If we want to understand how warfare is changing we're going to need that kind of data and that kind of information and there's a public discussion we'll need to have around that. Do we want that? Are we ready to go there? Does it have implications for foreign policy or defence policy? There are a hundred questions that the public has a valid point of view on. If you lock the public out of those discussions you're doing yourself a disservice, and that's the problem the Americans have at the moment.

RM: Is it something the US recognises as a problem?

CW: Yes, there are a number of congressmen and congresswomen who are very keen to see transparency and openness. Their focus, though, tends to be on the CIA's programme, or JSOC's [Joint Special Operations Command] programme in Yemen and Somalia. Interestingly there's much less heat about conventional use of armed drones in places like Libya or Iraq or Afghanistan, and I think actually we need to be looking at both. The media's focus has too often been on the CIA's use of drones — it's the big story. We knew virtually nothing about the use of armed drones on the conventional battlefield in Iraq or Afghanistan. One of the things I've tried to do with the book is speak at great length with the Americans, the Brits and the Israelis about that conventional use of armed drones, because we're so busy watching the targeted killing stuff that we're not actually measuring the effect on the regular battlefield. Most of it is probably good. I don't think it's necessarily a problem, but it is something that we need to understand.

RM: How much collaboration is there between the governments running drone operations and the governments of the countries in which the op-

erations are carried out? And how much responsibility do the latter bear for the actions that are taken?

CW: It depends entirely on which country you're talking about. In Afghanistan, for instance, there was intense intelligence co-operation over the years, but in the last year or two there has been real opposition from [Afghan President Hamid] Karzai because of the civilian casualties that armed drones were causing in Afghanistan. Let's be blunt: the United States is so extraordinarily well-endowed when it comes to intel, particularly on the tech side, that host governments are never going to be able to bring that to play. What they can bring is HUMINT (human intelligence). And that comes and goes in all of the theatres where armed drones are being used, depending on any tensions between the US or UK and the host government at any particular time, and that can have implications. If you lose your HUMINT, that can lead to higher civilian casualties, to greater collateral damage overall. There are implications for not having cooperation, but of course the counter to that is it can be hugely damaging to those host countries, particularly off the conventional battlefield. We've seen both the governments of Yemen and Pakistan significantly damaged in the eyes of parts of their population, I wouldn't say all of their population, but certainly vociferous and influential parts of their population.

So the act of cooperating can also have damaging blowback. And, military personnel in both Pakistan and Yemen have been directly targeted by insurgents and terrorists because they can't target the Americans themselves. Because it's remote warfare, there is this issue of displaced violence, that we don't fully understand and we're not building into our equations when we talk about remote warfare at the moment. So if you carry out a drone strike and AQ in Yemen sends a suicide bomber and kills a hundred soldiers at a passing out parade in Sana'a, do we count those numbers? And if we do count those numbers, does that influence what we think about remote warfare? Are the consequences more complex than we possibly give credence for? I think they are, actually. We oversimplify the idea of remoteness and of troops not being at risk.

Some attacks are driven by a sense of impotence, and this is the moral dimension to this warfare. If your troops are never in the field, where are the enemy going to direct their fire? Is that fire going to be directed at your civilian population, dispersed throughout the world? Or is it going to be directed at the host nation's? It's going to go somewhere. They're simply not going to suck up the violence. Nothing we've ever seen in warfare says they will.

RM: To what extent are journalists, NGOs etc able to provide a degree of oversight themselves for RPA programmes?

CW: It's without doubt a challenge, but it's not insurmountable. For example, my own research into civilian non-combatant casualties in Sararogha (former headquarters of the Pakistan Taliban) in 2009 tallied with the media's reporting at the time, with some degree of accuracy. We also know, for example, from the CIA's estimates in August 2011 of the number of militants and civilians they killed up to that point in Pakistan, which was around 2000. I've done some number-crunching on monitoring organisations and overall the numbers tally within 3-5% - certainly acceptable margin. So, I think the media's reasonable at getting the overall numbers - where

things get complicated is the status of those that are being killed, and that's the point of conflict in contention. Not how many (we're probably in the region of 2,500 killed in Pakistan, minimum), the question is how many of those were civilians. The CIA says 50; every other monitoring organisation and the government of Pakistan says 400. That's a huge gulf. And that gulf is pretty much the source of pretty much all the tension and public brawling over the CIA's use of drones in Pakistan. Why is the public's understanding of civilian casualties 8 times higher than the CIA's? That's the great contention.

RM: That's around the definitional issue, such as whether to include all males of fighting age as being combatants by default?

CW: The whole military age male issue, which is not confined, by the way, to the CIA in Pakistan; it's an issue in Afghanistan with the Americans as well. I go into that a lot in the book about how too often the Americans' language is too imprecise in war, to give them the freedom, if you like, to kill where perhaps they shouldn't be killing and where other nations would not kill. It is different, for example, from that of the British or the Germans and that is one of the conclusions I reach in the book: that America tends to fight its wars on behalf of civilians killed, and lose them because of the civilians it kills.

It was 2009 in Afghanistan before Sam McCrystal banged the table and said "if we don't stop killing civilians we're going to lose this fucking war". Why did it take 8 years for the Commander-In-Chief in Afghanistan to say that? There is something very wrong there. Once the hot war is over, you're into COIN (counterinsurgency), you're into post-conflict. You stop killing civilians. They didn't, so the drones get drawn into these bigger strategic questions. And the very interesting thing about armed drones is they have the potential to significantly lower civilian casualties in war. Their persistence, their precision, their ability to loiter, their real-time intelligence, their low yield on the present warheads — all of which are contributing factors to the ability to significantly lower civilian casualties, which is what we should all be aiming for in war. And, in fact, it's an obligation under the Geneva Conventions to use the weapon that causes the least civilian casualties.

But none of that matters unless it's coupled with political will, and I would say that has been the great distinction between British and American use of armed drones until recently — the Americans are much better at it now. The political will to restrict civilian casualties was there with the British and it wasn't there with the Americans until late in the day. And that's a fundamental difference in war.

RM: How have the approaches of the countries using armed drones in conflict changed?

CW: Before they were ever weaponised, drones were developed as persistent surveillance platforms. They were there to fill a hole and that hole was medium altitude, real time, loitering, incognito, delivery of intelligence that could then be remote fed, and the CIA was instrumental in that programme, as they often are in American ISR platforms. The weaponising of Predators came very late and was never intended; rather the Predator was weaponised specifically to assassinate Osama Bin Laden in

September 2000. By January 2001, the first successful trial had taken place using a Hellfire off a Predator and that's a problem we now have with RPAs: they are the first aerial sniper rifle. We'd never had that potential before. Aircraft go very fast, they tend to drop very big bombs and they tend to get out very quickly. RPAs, at least in their present iteration, have profoundly changed that. They loiter, they use these small yield weapons but they *are* sniper rifles in the air and they've been used aggressively in that role, not just by the CIA in, say, Pakistan, but on the conventional battlefield as well. So we know that the British have used their Reapers to carry out targeted killings; they publish the information themselves; it was cited in a recent defence select committee report. Now, if you've got a sniper rifle, it's always going to be a sniper rifle. You might pretend it's a regular rifle, you might pretend it can do a hundred other things, but it's still going to be a sniper rifle.

I think my concern for Reaper and Predator and the Israeli RPAs is: are we seeing a change in warfare that reflects the tools that we have? For example, I'm sure the British Military has, on occasion, had special forces carry out targeted killings on the battlefield, but in very limited circumstances. What we've seen with Reaper in Afghanistan is the rare become commonplace and the targeted killing of suspects in problematic circumstances happening quite frequently. And by problematic, I mean a bloke in province X which is nominally under Afghan/ISAF control riding a motorbike between town A and town B is targeted and killed. Why don't we pick him up? That seems to be pretty straightforward assassination really. I think the answer will be we don't want to put our troops at risk, and that's a valid point, but the point I would put in response is: are we changing warfare because we have the tools to change warfare? Are we thinking through the implications of the shift towards assassination/targeted killing as simply another *regular* aspect of conventional war and how will the enemy respond to that in time? I think we need to think about that.

RM: In what ways has the US failed and succeeded in its responsibility to identify targets and what have been the key difficulties?

CW: For the Americans, it got really complicated because of AfPak [US foreign policy approach of treating parts of Afghanistan and Pakistan as a single theatre of operations]. Between 2004–2008, the Americans predominantly targeted AQ in Pakistan with the active support of the Pakistan government. From 2008 onwards, the insurgency in Afghanistan was getting out of control and the Americans' targeting shifted aggressively from counter-terrorism [CT] to counter-insurgency [COIN]. So it was basically an extension of the COIN campaign across the border in Afghanistan smuggled in under the guise of the CIA's CT programme against AQ. And that's where things get really messy, because the insurgent groups that were being bombed – some of them were at peace with Pakistan, some of them were proxies of Pakistan. Pakistan then starts to get agitated with the Americans and the Americans started to introduce the signature strike [targeted killing on the basis of an intelligence 'signature' or pattern of behaviour], which on a conventional battlefield we call a target of opportunity. But as one CT specialist said to me, the problem here is that it's not a conventional battlefield; it's a civilian space in which we're looking to target. If you go looking for patterns of behaviour among a civilian population, you're going

to kill civilians. And that's exactly what they did.

I think the correlation between signature strikes and higher civilian casualties in Pakistan cannot be ignored. It should never have been permitted to carry out signature strike operations in a civilian environment. It's often implied Waziristan was this deserted area. When Pakistan began its military operations in North Waziristan, the estimated population was 350,000. 450,000 civilian came out; there's another 100,000 still there that we know of in this tiny bit of the world that's borne the brunt of American drone operations. These are strikes taking place in a civilian environment, and we've seen it recently in Gaza: if you bomb civilian environments with a reasonably dense population, you're going to kill civilians, and by that I mean civilian non-combatants.

I think the Americans got there in the end, as a response to public opinion. And I also think Obama also did eventually come in and bang the table and say "stop". So we have a comparable civilian casualty rate on both sides of the [Pakistan–Afghanistan] border now. We didn't have that before; far more civilians were being killed by drones in Pakistan than Afghanistan, but it was the same bloody war. You can't try and win a war with COIN values on one side of the border where you say we're going to avoid killing civilians, when the CIA is killing civilians in the same tribes as part of the same conflict. Who thought that that would ever bring anything but disaster?

RM: The Christof Heyns report raises concerns about drones lowering social barriers to conflict overseas. How true do you think that is?

CW: I think the slippery slope argument has some legs to it. When Obama ordered American engagement in Libya back in 2011, it was the first conflict America had been involved in since 9/11 that was not covered by AUMF (Authorisation for Use of Military Force, which was a congressional authority giving Bush and Obama the power to basically wage war wherever they wanted). So Congress said to Obama "you need Congressional authorisation for this, because it's a war" and Obama said "no I don't, because it's not a war, because there are no troops on the ground". I'm hearing similar noises coming out of the British Government at the moment, related to a possible deployment of our Reapers to the Horn of Africa. "If we go there it's not troops on the ground".

I have a particular concern with that – with the Brits in Afghanistan it was a UN mandate, it was a clearly defined conflict, very clear rules of engagement, we knew who the enemy were. The Brits are looking for a war for their armed drones; they want to stay in bed with the Americans; they're worried about that link being severed after more than a decade and we know that the British are considering sending their Reapers to the Horn of Africa – that means CT ops (counter-terrorism ops, not counter-insurgency ops) in wars that we're not involved in. That's pure slippery slope stuff and I think it is an indication of this lowered threshold for conflict. "We're not gonna have troops on the ground; we're just gonna send a dozen drones". Well, a dozen drones is a war. If you think what 5 British drones have achieved in Afghanistan since 2008. A tiny number of aircraft, kept basically in the air 24/7 carrying out this staggering number of strikes. So, a few drones is, these days, a war.

RM: What are your thoughts on the future of RPA technology?

CW: The more interesting thing about armed drones at the moment is that the present iteration of armed drones may not be with us for that much longer — they're slow, they're clumsy, but they bring pretty significant benefits to post-battlefield conflict. The next generation of armed drones that are being developed, most of them are jet-powered, they're fast, they plan to use much bigger munitions, and they're all about stealth because they're being used in a contested environment. Interestingly, the next generation of armed drones may lose us the battlefield benefits we have with this iteration, for example in terms of lower civilian casualties. If you're going in and out fast — one of the reasons we have bigger bombs on fast aircraft is because we want to be sure of the job. Because you have less time for the mission, you use a big munition to make sure the job is done, and therefore lose that advantage of lowering civilian casualties. So everything from Taranis to Avenger, which is the new General Atomics drone, they're all about speed and will be delivering big munitions quickly. It's just something to think about. We tend to think of armed drones as a continuum but I think we're actually about to see a technological leap which may not be to the benefit of civilians in the battle-space.

I think the Predators and Reapers work spectacularly against countries without air forces. It's the contested airspace that's the challenge and that's where all the Pentagon planning is. That means speed, that means stealth, that means throwing away a lot of the stuff we've gotten used to with armed drones. That said you could probably mothball the entire Predator or Reaper fleet today and unwrap it in 50 years time and it would still be as good, because it's about the technology you put on these things. They're perfectly solid platforms in an uncontested environment. And they'll do the job just as well 20/30/50 years down the line with whatever technology is needed at the time.

RM: In what sense is the US a trendsetter with a window of opportunity to establish an 'acceptable' pattern of use for drones, or has a damaging precedent already been set?

CW: Let's be absolutely clear, there are only two nations on Earth, as far as we know, that presently think that targeted killings beyond the hot battlefield are lawful (except in extreme circumstances) — that's Israel and the United States. The view of practically every nation is that such strikes are unlawful. So that's the legal thing and we too often swallow the American line that these are lawful and actually there's a very clear non-US position here that the British, for example, share, which is generally that these strikes are unlawful. The Brits have not been carrying out targeting killings by drone in Pakistan. Why? We're in the same war against the same people but we're not doing it. Why? That's a question we need to ask more often.

Within the highest levels of the American military and intelligence communities there is a profound debate at the moment about the efficacy of targeted killing, particularly off the hot battlefield. Very senior people are uncomfortable; others are very happy. There's a raging debate going on. So, is America by default laying down the ground rules? It could be argued "yes", but it's not a debate that's by any means over. You're seeing very curious shifts in American public opinion at the

moment. You're also seeing the Libertarian Right coming out very aggressively now against targeted killings which is interesting. Bizarrely, provoked by the Anwar al-Alaki killing, because of the constitutional implications that that had. It's certainly the view of the UN rapporteurs, Heyns and Emerson, that the Americans have been trying to lay down a precedent for targeted killings, but it's by no means clear that the rest of the world will follow. If the rest of the world did follow, my own view is that it would be anarchy. What would we think if Iran had a targeted killing programme beyond the hot battlefield? Or South Korea? Or even the Netherlands?

One of the things I looked at is that in the early days of the War on Terror the focus was not on assassination, the focus was on policing. It was rounding these guys up, aggressively, often involving extraordinary rendition, sometimes involving torture, Guantanamo. It was a messy business, but they were wound up predominantly without killing them. At what point did the United States become comfortable with targeted killing/assassination becoming another plank of foreign policy or military strategy? That's a fairly profound shift that I think is one I'm not sure the American public is as comfortable with as they would think. But maybe that's just my own spin.

We don't see China or Russia carrying out targeted killings so far, but we may. Of course it was Russia and China, both permanent members of the Security Council, who pushed for the UN investigation into armed drones. At the moment, there's more strategic benefit for them making trouble for the Americans over the use of armed drones – particularly the targeted killing stuff which is almost as unpopular as the torture programme – than there are to China or Russia going that way themselves. For them, the rule of law matters and targeted killing outside the hot battlefield is too problematic.

RM: Are we more likely to see countries that are more similar (politically) to the US that might pursue that route, such as the UK or France?

CW: The current coalition government certainly hasn't gone there with the military, but there is evidence that the British intelligence community has been complicit to some degree in the US targeted killing programme. That's worrying. If our public position is that our military doesn't do targeted killing but in essence we use the Americans like the neighbourhood hitman then I don't see that as a particularly healthy move for us as the UK. A case I've looked at myself was the killing of two ex-Brits who had their citizenship stripped by Theresa May, and within 18 months they'd been assassinated by the CIA in Somalia. I don't think that's a coincidence — I can't prove it and they won't tell me to what extent they shared intelligence on that, but I think that it's a challenge around intelligence sharing that could lead to lethal consequences. We've seen this with Germany, Australia, New Zealand and Britain now — it's a problem.

RM: Is the development of lethal autonomous RPAs (drones which identify a target and make a kill decision without the direct involvement of a

human actor) inevitable?

CW: My personal view is that we need to be in international treaty territory here and have them banned outright. The level of public disquiet is one thing, but also it's basic input/output. We're not very good sometimes at targeting the bad guys — we get it wrong. If we put those parameters into a machine it's going to get it wrong on an epic scale. I just don't think there's any interest from any of the Western militaries I've spoken with for autonomy. If you speak to people like Jim Cartwright, former Deputy Chief of Staff [for the JCOS in the US] they'll articulate a view that there always needs to be a human in the loop, and I think that that's the position. I think what gets confused is automation gets confused with autonomy. And there will be a lot of automation, a lot of processes will be automated. The head of the ISIR agency — the US Air Force's overall intelligence wing for drones and U2s etc. — walked me through a scenario where in the very near future raw intelligence coming in from a drone might be sifted for specific languages, phrases etc. Maybe only 1 or 2% of raw data ever makes it to the analysts — that's automation, and that's an inevitability. I think people will be less troubled by that, though it brings its own issues.

You're never going to carry the public on autonomy. Imagine up there now an autonomous lethal device policing, say. People would shoot it down! The fear and revulsion that brings in people. I'm not aware of any military planners who think this is remotely feasible or desirable. If they're out there, they're keeping their mouths shut.

RM: What sort of outcomes might we have seen in Pakistan/Yemen/Afghanistan etc if the United States had not used drones to carry out targeted killings?

CW: It's a really good question and I think the jury is still out. Let's take Pakistan — there's absolutely no doubt that armed drones have significantly denuded AQ and the Taliban and the insurgent factions, have profoundly changed their operational habits, their behaviours; have limited their ability to wage war. All of that's a given — that's tactical. What we don't yet understand is the strategic effect. I've spoken to a lot of US policy-makers on this: former ambassadors, intelligence officials, military officials. And there is really no clear view. We may have won a tactical war but lost the strategic one, is the risk. We don't know. With Yemen, Gregory Johnson has published his work showing that when the Americans began bombing AQ in Yemen in 2009 (not just with drones but with other...). There were about 900 of them, but within 5 years there were 3000 of them. Can you pin that to drones? If so, is it self-defeating. There are, I suspect, some very senior Americans who acknowledge and were always aware that in Pakistan there was only ever going to be a limited window to achieve what they wanted before blowback kicked in. And in the view of some of those former officials it already has. Some of them view it as kicking in a long time ago. So short-term, definitely; tactically, potentially a game-changer. Strategically, we don't understand. Is what's being done by us now going to have implications 10, 20 years down the line? We don't know.

RM: Are the US/Israel likely to change their approach to RPA usage due to legal/political/popular pressure and which will be the strongest factor?

CW: As I said, the United States — absolutely clear from all the data that's publicly available — from 2010 onwards a significant effort on both the conventional and the unconventional battlefield to reduce civilian casualties from RPAs. And it succeeded. The United Nations Mission in Afghanistan (UNaMA) — it monitors drone use there — around 5% of drones strikes they think in Afghanistan cause civilian casualties. That's not bad for a weapons system. If you go back 50 years to indiscriminate bombing to a situation where civilians are at risk from 1 in 20 strikes and in fairly small numbers where they are killed. Very unfortunate and sad but not huge casualties. All the indicators say that the US has made significant efforts to reduce civilian casualties and have introduced the reduction of civilian deaths as a political imperative. But I go back to what I say: the benefits of RPAs are for nothing if we don't have the political will to reduce civilian casualties, and I think we're seeing that right now in Israel with Gaza unfortunately. The level of civilian casualties from those air strikes is staggering. Partly that's the munitions they're using and partly it's their attitudes towards the people they're killing. That's the problem. I read a number to day and it actually shocked me. In the first intifada (1987 to 1993), the six-years-long intifada, no more than 500 Gazans died in six years of fighting between the Palestinians and the Israelis. We've seen 1200 killed in just a couple of weeks. It gives you an indication of the stunning intensity of the war in this tiny plot of land in which 1.5 million people are crammed in. Unless you have the political will — it doesn't matter how precise your drones are; it doesn't matter how effective your munitions are; it doesn't matter how well-trained your personnel are — then you're going to see problematic civilian casualties unless you tell them not to.

RM: You mentioned that by and large in terms of international humanitarian law and human rights law that by and large the framework is already there to deal with this — do you think there will be pressures to introduce something specifically to curb US/Israeli actions?

The Americans and Israelis are trying to change international law by example. The whole non-international armed conflict model that the Americans use — they're creating a hybrid law that straddles IHRL and IHL that is very vague in areas that really shouldn't be vague, in my view. The Israelis are in similar territory. Will they carry the rest of the world with them? There was a very interesting speech that John Brennan made back in 2012 where he stressed that there needs to be a rulebook for other nations to follow. The problem is that America has already written that rulebook, predominantly, and it's a rulebook that America will not want to be on the receiving end of. But you know, American exceptionalism — discuss!

RM: Future use of drone technology appears inevitable at this stage — what do you imagine is a realistic, ideal approach to their use in future, and how likely are we to see that become a reality?

CW: As early as 2010 the Americans were training more RPA operators and pilots than they were conventional aircrew. We passed that long ago. They're here to stay. What we're seeing in Afghanistan from the data the British are giving us is a profound shift in warfare. Some of the implications of that we don't really get yet in terms of shifts in personnel here. Really interesting stuff going on within MoD analysis and really theoretical discussions going on around longer term implications and, yeah, they're here to stay. They're going to continue to radicalise warfare. We haven't even begun to see the start of the rollout of operated land or sea vehicles and that again is going to have a huge effect. But that's a whole other tale.

RM: If you had the opportunity to write the rules for how they would be used in future, how would you go about it?

CW: My personal view is to keep them on the conventional battlefield. I'm a European and my book shows the perspective of a European. We don't execute people in this country. We put them on trial and we find them guilty and we put them away. In fact, our criminal justice system has been very, very good at dealing with terrorists, and our military has been very good at dealing with insurgencies. If you bolt onto that assassination beyond the battlefield, for me that's a problem area. Use RPAs on the conventional battlefield; they have a lot of benefits over other weapons systems and I don't see them as being particularly controversial, except where we see this leakage where targeted killing becomes a regular affair on the conventional battlefield. That's a big grown-up discussion that the public need to be part of. Is this how we want to be conducting our wars? And what are the implications back home. There are implications, by the way. Military lawyers are absolutely clear that remote personnel based in the UK and America are lawful targets. Does that mean their families, their homes, their vehicles, their towns are too? You can see the potential for collateral damage. These are discussions we need to have about how if we're going to have war-fighters living among us, what does that mean in terms of the risk to them and to the broader communities they live in? There are other issues there as well.

Drones and the RAF: An Interview with Squn Ldr Keith Dear

JAMES FERGUS ROSIE

Squadron Leader Keith Dear is a serving officer in the Royal Air Force, intelligence officer with 10 years experience in the field. He is also the author of *Beheading the Hydra? Does Killing Terrorist or Insurgent Leaders Work?* (Defence Studies Volume 13, Issue 3, 2013) and is working with Oxford University to apply the insights of modern psychology and behavioural sciences to full spectrum targeting. The views expressed in this piece are Keith's alone and do not represent the views of the RAF.

JFR: Given the RAF's recent commitment to expand the number of drones, how significant do you feel this for the future direction of the RAF, especially with the forthcoming SDSR?

KD: The biggest problem the Royal Air Force might face would be a major state on state conflict, perhaps in Europe, in which our involvement was considered truly non-discretionary after years of focusing on the non-state adversary. The challenge in this eventuality would be the speed with which we could expand our current force to meet a peer competitor. If we recall that the biggest challenge in the Battle of Britain was not the loss of aircraft, but the loss of pilots, the increasing use of drones may in time come to mitigate this risk, keeping 'drone' pilots in the rear and away from immediate danger to enable us to grow more rapidly by reducing the loss of pilots to enemy action. Drones may also help to offset the rising unit cost of aircraft. In his Trenchard address ACM Pulford challenged industry to reverse what has become known as Augustine's Law the exponential rise in the Unit cost of aircraft. Drones might perhaps offer some of the savings sought — they remove the need for the messy compromises in aerodynamics, weight and g-limitations that putting a person in the aircraft brings. If this is the case they could again help us to grow rapidly to meet a future state adversary.

I think in the long-term drones will play a greater role because of their manoeuvrability and the growth of passive detection measures. In the future it will be increasingly difficult to hide aircraft and they will therefore have to get smaller to be effective. In addition to this, as missile technologies improve, the g limitations of human beings will mean that the advantage in end-game manoeuvre is increasingly with air-to-air and surface to air missiles. Smaller aircraft will be harder to find with surveillance techniques, harder to target due to their lower radar cross section and emissions and able to manoeuvre harder in the end game if they are targeted. I think therefore that in time unmanned aircraft will have a higher survivability rate.

The expansion of our drone force under these circumstances seems certain.

That said, we are a long, long way from replacing our manned aircraft with drones just yet. The RAF's commitment to expand the number of drones it operates acknowledges that remotely piloted aircraft are going to make up a growing proportion of our force, but it does not commit us to an arbitrary percentage. I also think there will always be a need for a number of manned aircraft for flexibility. It is possible that a future ECM environment could render all remotely piloted aircraft ineffective. In this eventuality we would need pilots to fly machines that were entirely self-contained in order to operate.

JFR: Although drones, in the public imagination, are strongly identified with missile strikes and counter-terrorism operations, how important to you consider this in relation to their role in ISR?

KD: Drones do so much more than the public and much of the military credits them with. Their association with missile strikes and counter-terrorism operations is justified, they have played a huge role in US operations around the world. They have also allowed the US to operate in the air space of countries that wouldn't have been prepared to allow manned aircraft to operate. This is both fascinating and unique and I think accounts for their close association with counter-terrorism operations — the public understands that this capability is allowing the US to operate against terrorist cells across borders in a way it could not have previously done. Quite why unmanned aircraft should be more acceptable than manned aircraft to states such as Yemen and Pakistan is a subject worthy of greater study. I suspect that psychologically the use of unmanned drones feels less of a violation than giving up you airspace to pilots from another country. Illogical though this is, the unique freedom to operate that has been granted to drones is new and accounts for the strong identification of drones with counter-terrorism in the public imagination.

However drones are much more than just strike platforms with unique freedom to operate. Their endurance makes them first and foremost ISR platforms able to provide continuous video feeds of activity on the ground for many hours at a time, which in turn provides us far more information on potential targets than ever previously available helping to target more precisely and reduce unintended damage or deaths. But drones are not just cameras in the sky either, a common misconception within the military. They can carry a range of collection capabilities, which can sometimes be more important than the video feed they are providing or the bombs they can drop. Indeed, as I described in *Beheading the Hydra* the missile strikes themselves can, under certain circumstances, be counter-productive. Far more important is the building of the intelligence picture, the help they can provide in enabling us to locate and understand our adversary in order to interdict attacks and understand how he operates and future intent.

JFR: Elsewhere you've discussed the possibility that the simple knowledge of being observed by a drone can affect how someone acts. Could you expand on this idea?

KD: That the feeling of being watched can change behaviour has been shown beyond

doubt. A picture of human eyes placed above a university coffee bar honesty box increased donations to the fund threefold. (M. Bateson, D. Nettle, and G. Roberts 2006) Adding eye images to a university cafeteria reduced littering in the cafeteria by half; (Ernest-Jones, Daniel Nettle, and Melissa Bateson 2011) eye images had the same effect on littering campus wide; (M. Bateson, Callow, et al. 2013) adding them to charity donation buckets in supermarkets increased donations by 48% (Powell, Gilbert Roberts, and Daniel Nettle 2012) and they reduced bicycle theft by 62% when displayed at bike sheds. (D. Nettle, Nott, and M. Bateson 2012) Placing eye images by bus stop rubbish and recycle bins increased the correct use of the bins and the volume being recycled. (Francey and Bergmüller 2012) People issued stronger moral condemnation of immoral actions in the presence of eye cues than in their absence. (Bourrat, Baumard, and McKay 2011)

Feeling observed can increase altruism even when it comes at a personal cost. Eye images increased generosity in an anonymous ‘Dictator Game’ where a person is given an allocation of \$ 10 on a computer screen and then has 20 seconds to allocate an amount (or nothing) to another player, keeping the rest for himself. After the experiment the subjects are paid anonymously. When subtle eye cues were present on the screen, allocations rose by an average of 31.4%, when the eye images were clearer, allocations rose by an average of 55%. (Haley and Fessler 2005) A similar experiment at Harvard University showed the presence of eyes, increased altruistic contributions in an economic simulation by 29%. (Burnham and Hare 2007) It has been comprehensively proven that feeling watched directly or by ‘eye cues’ changes behaviour. It is equally clear that this response is subconscious, since subjects cannot be responding rationally — the presence of stylised eye images is no greater reason to refrain from stealing a bike or to give away more money. This is fascinating but not surprising. Neuroscience shows that human and non-human primates have over 30 regions of the brain dedicated to visual processing, ‘including areas that contain neurons responsive to visual social signals’. Many primates rely on gaze perception and gaze detection to gain valuable social clues as to how to behave. (Emery 2000, p. 582) It may be the amygdala that is responsible for this sensitivity to gaze. The amygdala is associated with emotion and social behaviour, creating a response to perceived threat or embarrassment. (Emery 2000, pp. 596–597) Being (or feeling) observed is often a critical component or precursor to both embarrassment and/or threat, explaining perhaps the amygdala’s involvement and providing further evidence to suggest there is an uncontrolled emotional response to being or feeling watched which may alter behaviour subconsciously.

We might therefore suggest that when drones (or other ISR assets) are used to ‘stare’ at people their behaviour will change. There is both science and a real-world experiment to support this hypothesis. The feeling of being watched can be induced indirectly and still reduce cheating, an insight that suggests surveillance via technology may have similar effects on behaviour to direct gaze and eye cues. This has been shown in children who thought an imaginary friend was present when playing games, in adults when the 10 Commandments are displayed (invoking the idea of an all-seeing God), and in lab students when they believed the ghost of a former student may be present. (Zak 2012, Piazza, Bering, and Ingram 2011, Shariff and Norenzayan 2007) In each example the belief or feeling that someone was watching changed behaviour. George Clooney and the human rights activist John Prendergast established a project with Harvard University paying commercial satellites to ‘stare’ at Southern Sudan with the aim of reducing human rights abuses. This Satellite

Sentinel Project is putting the assumption that surveillance can change behaviour to work in the real world, but the number of confounding variables make it impossible to know if it is working or not. I believe there is enough science to show that surveillance might change behaviour, and that if it does, we must understand how and to what extent it does so. Proving the hypothesis that surveillance changes behaviour could directly affect how we employ our drones and ISR technologies. It would also provide a powerful argument for the procurement of more such assets — if we demonstrate that ISR can do far more than just allow us to ‘see over the hill’, that it can have a behavioural effect in the battle space, then we have a whole new way of looking at what we do with drones and how we use them.

JFR: How closely do you think any effect on behaviour is linked to the idea of deterrence?

KD: Do you mean deterrence in the sense of deterrence theory, or deterrence in the more general sense? In the former example I think it depends on the situation. Effective surveillance in a peace-keeping scenario helps to reduce information asymmetries which allows combatants/participants to understand the position of the other. I think this can aid deterrence in the sense that it allows the other party, and the international system, to respond and react thus deterring further activity. A good example from my own experience is Abkhazia, Georgia. Prior to the 2008 conflict we were in the process of buying UAVs as well as air and maritime surveillance radar to better understand the movements of Georgian and Russian military forces in the ceasefire area. Without this both were, we thought, exploiting a mountainous area between the two areas patrolled by UN. Had we been able to expose any of the movements we believed may have been occurring I think both sides would have drawn back, which would reduce the risk of conflict and miscalculation.

There are other obvious examples where surveillance can be linked to deterrence: when surveillance is often followed by attack, as with the use of drones in Northern Pakistan and Afghanistan, or with the threat of prosecution of war crimes, as in the Satellite Sentinel Project’s stare at Sudan. However I think most interesting is the effect that has little to do with the conscious cost-benefit equations we are dealing with when we discuss deterrence. It’s the pre-conscious effect, that which reduces cycle theft when pictures of eyes are placed in a bike shed, or increases the collection of litter in canteens when eye images are placed on the walls. It’s fascinating, and potentially powerful, but it owes little to the conscious weighing of possible positive and negative outcomes. It’s a very neat example of why our common-sense employment and understanding of Rational Choice Theory is not sufficient for understanding behaviours and therefore is not a sound foundation for planning military operations.

References

- Bateson, M., L. Callow, et al. (2013). “Do Images of ‘Watching Eyes’ Induce Behaviour That Is More Pro-Social or More Normative? A Field Experiment on Littering”. In: *PLoS ONE* 8 (12). DOI: [doi:10.1371/journal.pone.0082055](https://doi.org/10.1371/journal.pone.0082055).
- Bateson, M., D. Nettle, and G. Roberts (2006). “Cues of being watched enhance cooperation in a real-world setting”. In: *Biology Letters* 2, pp. 412–414.

- Bourrat, Pierrick, Nicolas Baumard, and Ryan McKay (2011). "Surveillance cues enhance moral condemnation". In: *Evolutionary Psychology* 9 (2).
- Burnham, T.C. and B Hare (2007). *Engineering human cooperation — Does involuntary neural activation increase public goods contributions?* Vol. 18, pp. 88–108.
- Emery, N. J. (2000). "The eyes have it: the neuroethology, function and evolution of social gaze". In: *Neuroscience & Biobehavioral Reviews* 24 (6).
- Ernest-Jones, Max, Daniel Nettle, and Melissa Bateson (2011). "Effects of eye images on everyday cooperative behavior: a field experiment". In: *Evolution and Human Behavior* 32, pp. 172–178. URL: <http://www.staff.ncl.ac.uk/daniel.nettle/ernestjonesnettlebateson.pdf>.
- Francey, D and R Bergmüller (2012). "Images of Eyes Enhance Investments in a Real-Life Public Good". In: *PLoS ONE* 7 (5). DOI: doi:10.1371/journal.pone.0037397.
- Haley, K. J. and D. M. T. Fessler (2005). "Nobody's watching? Subtle cues affect generosity in an anonymous economic game". In: *Evolution and Human Behavior* 26, pp. 245–256.
- Nettle, D., K. Nott, and M. Bateson (2012). "Cycle Thieves". In: *PLoS ONE* 7 (12). DOI: doi:10.1371/journal.pone.0051738.
- Piazza, Jared, Jesse M. Bering, and Gordon Ingram (2011). "Princess Alice is watching you": Children's belief in an invisible person inhibits cheating." In: *Journal of Experimental Child Psychology* 109 (3), pp. 311–320.
- Powell, Kate L., Gilbert Roberts, and Daniel Nettle (2012). "Eye Images Increase Charitable Donations: Evidence From an Opportunistic Field Experiment in a Supermarket". In: *Ethology* 118.11, pp. 1096–1101. ISSN: 1439-0310. DOI: 10.1111/eth.12011. URL: <http://dx.doi.org/10.1111/eth.12011>.
- Shariff, Azim F. and Ara Norenzayan (2007). "God is watching you priming God concepts increases prosocial behavior in an anonymous economic game." In: *Psychological Science* 18 (9), pp. 803–809.
- Zak, Paul J. (2012). *The moral molecule: The source of love and prosperity*, p. 150.

On the Ethics of Drone Strikes, Optimism and Obscuring Language: A Conversation with an Anonymous Academic

CHRISTIANA SPENS

CS: Is there an ethical dilemma regarding the use of drone strikes, and is that dilemma specific to drones, rather than air strikes, for instance?

AA: I think there are ethical dilemmas specific to drones because of the ways that drones are deployed. So they're deployed by people who are entirely remote from the target. And therefore, the kind of decision processes that human beings are normally capable of when they are in a relationship with their environment and capable of picking up all kinds of cues, both consciously and subconsciously. That sort of relationship with the environment — those sorts of feeds to intelligent decision-making — are absent. Therefore I think there are specific issues.

CS: Is it fair that there should be so little risk for the drone operators? Does it matter that one side risks so much less than the other?

AA: I think this is part of a larger question, whether it is now possible for a just war to be fought justly. Now this is a big philosophical question, and I'm not an expert on it, but it seems to me that increasingly, there are things that suggest that the answer to that is no. Part of that is that the attacker in this case has much less at stake than the potential victim. So I think there are another series of issues there that merit exploration.

CS: More generally then, if killing is made 'easier' through such technology, then how does this affect the people instructed to kill, and the action of killing?

AA: I would be very interested to know the answer to that. I was chatting to somebody within the last week who says there's been some interesting work on that recently, and some science of psychological issues and mental health issues as a result. Which I think one would expect, but previous work on PTSD and trauma and killing suggests that the greater distance — physical and psychological — from the target — in a sense the easier it is to manage the personal and psychological consequences. So that would be a very interesting thing to explore.

CS: From a philosophical rather than psychological point of view, do you think, if the killing is at a distance (physically and psychologically), does that make it any different, morally? Does it make a difference?

AA: To the targets it doesn't make any difference. They're going to be killed. There's an ethical dimension over the accuracy of these weapons. And it seems to me that there's quite a lot of mythology surrounding — and loose use of language surrounding — modern high tech weaponry. There are these clichés about surgical strikes, that these would only 'take out' or whatever is the current euphemism — enemy targets — and this, quite clearly, is not the case. And yet the discourse surrounding this — in particular from the military and from politicians — is, I would suggest, really quite misleading. And I think greater care needs to be taken in ensuring that people who are not only within the system, so to speak, that is resulting in deaths via the use of these weapons — but also the public and politicians are much more careful in their use of language.

CS: If the people involved, then, are misled into thinking that, perhaps by the language used, that these strikes are ethical because they're more specific than they really are — whose responsibility is it, then? Is their moral responsibility less because they're being misled?

AA: Well, I would be interested to know more sufficient detail to know how the kill chain works, to be able to answer that question. But I don't know how it works. An analogy of the decisions that led to the dropping of the bombs on Hiroshima Nagasaki — in which, it has been suggested, in a very good book by Jonathan Glover, that *nobody* really felt responsible, from the president downwards. And that is possible, I suppose, with the spread of responsibility and the very large numbers of people who are involved in that decision-making. And the way that they will rationalise and justify and imagine what it is that they are doing. I don't know whether that's a good analogy or not, but I find it quite a helpful one.

CS: So perhaps no one has any direct responsibility for actually killing someone, if they can rationalise their part in it by saying 'I was told to do this' and so on... That comes about through a diffusion of responsibility, but ultimately people still die.

AA: People still die. Just to go back to my atomic bomb analogy — President Truman, according to his journals, appeared to have convinced himself that those two bombs were attacking military targets. And that is quite an interesting definition of military target — if you're actually going to wipe out large amounts of two cities. So I think a lot of the things that are going on here, as you say, diffuse the sense of moral and ethical responsibility. And actually, the responsibility of making decisions.

CS: And going back to the first question, is that specific to drone strikes? Or is this the latest manifestation of the tendency of responsibility to be diffused? Is it also an inevitable consequence of technological advancement?

AA: I think that there is a difference to the experience of a pilot in the air, and the operatives, often contractors, who are on another continent. I think it is a difference

in experience. And it goes back to my original point about environmental clues and feedback informing decisions. That said, the literature on bombers and fighter pilots, certainly in the Second World War (I'm not so familiar with the more recent literature), suggests that for them, killing at a distance was considerably easier than for people who were kind of hand to hand.

CS: Are there historical precedents to the use of drone strikes in Afghanistan (especially), and, if so, what do these precedents tell us about current strategy and its possible strengths and pitfalls?

AA: Obviously a drone is different to previous sorts of aerial bombardment, but Afghanistan, as I recall, was the first area in Central Asia, where after the First World War, the UK bombarded from the air, in the so-called, very brief, Third Afghan War. I think what we can learn, going way back into the first Anglo-Afghan War in 1839–41, is that British military activity in Afghanistan has resulted in the reputation of the British being extraordinarily casual about civilian casualties. Memory in societies with oral traditions is long — memories get confused — but are still strong — and stories about the excesses of the army of retribution, after the disastrous retreat of the First World War, were still current around 1970 when the American anthropologist Louis Dupree visited the site of the British retreat and collected such stories. And what the Brits did with the Indian seapoys to exact revenge in Afghanistan in 1842, was a terrible atrocity, and these things are remembered, albeit in a mixed up way — and of course the Afghan written accounts of what the Brits did in the first two Afghan wars are very different to the accounts that I'm familiar with, you're familiar with — what was written by the Brits. So what's the relevance of that to drone strikes? That the drone strikes provide further evidence of this casual approach to civilian casualties in conflict on the part of the Brits. And I would have thought, in spite, no doubt, of their best efforts otherwise, the US military would have gained a similar reputation. So I think that's an important theme.

CS: And in terms of propaganda, obviously those against the Americans can use these memories and this construction, whether true or false, that this is a long injustice that has been going on for many years, and one that should be rebelled against... So it feeds into a current propaganda war also.

AA: It does. It does not surprise me. I expect history will judge the drone campaigns, and the intensity of them in that area, including in Pakistan, as having been a cause of exacerbating the security problem in that region and internationally. To some extent — I mean I can hear the US military, if they were here, or the UK military, if they were hearing me say this, would say, but you (plural) are beneficiaries of this because we have killed so many leading members of Al Qaida. Well I have my doubts about this... One might need to define success in a broader way than the number of enemies killed.

CS: So a longer view of success?

AA: Absolutely, a longer view. And a broader definition. One needs to think what it is like for the people living in the FATA area, having drones above them all the

time. Well, a lot of the time. The effects of that must be extraordinarily disturbing. I imagine that it's unlikely for people who are affected by drones, either directly or indirectly, to think that what the US is doing is justified and righteous.

CS: What do you think would be a better alternative to using drones in Afghanistan and Pakistan (and whether or not that depends on the region)? Would air strikes be better, or would more careful assassinations of certain people be better, and does that vary, region to region?

AA: There must be a difference between drone strikes within Afghanistan and drone strikes on sovereign Pakistan territory, which must create huge difficulties for the Pakistani authorities, and for the way that Pakistan is trying to secure itself. As to methods of assassination, I'm not sure I'm in the position to judge.

CS: I suppose I mean that, in effect, drone strikes can seem more like a messy type of assassination, if the aim is for 'surgical strikes'. But assassination isn't seen as a great idea for various legal reasons. Pragmatically, though, would assassinations actually be more ethical than drone strikes, when [drone strikes] involve so much collateral damage?

AA: Well I wouldn't want to be in a position of attempting to justify assassination. And I think what we're talking about here rather depends on how one frames the activities of the Allies: what is the mission in Afghanistan, what right is there for the US to be killing people in Pakistan? So I'm not sure in this context what 'assassination' would mean.

CS: I suppose I just mean is that when talk of drone strikes is about 'surgical strikes' and the 'taking out of certain key targets', firstly that isn't really any different to assassination, and secondly, other types of assassination might actually be more ethical, since there could be less collateral damage.

AA: Well are not drone strikes a method of assassination?

CS: If the intention is simply to take out certain people, I don't see how they are very different, really. And it would be more ethical to just take out one person, than take out various others as well.

AA: Well I'm not sufficiently expert in knowing about whether it is possible to take out fewer people using different methods of assassination. . . I think that clearer thinking about what drone strikes do [however], and what the language used actually means, would help focus minds. 'Targeted killings', 'collateral damage', 'taking people out' . . .

CS: I suppose that's the problem — a lack of transparency when it comes to describing the effects of drone strikes.

AA: The debate *is* obscured by the use of language, it's also obscured by the extraordinary over-optimism of what the military tend to claim that they're able to do. A book I'd strongly recommend [on this subject] is *Overconfidence in War* by Professor Dominic Johnson. . . He explores the adaptive utility of optimism, in con-

flict. So an example is the extraordinary optimism there would appear to be about — and enthusiasm for — allied air strikes on Iraq and Syria, as if there somehow will be a panacea, and this tends to be a characteristic of discourse at the opening of hostilities. Exaggeration — well meaning — by wonderful people — about what can be achieved.

Review: Ramsay, Gilbert (2013), *Jihadi Culture on the World Wide Web* (Bloomsbury: New York)

RODERICK MCKENZIE

In *Jihadi Culture on the World Wide Web*, Dr Gilbert Ramsay offers a fascinating insight into a highly topical area with his analysis of how online jihadis define themselves, express themselves and defend themselves on the internet. In the early part of the book, Dr Ramsay makes the important observation that ‘jihadi’ behaviour on the web, as extreme as it may often appear, is a far cry from the perpetration of physical acts of violence. Rather, he suggests that the online culture of jihadis has more in common with more ‘conventional’ online groupings, such as the obsessive fans of features of popular culture and those with a general desire to reach out through social media.

It’s no secret that many among us are far more vocal online than we would ever be in person (occasionally to our detriment), and Ramsay suggests that online jihadis are little different in that regard. He warns of the dangers of confusing those of a radical Islamic disposition with actual terrorists, simply because their views are considerably more extreme than most people are comfortable with. In his words, “[t]he problem is not with the old cliché about the impossibility of defining terrorism, however. Rather, it is with the tendency for the meaning of the word, which surely ought to refer to specific sorts of violent action, to be applied to movements and ideologies which, however dangerous they seem, are not equivalent to actual violence happening in the world.” In this respect he convincingly plays down the fears that many within the media and counter-terrorist circles have about so-called ‘terrorist websites’ by highlighting the lack of evidence that the role played by the internet has led to an increase in acts of physical violence.

In the early part of the book, Ramsay demonstrates his considerable knowledge and understanding of both Islamic culture and the Arabic language as he considers the definitions and implications of the terms *jihad*, *jihadism* and *jihadi* as well as their distinction from the physical acts of the *mujahedin*. He also shows that he is not afraid to (respectfully) critique the established names in the supposed field of ‘terrorism on the internet’ by criticising the tendency to try and isolate this field as a single area of research, instead indicating that usage of the internet by the spectrum of actors from radical Islamists to genuine terrorists needs to be considered with the broader context of their behaviour both on and offline. Specifically, Ramsay convincingly questions the usefulness of the internet as a tool for such areas as attack planning, terrorist knowledge sharing, fund-raising and recruitment, indicating that the number and scale of physical attacks by so-called self-starters inspired by what

they may have read on the internet are little different to the level of violence one might expect by individuals motivated by what they have seen on conventional news reports. While not dismissing its potential, he highlights that claims that the internet has in any way contributed to an increase in terrorist attacks are as yet unproven.

In a detailed analysis of the theoretical aspects around group behaviour on the internet, particular amongst television fandom, the book suggests that many members of jihadi online communities take part as much because of a sense of escapism and a sense of community as because of the actual content of their communications. Ramsay scrutinises the content of self-proclaimed *jihadi* websites, looking at the use of imagery, video clips and music (*nashids*) and shows a clear understanding of the non-linear fashion in which information is created, shared and stored on the web. The book offers a fascinating incite into the heart of *jihadi* forums, such as the sense of community or lack thereof as the closed, controlled nature of *jihadi* culture conflicts with the free-thinking, discursive nature of the modern internet.

A particularly interesting (and oddly entertaining) chapter looks at the interactions between *jihadis* and non-*jihadis* online, considering the struggles *jihadis* face in trying to convert others while avoiding coming across as overly radical, yet simultaneously trying to justify their engagement in digital — rather than physical — *jihad*, both to others and, it would seem, to themselves. This internal conflict, in which online *jihadis* must justify their online engagement as sufficient to satisfy their own obligations towards *jihad*, while simultaneously insisting that it is entirely necessary for others to carry out physical acts, is particularly thought-provoking. Ultimately, Ramsay determines that internet *jihadism* is not merely a precursor to physical acts, or even a lesser activity in the eyes of those involved, rather it is a separate action with its own merits.

To reinforce his arguments, Ramsay offers a comparison of online jihadi culture with Islamophobia and Crusaderism on the web. While recognising the seriousness of the problem of Islamophobia, he remarks on its similarity with online *jihadism* in that it does not necessarily correspond to physical acts of violence, and that the internet itself has not necessarily led to an increase in acts of violence.

The book is very well written and makes for an engaging read. There are sections of the book that are heavy on theoretical analysis (particularly the second chapter) and which may consequently put off readers from a non-academic background, but overall the book is written in an accessible form with some clearly described and dispassionately considered conclusions. The highly topical nature of the content — particularly as governments seek to extend their own powers to control and carry out surveillance on the actions of their citizens online — together with the original insights presented ensure that this book makes an extremely valuable contribution both to the world of academia and, hopefully, to policy-makers, who would do well to consider this measured assessment of the true level of risk posed by radicals (of all kinds) online.

Review: Gary J. Bass (2014), *The Blood Telegram: Nixon, Kissinger and a Forgotten Genocide* (Hurst & Co: London)

CHRISTIANA SPENS

It is often said that ‘history is written by the winners’, though there is some room for challenge to that truism, it would seem, given the publication of Bass’ recent exposé of the role of Nixon and Kissinger in the massacre of hundreds of thousands of (mainly) Bengali Hindus in 1971. Whether power can be won in retrospect with critical historical research is a topic for another essay, another book even, but certainly we see in Bass’ astounding volume a shifting of perspective and understanding of a previously hidden chapter of American as well as Pakistani, Bengali and Indian history. Specifically, *The Blood Telegram* exposes the manner in which Nixon and Kissinger, during the Cold War, illegally and covertly supported Pakistan’s assault on East Pakistan (now Bangladesh), which killed hundreds of thousands of civilians and displaced around ten million more, putting huge strain on India, where most were taken in.

Bass focuses on the American role in this story, and specifically the diplomat whose outrage at the massacre was most vocal: Archer Blood, the US consul general in 1971 in Dhaka, the principal city of East Bengal. His dealings with, and protestations of the behaviour of the higher American administration are telling, certainly, and to focus on this diplomat’s place in the unfolding atrocities and related political manoeuvres is, in itself, a clever choice on the part of the author. An underlying understanding of what makes a good story, and what makes history readable, is key to the book’s wider appeal and effect in communicating a brutal and complex report in a compelling fashion. Learning the details of the massacre and the role of Nixon and Kissinger in its unfolding violence, through Blood’s cables and telegrams (which reported the gruesome reality of the genocide to those in DC), as well as new interviews and previously unheard White House tapes, provides a gripping narrative and sense of urgency that is eminently readable. The story exposed remains as shocking as it did at the time: “At the White House, Kissinger’s aides were shaken by Blood’s reporting. “It was a brutal crackdown,” says Winston Lord, Kissinger’s special assistant, who says he read some of the cables. “In retrospect, he did a pretty good reporting job,” says Samuel Hoskinson, about Blood. “He was telling power in Washington what power in Washington didn’t want to hear.”” (73) Those reports were damning and provocative then, and form the skeleton of *The Blood Telegram*, in which Bass harnesses the momentum of the original cables (which were of course covered up subsequently by Nixon, Kissinger, and aides), and uses it to fuel a fresh

reflection not only on that period, but also on the effort to conceal it.

First describing the personal and political context (on the American side) that paved the way for Pakistan's brutal crackdown on East Pakistan, Bass explains the prejudices of Nixon and Kissinger against India (and its leader, Indira Gandhi) and the Bengali people, and suggests that those personal, emotional impressions made possible an excessively lax view on the consequential mass casualties and political upheaval that their involvement caused. The role of emotion in these political and military decisions is particularly interesting, and by telling the story in a way that is perceptive of the characters involved, and sensitive in their portrayals, Bass brings a rare emotional intelligence and insight into charting the escalation of violence. This perceptiveness in identifying the personal prejudices involved also adds weight to the assertion that the mass killings constituted a 'genocide', a term which obviously implies a racist motivation or undertone to the decision to kill hundreds of thousands of people (as opposed to 'mass killing', which need not have such motivation.)

As Bass points out, these personal prejudices were inappropriate given America's own political principles, not to mention the expected professionalism and lawfulness of its leaders; the contradiction betrays an interesting tension between the personalities in power and the structure and laws they were supposed to protect and promote. The pronounced conflict between Archer Blood and his staff, and their superiors in the White House is not only interesting as a thorough description of that pivotal moment in history, but also as a symbolic struggle between American principles and the preferences of particular leaders. In this case, of course, the dissenters were silenced. Despite Blood's reporting of the genocide, his linking of it to American sponsorship and weapons, and then his outright protest (together with other staff in the consul, via a "dissent cable" which explicitly spoke out against the "moral bankruptcy" of Nixon and Kissinger's policy), the genocide, and its American support, persisted.

Both Nixon and Kissinger flouted US law, knowingly, by allowing the transfer of American F-104 Starfighter jet interceptors to Pakistan, and rather than be deterred by Blood (et al)'s protestations, they were irritated by them, and only strengthened their military sponsorship in an attempt to hit India by proxy. The conflict also served as a cover for their clandestine communications with Mao Zedong's China, and Kissinger's trip there, to secure Chinese support against the Soviet Union (as well as further isolation of India). This type of struggle has repeated itself, on some level, many times over since. The use of proxy wars and parallel covert operations was hardly limited to the Cold War, let alone this particular period of it, and this exploration of these military behaviours has implications for more recent manifestations of the same tendency. In that sense, learning about this chapter in history is a useful tool for anyone interested in parallel issues in international relations since. As well as identifying a general pattern in US foreign policy, and its inherent problems, Bass also illuminates a time in American and global history that has had lasting implications, not least for the region itself, where the 1971 genocide only worsened relations between India and Pakistan, and goes some way to explain the complicated complicity, to this day, between the US and Pakistan.

Perhaps the most fascinating element of this story, however, is its previous concealment, and the subsequent uncovering that this book represents. Bass explains meticulously the efforts that Nixon and Kissinger went to in order to conceal their culpability in genocide, and to present, instead, images of themselves as good and law-abiding statesmen. The levels of manipulation and deception involved in that cover-up, not only by Nixon and Kissinger, but in their various aides and supporters,

is a compelling subject indeed. The gulf between real actions when in office, and reputation is pronounced here, and the ambitiousness required to attempt to gloss over that guilt and hypocrisy is quite astounding. Bass exposes an awful period of American foreign policy and personal ruthlessness, and in so doing leaves lingering some profound and timely questions and ambiguities concerning rogue leaders, illegal proxy wars and the heavy human price paid for underhand military coups. He also raises to prominence the (until now) silenced voices of dissent within the US foreign office, their principled struggle to act in accordance with American laws and ideals, and their personal sacrifices in doing so. *The Blood Telegram* is a brilliant account, therefore, of bravery as well as hypocrisy, and principles despite realpolitik.