THE VALIDITY OF DETERRENCE IN THE TWENTY-FIRST CENTURY

Peter Roberts and Andrew Hardie

Royal United Services Institute

OCCASIONAL PAPER
About the programme or study
This project is within the Sea Power Research programme. The broader research draws together practical and diverse experience, theory and academic discussion to promote innovative thinking about Sea Power. The authors are most grateful to King’s College London, Oxford University and the RUSI Associate Fellows network for their assistance in the construction of this paper.

About RUSI
The Royal United Services Institute is the UK’s leading independent think tank on international defence and security. Its mission is to be an analytical research-led global forum for informing, influencing and enhancing public debate on a safer and more stable world.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Annual membership subscriptions and donations are a key source of funding for the Institute; together with revenue from publications and conferences, RUSI has sustained its political independence for over 180 years.

RUSI is a registered charity (No. 210639).

For more information, please visit: www.rusi.org
The Validity of Deterrence in the Twenty-First Century

Peter Roberts and Andrew Hardie
## Contents

*Executive Summary*  
v

**Introduction**  
1

I. Theories of Deterrence  
3

II. How States Use Deterrence  
13

III. Israel Case Study  
27

IV. East Asia Case Study  
31

V. Conclusion  
35
Executive Summary

The last twenty-five years have seen rapid changes in the global balance of power, weapons proliferation and information technology. Governments and the general public have become interested in the rise of non-state actors, which have radically altered the paradigm of strategic-level decision-making. Recent events in Ukraine and, going back further, conflicts in Israel offer differing experiences on the relative failures of deterrence as a strategy. In contrast, deterrence has provided stability for Japan, South Korea and Taiwan – all of which rely on this concept to counter existential threats. Finally, there has been a marked change (particularly in the West) in decision-makers’ psychological understanding of deterrence. Part of this change is due to evolutionary sociological history; another part originates from the diminishing norm of non-intervention in the territory of other states – a central tenet of the Westphalian construct. All these factors point to the requirement to revalidate the key assumptions that influence ‘accepted’ doctrines for national defence and security.

Deterrence is the fundamental concept that currently underpins these doctrinal assumptions. The concept has a robust historical and scholarly literature associated with it, but has been called into doubt given recent failures in Western execution. Counter to this, some states – notably Russia and China – have employed military, diplomatic and economic deterrence extremely effectively for discretionary activities, while others continue to rely on the concept for existential reasons.

The aim of deterrence is to prevent certain actions by another actor – whether a leader, state, group or other body – from occurring. Deterrence can be considered as an act, or as a state, posture or structure. It is a philosophy that must be properly understood in order to be executed effectively within national-security policy or defence strategy.

The conduct of effective and successful deterrence is built upon the understanding that deterrence is focused on the mind of the adversary (the subject of deterrence), who must be made to believe that by whatever means, the deterrence posture of the other state is sufficient to deny the success of the adversary’s action. In essence, deterrence is the perception of denial of success for the subject of deterrence.

The actor that is subjected to deterrence is therefore crucial to the strategy’s success. While military deterrence is the area most often considered, there are also useful models of economic, diplomatic and law-enforcement deterrence that are available to states. The efficacy of each lever is not constant, however, and must be nuanced based on the threat in question. Judgements on rationality, desire, outcomes and culture are equally essential in assessing
which exact tools will change the balance of risk in the adversary’s mind. In this way, successful deterrence must be tailored towards the specific actor.

Such an approach is however highly specific, ignoring the broader utility of general deterrence, which may abrogate the need to consider threatening behaviour in the first place. Thus a national posture – which provides sufficiently broad deterrence combined with a measure of resilience and the acceptance that deterrence involves a degree of self-harm – has wider utility than deterrence conducted solely against an explicit threat.

A policy of deterrence, however, can lead to escalation. This can occur in qualitative, vertical or horizontal frames: an expansion of the conflict in scale, from strictly military actions into those with economic consequences, and across warfare domain or geographic boundaries. This has been a subject of renewed interest in the areas of cyber- and economic warfare. These types of warfare may have shorter timeframes for decision-making in any conflict. Indeed, such concerns have been exacerbated as states become increasingly concerned with violent non-state actors and groups not adhering to the Westphalian model in which deterrence has traditionally been employed. As governments try to understand what outcomes they want, what they want from other actors, and the risks involved in obtaining these, greater awareness of the limitations of deterrence, both generally and when conducted against a specific actor, is required. These are also important in conceptualising when not to act, especially in the case of being goaded into an action by another party.

Ignoring some or all of the points above can lead to a failure of deterrence. It is also significant that deterrence cannot occur ex post facto. The threat of punishment for an action may indeed be an essential element of a deterrent posture, but once deterrence has failed – or where the threat is existential – the rules change markedly. As soon as a state starts to punish an actor, it is no longer deterring the original act. Law-enforcement models often incorporate a counter to this logic, one that the Israeli government uses at a national level under a ‘rules-of-the-game’ doctrine. This approach responds with punishment when actors fail to adhere to deterrence red lines. After the initial response, the trigger for further action is usually set at a lower level. This, in turn, contributes to a wider deterrence posture for the state. By enforcing a will and intent to carry reprisals at disproportionate levels, future undesirable action can be avoided.

Deterrence has a long history. It remains as valid today as it was when practised by the Athenians and Spartans in the Peloponnesian Wars. Establishing a better understanding of the broad principles of when and how to apply it will reinforce its future utility.
Introduction

The Cold War generated renewed interest in the idea of deterrence, which became synonymous with ‘nuclear deterrence’. While the nuclear dimension is significant, it is only one part of an overarching theory spanning economic, diplomatic and military power. There has been much scholarly work on deterrence over the past decade, but much less consideration has been given to the concept in policy terms. However, recent events in Ukraine and Iran have – once again – brought the subject into the spotlight. This paper examines deterrence in the current world and draws on case studies to demonstrate how the concept applies in an evolving global order. It seeks to inform policy-makers as society enters a new geopolitical and strategic era in which many great-power relationships need to be re-evaluated. The balance of non-state and interstate activity will also change. Currently, this concept is linked to, and characterised by, the idea of ‘hybrid warfare’: traditional approaches to conflict being blended (mixing propaganda, terrorism, guerrilla activity and conventional military force).

Yet there is always a risk in drawing too many conclusions from recent events that could just be aberrations. Therefore, this paper draws on a wide array of examples to illustrate the continued efficacy of the concept of deterrence.

The UK is undertaking a major review of its National Security Strategy and government-spending plans during 2015; this will include a further assessment of defence and security requirements. The factors that inform these debates are based on a historical understanding and recognition of the validity of certain concepts, doctrines and strategies. Few of these have been reviewed outside academia to test whether they remain valid in the twenty-first century. With further expected reductions in UK defence spending, it is vital to consider deterrence – often seen as a cornerstone of both the British and NATO defence doctrines. Achieving national objectives while avoiding conventional conflict can save both lives and money.

This paper demonstrates why the future of deterrence must be at the forefront of security policy within NATO. It further identifies some of the key requirements for the concept to be applied successfully in the future. The Atlantic Alliance was designed primarily to draw states together after the Second World War with a military aim of deterring an attack from the Soviet Union. Deterrence, as a concept, therefore sits at the very heart of NATO, of which the UK is a vital member.

This paper also answers some key questions about the future of British deterrence policy. Why is it so important that the concept of deterrence remains a cornerstone of the National Security Strategy? How should the UK’s deterrence policy be changed and implemented to deal with powerful
and emerging threats? Can deterrence work against non-state actors? Is it possible to possess exclusively military or nuclear deterrence, without other capabilities? Are deterrence and resilience divergent objectives or are they mutually supportive? Does the changing threat landscape of, for example, cyber- and ballistic weapons radically change the deterrence dynamic, or is it a manageable transition for policy-makers?
I. Theories of Deterrence

As a military doctrine, deterrence has been used as a strategy for thousands of years – in antiquity, criminal punishment was perhaps more focused on retribution than discouragement, which occurred if there was a failure to deter the criminal act – and falls under a wider umbrella of coercion theory. Coercive diplomacy combines techniques of deterrence and compellence to elicit desired actions from targeted actors. Deterrence is usually defined as ‘Discourag[ing] [someone] from doing something by instilling doubt or fear of the consequences’.¹ It is therefore intended to pre-empt and prevent actions. Compellence, on the other hand, offers positive reinforcement to elicit desired actions from targeted actors. If an undesirable action has already taken place, the act of preventing further action, or encouraging a reversal of the decision, is termed as coercion.

The UK has a long experience with coercive deterrence theory, dating back over a century to ‘gunboat diplomacy’. This theory of coercion has been most thoroughly defined by James Cable in a series of works starting in 1971. He defined it as ‘the use or threat of limited naval force, otherwise than as an act of war, in order to secure advantage or to avert loss, either in the furtherance of an international dispute or else against foreign nationals within the territory or the jurisdiction of their own state’.² By strategically locating and manoeuvring naval power, a sufficiently powerful display of strength may coerce another state into acting in a desired manner, without the need to use force.

The concept of deterrence was brought to the fore during the Cold War and resulted in some of the first pieces of academic research in the late 1940s. Thomas Schelling is often attributed as being the father of coercion and deterrence theory and his books – The Strategy of Conflict and Arms and Influence – are often quoted as its founding documents.³ As an economist, Schelling understood bargaining and how it applied to military strategists. Schelling argued that states with greater military force could ignore those with smaller martial powers, as the latter did not have the capacity to inflict significant harm. While this may be true for bargaining with a rational state actor, successful deterrence in asymmetric warfare with seemingly irrational non-state actors requires more than overwhelming military strength.

---

Schelling highlights the ‘will to suffer’ as an important influence on bargaining ability. This is especially relevant today. Modern advances in air warfare and missile technology have added an extra dimension to the battlefield and now mean that anyone can potentially be targeted by military force. This does not apply solely to the battlefield; these advances can, in effect, make a state’s territory and citizens vulnerable at any time. Actors can no longer hide behind military defences. Symmetric warfare has moved from a contest of strength to a contest of endurance, risk-taking and calculated decisions. This type of warfare is analogised well by Michael Kinsley: 4

You’re standing at the edge of a cliff, chained by the ankle to someone else. You’ll be released, and one of you will get a large prize, as soon as the other gives in. How do you persuade the other guy to give in, when the only method at your disposal – threatening to push him off the cliff – would doom you both? Answer: You start dancing, closer and closer to the edge. That way, you don’t have to convince him that you would do something totally irrational: plunge him and yourself off the cliff. You just have to convince him that you are prepared to take a higher risk than he is of accidentally falling off the cliff. If you can do that, you win.

While game theory is a relevant part of deterrence, it is unpredictable both in its very construct and in practice. In reality, this type of deterrence can only apply between two actors with similar capabilities. In some respects, the Cold War is a practical example of this theory. It is incredibly difficult to implement in asymmetric conflict as one side has more to lose; portraying a willingness to take high levels of risk is therefore more difficult.

More recently, there has been widespread focus on violent non-state actors (VNSAs). An adversary whose leadership has no population to protect becomes difficult to threaten through conventional methods. For example, during the recent resurgence of violence in the Middle East, Daesh (also known as the Islamic State of Iraq and Syria, ISIS) seems to be an irrational adversary with which its opponents cannot bargain. This group, which has little regard for human life and no nation to defend, has become a serious problem requiring careful consideration.

Recent Russian actions in Ukraine also present an increasing deterrence problem for the West. The public became comfortable with Russia as an adversary during the Cold War, overtly increasing its nuclear stockpiles. The way Russia secured its initial objectives in Ukraine sits less comfortably with the West and has raised some difficult questions on deterrence. Despite having much weaker conventional forces than the West, Russia has used covert and ambiguous actions to plausibly deny involvement in the Ukrainian

crisis. Moscow’s approach has made NATO reluctant to overtly engage: its activities were managed so that they did not cross the Alliance’s deterrence threshold. Shadowy actions carried out by skilled special forces, coupled with Russia’s well-maintained nuclear capabilities and ambiguous nuclear-escalation doctrine, appear to have successfully deterred the West from doing anything but imposing sanctions.

The methodology which President Putin uses to make these territorial gains raises a difficult issue for the practice of deterrence: how is it possible to deter possible Russian agitation and subversion in, for example, the Baltic States, if undertaken in a similar, ‘deniable’ fashion?

Defining Deterrence

The military can use violence in two ways. Firstly, it can physically attack and destroy capabilities through brute force, rendering the adversary physically unable to compete. Secondly, it can coerce an opponent by influencing his decision in the cognitive domain. Almost all conflicts end in the cognitive realm and occur when a leader concedes defeat, realising that continuing is futile. These concessions may be linked to the physical domain. For instance, a physical victory may result in adversaries withdrawing; in turn this discourages leaders from continuing to fight. Ideally, all conflicts would be settled without the need to apply force, as the financial and human costs are less. However, this is not the only possible end to a crisis: an escalation to physical actions is the clear alternative.

Since the end of the Cold War, the West has preferred to address crises with methods other than pure physical force. To be victorious in the cognitive domain, one must successfully coerce and deter opponents; however, it is relatively more difficult to predict the outcome compared to physical conflict. Successful coercion and deterrence require prevailing capability coupled with appropriate signalling and credibility. These facets are crucial in terms of maintaining the strategic initiative. The actor must actively shape its coercion and deterrence strategy, rather than merely reacting to strategies of adversaries.

Even if deterrence fails, coercion is practiced in parallel to combat. This aims to prevent the conflict from escalating in terms of its geography, scale or intensity, or to stop it from spilling into other domains, such as the economic. At its core, deterrence is designed to avoid conflict and is intended to operate purely in the cognitive domain. However, it is important to understand that it can also operate alongside the physical domain in order to manage escalation.
Edward Luttwak’s work *The Political Uses of Sea Power* expands on James Cable’s notion of gunboat diplomacy explored earlier. Luttwak categorises deterrence under the broader topic of suasion. His classifications of suasion can be seen in Figure 1.

**Figure 1:** Luttwak’s Classifications of Suasion.

![Image of Luttwak's Classifications of Suasion](source)

In terms of deliberate actions, coercion is split into negative and positive subsets: deterrence and compellence. Deterrence dissuades an actor from doing what he wishes to do (through the anticipated negative consequences of a response, or failure to do something). Compellence persuades an actor to carry out an action he otherwise would not (through an actual response which raises the costs of his decision). Deterrence also falls under the latent, undirected, branch. In this case, a target is not specifically chosen; rather, the action of a player signals his capabilities to other actors more generally. This type of deterrence is described by various terms such as ‘general’ or ‘inherent’. This builds on Cable’s idea of gunboat diplomacy, as he only accounts for deliberate action and does not include latent effects.

In 1995, the first edition of the UK’s strategic maritime doctrine strived to combine the theories of Cable and Luttwak, highlighting three main concepts: coercion; symbolic and preventive deterrence; and precautionary and pre-emptive activities. In this case, coercion combines both deterrence and compellence, allowing for the limited use of violence. Symbolic actions

---

do not have to be directed at a specific actor: they can compel or deter, and require military deployment without any use of force. Preventive, precautionary and pre-emptive acts do not fall under a specified mission but display a readiness for involvement in achieving various objectives. These are not intended to be directed or symbolic, but may influence the decisions of other leaders. For example, the presence of a continuous at-sea deterrent is not directed against an individual state; it is rather a statement of national intent and resolve.

The power of armed suasion (or inducement) can also be separated into three categories: symbolic; robust; and limited violence. Symbolic armed suasion involves a display of capability that is too modest to involve violence, such as the UK naval presence in the Gulf in the 1960s. Robust displays may lead to some violence but this is not the intended result. An example of this category is the garrison of the Falkland Islands. Finally, limited violence constitutes an armed inducement that uses minor instances of violence to deter or compel. The UK and US presence in the Straits of Hormuz during the Tanker War in the 1980s exemplifies this type of armed suasion.

Armed suasion is not always designed to have a serious deterring effect on potential adversaries. In many cases, shows of strength in strategic locations are more geared towards supporting third parties or to send a message to a domestic audience. It can be argued that an adversary likely already knows whether a deterring state is capable of deploying and retaliating effectively, which may mean that such displays do not markedly contribute to improving general deterrence. Yet they still increase one’s sphere of influence which may compel allies, bolster relationships and maintain the public’s faith in its country’s armed forces.

It is also important to note that latent suasion can quickly collapse and result in active suasion. As an example, the nuclear, continuous at-sea deterrent is only intended for latent suasion, with no active objective. However, if required it can be readied and a target can be specified quickly, becoming a form of active coercion. While the above terms were created for naval application, they can also be appropriately applied to land, air and cyberspace doctrines. Indeed some modern, conventional military capabilities have an impact across functional warfare domains and provide national deterrence and resilience themselves. The possession of a deployable ballistic-missile defence system, for example, provides for resilience as well as deterrence in both the active and latent senses. These systems permit greater freedom of action for countries that would otherwise be subject to threatening behaviour.

Deterrence can be defined as a policy designed to dissuade an actor from carrying out a certain intended course of action. Schelling highlights that the ability to hurt another state could be used as a motivating factor to influence
its decisions and behaviour. The potential to harm (for instance with military strikes, economic sanctions and embargoes) can be used as a bargaining chip to influence the actions of others. If the costs that a state would incur outweigh the benefits of following a certain course of action, it is unlikely to carry out its plan. However, the state needs to know that it would not incur these costs if the action were not taken. This technique can be applied to protect home soil against adversaries; this is known as immediate deterrence. The US activity during the Cuban Missile Crisis is normally cited as a classic example of this concept. Alternatively, it can be adopted to protect a third party, which is known as extended deterrence. The US nuclear umbrella covering Japan, Taiwan and South Korea is an example of this. The ability to do this successfully is generally restricted to powerful states.

Successful deterrence requires a number of elements. For state A to successfully deter state B, state B must know that state A has the following:

- The capabilities required to harm state B
- The will to launch a credible reprisal and the reputation that it would
- Knowledge of what will cause state B such losses as to deter it in the first place
- The resolve to accept any harm to it that may be caused by a reprisal act in response to the original deterrent act.

If it is known that a state has all the capabilities required to damage another, but lacks the will to go through with retaliation, deterrence fails. Furthermore, if it has the capability and the will to retaliate, but would retaliate by targeting something that is of little worth to the aggressor, deterrence again fails. As mentioned above, it is important that the aggressor knows that it will not incur costs if a planned action is avoided. If a country thinks it is going to be attacked anyway, such as Japan in 1941, then it may attack in order to reduce its losses, even if it loses more than it gains. Tied into this is the importance that the threatened retaliation is credible and commensurate. If the threat is not credible and is in fact disproportionate, it may not have the validity required to produce the desired effect. The UK, for instance, did not drop nuclear weapons in response to an Argentine invasion of the Falkland Islands in 1982.

Even if a state has the capability, will and knowledge to retaliate effectively, it must communicate its position. Unless others receive the message clearly, they will not fully comprehend the repercussions of potential actions. If these are not understood, their actions may result in unforeseen and calamitous results. Therefore, effective signalling is fundamental for successful

deterrence. It is often poor communication and misunderstanding that lead to its breakdown.

While procuring credible capability can take decades, the will to retaliate can change overnight. This makes deterrence risky, as aggressors must believe that the defending state satisfies the four points made above. If this will erodes, and the credibility and reputation of a deterring state dwindle, it may require greater retaliation to rebuild credibility and reintroduce the belief of other actors that the deterrer will not tolerate infringements against them.

Specific or directed deterrence is normally aimed at the leadership of a state or organisation. Leaders often cannot personally back down from activities that have triggered deterrence action without enduring domestic political cost and embarrassment. The deterring party may need to make provisions for the deterred actor to climb down in order to prevent unintended escalation. The US government often provides the Chinese leadership with an ‘off-ramp’ for it to use when it has taken actions and decisions without realising that these would trigger a higher level of deterrence than had been expected. In these instances, focusing deterrence on the support base of a particular leader may be a more effective approach. Successful deterrence can reduce a leader’s support and force certain decisions that might as such be favourable to the deterrer. However, if not correctly implemented, this can produce undesirable results – such as the nation rallying behind its leader. A population may feel more united and buoy the leadership with public support as a result of coercive attempts by external actors.

Moral and legal concerns are another important aspect of the application of deterrence. The perceived legitimacy of actions can win or lose the support of not only the domestic population, but also of other states, which may be potential allies. If a friend or ally views acts of deterrence as immoral or illegal, it will most likely not support coercive techniques, subtracting from the overall power of the deterring party.

As noted, deterrence lies in the cognitive domain, where likely results are more difficult to predict than those occurring in its physical equivalent. It cannot be assumed that strategic decisions can be based on a rationally predicted outcome of a cognitive process – there are simply too many variables involved to successfully engineer a precise solution. Instead, it is essential to develop plans that do not involve such complex calculations or, at least, produce contingency plans whenever the cognitive domain is involved. Even though outcomes vary and deterrence is not an exact science, future actions can sometimes be successfully predicted; military strategists can reap huge benefits from correctly forecasting the outcome of deterrence. To generate meaningful predictions it is vital that the number of unknown variables is reduced to a minimum from the outset.
It is therefore imperative to study and understand the beliefs, culture and objectives of an adversary, as this will lead to clearer insights into the most effective deterring methods. Each situation is unique; a strategy may deter one adversary but may be completely ineffective against another. Success lies in understanding which practices can be put in place to deter a specific target. However, it cannot always be anticipated where the next threat will come from or which group to target specifically. Accordingly, to protect against potential threats, general or inherent deterrence becomes important. In this way, a state may display to all actors that it has sufficient capability and will to respond to any threat. These displays need to be credible – simply displaying a large standing force on its own may not deter infringements by allies or may not work in areas of interest far abroad.

**Criticism of Deterrence Models**

There are critics of the concept of deterrence. Richard Lebow and Janice Stein brand contemporary deterrence theories as ‘poor predictors of critical cases of strategic behaviour and equally poor guides to policy’. Their chief grievance is that modern-day deterrence is based on an assumption of calculable rational actors. Even ignoring irrational parties, they claim that rational thinking cannot be predicted – and behavioural scientists have provided some evidence for this. Some actors may strive to minimise losses while others may try to maximise gains. Therefore, rationality must encompass both the risk-seeking and risk-averse. Lebow and Stein argue that current models of deterrence assume an initiating adversary who is risk-prone and exclusively wishes to maximise his gains. However, in reality, serious challenges come from initiators who are also risk-prone but focus on minimising loss. This group of aggressors, such as the Japanese leadership during the Second World War and Egyptian President Anwar Al-Sadat in 1973, complicates the understanding of how actors approach the cost-benefit calculation. In both highlighted situations – the sneak attacks of Pearl Harbor and the Yom Kippur War – the initiator expected the cost of war to be very high, the probability of emerging victorious as slim and the probability of retaliation as certain. In the case of Al-Sadat, the political consequences of continuing inaction over the Sinai Peninsula were perceived to be too great to endure. Hence, despite Israel’s stronger military forces, he initiated conflict with Israel, as he could not abide the potential consequences of inaction.

This indicates that it is not always possible to know what actions ‘rational thinking’ will lead to: what may be rational to one party may not be to another. Therefore, for deterrence to work, both parties must hold the same rational beliefs; yet this is not always the case, which can lead to complex relationships in which interests are not always compatible. Deterrence is

---

therefore a relationship between parties, not just a one-way decision. Critics of deterrence point out that political leaders assume that their opponent follows a broadly similar rational outlook as theirs, leading to potentially false assumptions based on purely subjective decision-making paradigms. Indeed, the construct of such decision-making problems cannot negate the fact that elements of such actions are prone to be instinctive and these can never be controlled or predicted in a rational manner.

Lebow and Stein further argue that deterrence is not suitable as a stand-alone policy and should be incorporated into a broader strategy of foreign policy.\(^9\) Further strategies should be incorporated to improve the basic assumptions of the cost-benefit calculus as a value proposition; the aim is to consider the entirety of the problem rather than only those elements that are directly impacted or are financially measurable. The authors explain that instead of using a credible threat, foreign policy should build on using reassurance to reduce the appeal of, and need for, force. This approach is very much an element of contemporary US foreign policy towards Iran and China – the military presence in their regions is countered and supported by a political dialogue which seeks to reassure those states that the presence of US forces is not a threat in itself, but merely an effort to stabilise the region.

In addition, the thought processes of adversaries may be unpredictable, both in general and with reference to a specific act of deterrence. The concept of deterrence is founded upon the notion that a certain act or threat will change the view of the target: that is, elicit a favourable response. However, the direction of change is uncertain. For example, the Cuban Missile Crisis was triggered by the Soviet response to the deployment of US missiles in Turkey and Italy which threatened the USSR; instead of deterring the Soviet leadership, it incited the USSR to deploy nuclear weapons just 100 miles off the coast of Florida.

A final critique made by Lebow and Stein is that for deterrence to work there must be a clear challenger and defender.\(^10\) This is often open to interpretation – both scholars and the actors themselves may not know who plays which role. Often, both parties will perceive themselves as the defender. Again, the crisis between Egypt and Israel in 1967 can be viewed through this prism. Egypt had grievances with Israel since losing the Sinai Peninsula and therefore believed that it was rightfully defending its territory. Israel saw Egypt’s campaign as a hostile attack on Israeli territory against which it had to defend itself. Likewise, during the Cuban Missile Crisis, each side perceived itself as a defender. In the western Pacific, either China or the US could be the defender.

---

This ambiguity could lead to either side misinterpreting the actions of the other as being aggressive rather than defensive. This makes it challenging to pinpoint examples of when deterrence has failed or succeeded, and can also break a model that in some ways relies on the understanding that each party has very specific roles. This single critique could be used to undermine deterrence policy, but importantly there is little evidence that perceptions are a significant driver in the dynamic of deterrence or in preventing action, specifically perceptions about who is the attacker and who the defender.
II. How States Use Deterrence

Deterrence works best between rational actors who have a mutual understanding of the status quo and who, to some extent, understand each other’s motives. In this context, deterrence by denial or retaliation is effective. Politically, deterrence is therefore perceived as an attractive policy option: it is believed to have a track record of success while helping to reassure one’s own population and allies.

This does not mean deterrence is solely passive in nature. The modern security relationship between Russia and China is, in effect, one of deterrence based on geography, national policy, military posture and historical precedent. However, it was established only after the Soviet naval action in the vicinity of Zhenbao Island in March 1969, during which the Chinese received a bloody nose and reset their relationship with the then USSR. It could be argued that this alone stabilised the land border and formed the basis for political dialogue. The understanding that Russian decision-makers had of the thought processes of the Chinese leadership and their appreciation of China’s red lines was critical in Moscow’s assessment of how to act. It was a very well-calculated risk which was part of a wider deterrence strategy.1

Some have called for a ‘ladder of escalation’ to provide a handrail for decision-makers: a guide that would conceptualise how activities within a given scenario relate to broader deterrence.2 Reaction and deterrence can become more integrated with policy if there are clearly-set guidelines. Outlining a promised response may also help to deter adversaries. The danger of this policy, however, lies in its predictability. If potential aggressors know a defender’s rules, they can test boundaries and assess the resolve to climb the ladder. Ladders of escalation also relate to disproportionate responses: one cannot reset acceptable behaviour without responding disproportionately. If this response is promised in a ladder of escalation, credibility becomes very important. While there is no way to feasibly adopt a strict ladder-of-escalation model today, a very general, conceptual framework could assist decision-makers. However, the usefulness of such a general outline is questionable given the uniqueness of each scenario. A ladder of escalation cannot account for individual circumstances and predetermined sets of rules can thus not be used; some degree of ambiguity and unpredictability must be at the heart of a pragmatic and successful deterrence policy.

Economic and Diplomatic Deterrence Options

While deterrence and compellence have been discussed as military strategies, the concept can be applied outside of the military sphere, to

---

include economic or diplomatic actions. A country may impose economic sanctions to harm a state financially. In the diplomatic sphere, a state may curtail or sever relations with another, which can affect previous agreements as well as public opinion, especially if the deterring state is a major power or a state with which a relationship offers great benefits. A recent example is China’s refusal to engage politically with Norway after the award of the Nobel Peace Prize to Chinese dissident Liu Xiaobo in 2010. While the Chinese government gains from this action directly, it offers a compelling statement to other states who wish to maintain relations with China. It is an excellent modern example of diplomatic deterrence.

A combination of political and economic deterrence strategies can prove effective and achieve tangible results without the need to resort to violence. Recently, such actions have become more prominent in response to original acts of deterrence, for example relating to Iran’s nuclear-development programme.

In the economic domain, sanctions have had mixed success. In increasingly liberalised nations, economic sanctions have become popular tools, but the impact of their imposition has not always been predictable. More recent examples include the 2014 Ukrainian crisis and Russian deterrence of the West.

**The 2014 Ukrainian Crisis**

Russia has recently been subject to numerous economic sanctions after the illegal annexation of Crimea. Many argue that the use of sanctions post hoc was an approach doomed from the start and, because of the sequencing, was not, in fact, deterrence. Yet the aim of imposing sanctions has been to deter further escalation of the conflict. It is more likely that the failure of decision-makers to understand the target was the critical factor in undermining the impact of economic deterrence, along with the fact that external states have been unwilling to share in the discomfort of imposing such measures. There is little evidence that these economic sanctions had any impact on decision-making in Russia. The more challenging economic conditions felt in Russia have arguably been caused by the huge reductions in the price of wholesale oil rather than by the limited sanctions imposed against Russian oligarchs.

Yet with the West unwilling to intervene militarily, sanctions have been the only option. They were initially threatened in the hope that Putin would

change course without actually having to enact them. They were then imposed to signal that more would follow should Moscow advance further. Although sanctions were not intended to cripple Russia, with Putin not altering his stance and the concurrent development of price declines in Russia’s chief export product – oil – they now have an impact on the Russian economy. The World Bank revised Russia’s economic growth rate to near zero for 2015, falling from an early estimate of 1.1 per cent, and with a negative forecast for 2016. Russian banks and companies have been frozen out of traditional markets, upon which they rely heavily for credit access. Sanctions on oil projects have affected Arctic oil exploration as the Russian energy industry depends on foreign experience and expertise to successfully discover and exploit new fields. However, Moscow knows that these sanctions also hurt Western companies.

Thus far, economic sanctions have not persuaded Putin to withdraw from interfering in the Ukrainian crisis. This is partly a result of the West’s misunderstanding and underestimation of the Russian government’s conception of the role Ukraine plays in its security. So, while sanctions may cause serious problems, Russia sees the prospect of a democratic, pro-EU and pro-NATO country on its border as a bigger threat. Given Putin’s strong personal power as president, his close group of the ruling elite in both business and politics and the reality of politics in Moscow, sanctions may be less effective on Russia than elsewhere. Russia harbours a strong nationalist sentiment, bolstered by the recent annexation of Crimea. The media is closely controlled and manipulated, and has appealed to constituencies which believe that Russia is a strong power that should stand up to an interfering and hypocritical West. Control of the media allows Russia to favourably spin any economic downturn as resulting from sanctions and blame the West for the population’s hardship. This ‘rally round the flag’ effect may mean the population can endure even harsher economic punishment if necessary, as it believes this hardship is a symbol of Russian steadfastness. In sum, Putin has now engineered a situation in which the government cannot be blamed for declining standards of living.

It is nevertheless possible to argue that these sanctions have demonstrated the EU’s resolve and willingness to itself suffer an economic impact in order to deter Russia. Such arguments assume that Moscow will interpret this suffering as a will or resolve that can be applied to other domains: if Europe will take actions detrimental to its economic wellbeing, then Russia may believe it to be willing to do the same in the military domain. Although Europe knows that heavy losses would occur in a conflict with Russia, it has shown its willingness to suffer. Such sacrifices may have made it more difficult for Putin to take Moscow further down the path of aggression.

It is also important to consider how much the sanctions imposed have, in fact, harmed the West. While widely accepted that the current sanctions will have a greater impact on Russia, so far these measures have indeed done little damage to Europe’s economy. European leaders have carefully attempted to balance an EU demonstration of resolve with a marginal impact on the Eurozone’s overall economic wellbeing – with the provision that mitigation is achievable. For example, Russia’s retaliatory ban on EU fruit and vegetable imports has reportedly cost the EU €125 million in compensation to the agriculture industry. Considering that Russia predicted the ban would cost the EU €12 billion, the result was far less considerable. This may change in 2015, but if the economic damage is tolerable to both Europe and Russia, this factor becomes immaterial in a decision-making paradigm and irrelevant to any deterrence calculation. In either case, history shows that economic sanctions for deterrence take longer to change the situation unless the measures are extreme (see, for example, the British government’s model of unrestricted economic warfare of 1913–14).

The Ukrainian case study draws out a key facet of deterrence behaviour: the deterring state must be willing to both inflict and suffer the consequences of punishment (and its threat), unless it possesses systems that provide mitigation. This is also true in militarised deterrence strategies.

**Russian Deterrence of the West**

It is worth considering the deterrence situation from the other side of the conflict. The West could not compel Putin to withdraw Russian troops from Crimea. Beyond the promise of economic sanctions and strong words, there is little the UK can feasibly do to change Putin’s plans. In April 2014, Putin stated on national television that there were Russian troops in Crimea, with tens of thousands waiting just across the border. Yet the West has made no move to use or threaten force. Russia’s plausible deniability has offered the West a curtain to hide behind to avoid having to make a serious physical response. There have been ample opportunities for a response beyond the conflict in Ukraine; provocations include the recent (suspected) Russian submarine spotted in Swedish waters and Russian aircraft impinging on NATO airspace. Despite all these testing actions, the West has mustered little action against the Kremlin.

In 2013, Russia had 766,000 active military personnel with a further 2 million in the reserves. Apart from the US, this dwarfs the militaries of NATO members. Discounting the readiness, training and operational effectiveness


of the majority of Russian forces, this mass is an imposing problem for
continental Europe – the existence of those forces is thus a deterrent in
itself. Yet the way in which such forces have been used – to conduct and
orchestrate political outcomes below the threshold of a deterrence response –
is actually the issue for the Alliance. Unless NATO is willing to lower the
threshold for which it will respond to Russian aggression in military terms, its
deterrence position will be continually weakened.

While Russia also remains a nuclear power, the threat of nuclear escalation
over Ukraine has remained ambiguous. There is a rational assumption that
Putin would not use nuclear weapons in a conflict over Ukraine; however,
Russia’s nuclear capability may have been enough to produce a restrained
response from the EU and the US. Putin knows Russia no longer has the
same conventional power that it had as part of the Soviet Union. In the past,
Moscow could present a serious threat to any capital in Europe. It no longer
has this capability and hence the ambiguous nature of the nuclear threat has
played an effective part in deterring the West.

The legacy of the Cold War and the devastation that was avoided in the
twentieth century are still fresh in the mind of decision-makers who will
do all they can to avoid a repeat of nuclear tensions. Putin also knows that
the West is fatigued after over a decade of fighting wars in the Middle East,
which has taken its toll on NATO armed forces. Equipment is worn down
from long use and personnel are weary from multiple missions. The public –
especially in the UK – has also tired of recent campaigns and there is virtually
no chance of public support for freeing Crimea, wider engagement in Ukraine
or potentially even the Baltic. This might well be more a case of Western
war weariness, but it does have an impact on the deterrence equation:
when policy- and decision-makers have less confidence in the military lever
of power to deliver results, there is less inclination to be vocal about its
utility – thus undermining deterrence policy and posture as a whole. Putin
has vocally reinforced Russian might to communicate that NATO should not
confront him. ‘I want to remind [the West] that Russia is one of the most
powerful nuclear nations’, the Russian president said in August 2014. ‘This
is a reality, not just words’. He went on: ‘We must always be ready to repel
any aggression against Russia and [potential enemies] should be aware ... it
is better not to come against Russia as regards a possible armed conflict.’

Despite the many reasons why the West does not wish to militarily confront
Russia, such a confrontation could still occur. Putin has correctly deduced
that the West does not value Crimea enough to become physically involved
and has used this to his advantage. However, if he continues his policy of

---

8. Comments made by Russian President Vladimir Putin on 29 August 2014. See, among
others, Greg Botelho and Laura Smith-Spark, ‘Putin: You Better not Come after a
Nuclear-Armed Russia’, CNN, 30 August 2014.
‘protection of Russian ethnic minorities’ into NATO’s Baltic member states, Russian deterrence may not be sufficient to prevent a military NATO response.

**Nuclear Deterrence, Proliferation and Rogue States**

There is a relationship between nuclear and conventional capabilities in deterrence theory and practice. Practically, for states fielding both capabilities, nuclear and conventional assets can complement each other within an overall deterrence policy. Deterrence theory accepts that they are mutually supportive concepts across the spectrum of suasion against conventional state actors. Yet these assumptions are being questioned: the rise of rogue states and non-state actors who desire nuclear capabilities, and the narrative of weapons proliferation both in terms of scale and effect, represent a challenge to deterrence theorists.

Even though nuclear stockpiles have reduced since the end of the Cold War, Russia and the US still retain close to 8,000 warheads each, and China, France, India, Israel and Pakistan have stockpiles, albeit in significantly smaller numbers. Yet proliferation of weapons remains a risk at the forefront of national-security strategies across the world. North Korea’s few warheads could still pose catastrophic consequences to the global order and Iran will have a capability to strike further into NATO-state territory over the coming five years through ballistic-missile programmes. The greatest risk however currently appears to come from proliferation of such weapons to other rogue states or actors. The desire of Islamic fundamentalist groups to obtain such capabilities is well known inside the defence and security community, while the sale of such capabilities to, for example, Syria would cause significant problems for Western decision-makers.

Those who counter the claims over ever-increasing proliferation and risk state that these arguments make rational and logical leaps that are hard to substantiate. There is little evidence that nuclear powers would sell such weapons: the circumstances under which, for example, Iran would provide a nuclear ballistic missile to Hamas or Hizbullah are highly complex. Similarly, it is hard to predict whether, how and when theft or use of nuclear weapons by less technically-advanced actors or states is possible. As a result, Western decision-makers are almost unable to foresee any scenario in which they would authorise the use of nuclear weapons, including the case of so-called rogue states.

Tom Nichols, professor of National Security Affairs at the Naval War College, argues that nuclear deterrence is hollow against rogue states and that the only way to deter these is to promise the West ‘will precipitate major conventional war with the explicit goal of regime change and the apprehension or death
of the enemy leadership’. Nichols states that regimes controlling rogue states do not care for their people, but merely for their own survival and the control they hold over the state. When the subject of deterrence does not act according to a rational methodology understood by Western actors, Western norms about nuclear-deterrence actions are relatively useless. Nichols claims that the failure of nuclear deterrence against Saddam Hussein and Muammar Qadhafi are prime examples of the limitations of deterrence in relation to rogue states. Yet Nichols’s argument relies on assumptions of reductionism both in terms of behaviour and rationality. Will all rogue leaders behave and respond in the same way as Hussein and Qadhafi did to nuclear deterrence? Is it really feasible to state that the only method of countering a rogue state is regime change and that nuclear or conventional deterrence has no role? Recent experiences in Libya, Iraq and Afghanistan where the decision-makers responded very differently to deterrence actions after 2001 – namely with the use of military force – show that this argument is flawed.

The Relationship between Nuclear and Conventional Deterrence: India and Pakistan

It is often argued that conventional conflict between two nuclear-armed states would escalate to nuclear exchange. Likewise, if a nuclear-armed state has conventional superiority in a competitive relationship with another nuclear-armed state, nuclear deterrence may be appealing for the weaker country. Such a situation exists between India and Pakistan. Due to its weaker conventional forces, nuclear deterrence plays a crucial role in Pakistani foreign policy. India can call upon greater conventional power, outnumbering Pakistan, for example, by 2:1 in fighter jets and 1.7:1 in main battle tanks. This unfavourable force ratio provides a major motivation for Pakistan to keep nuclear response a viable option.

During the Kargil border dispute of 1998–99, the massive Indian conventional response to Pakistan’s occupation of border posts in Kashmir ended without any Pakistani gains and heavy military losses. While both states had declared themselves nuclear powers shortly before the outbreak of hostilities, neither could face the potential consequences of using them. This added weight to the presumptions of nuclear-deterrence theory which expects a balanced nuclear relationship to reduce the risk of the conflict escalating to a nuclear one. The conflict however also raised the paradox of nuclear forces bringing about instability. Some have mooted that Pakistan was encouraged into


10. For a full discussion of this topic and further reading, see E Sridharan (ed.), *The India-Pakistan Nuclear Relationship: Theories of Deterrence and International Relations* (New Delhi: Routledge, 2007); Zafar N Jaspal, ‘Paradox of Deterrence: India-Pakistan Strategic Relations’, *Strategic Studies* (Vol. 19, No. 4, 2009).
action in Kargil by the reassurance that its possession of nuclear weapons could deter India from invading its sovereign territory.\footnote{George Perkovich, ‘Options Available to the United States to Counter a Nuclear Iran’, testimony before the US House Armed Services Committee, 1 February 2006.}

The tension between India and Pakistan highlights another limitation of conventional deterrence. While it is easy to signal unacceptable costs with a nuclear deterrent, such costs are much more difficult to judge with conventional forces. Even though India’s forces outnumber Pakistan’s by around 2:1, its advantage is not enough to guarantee a victory. This inherent uncertainty can make conventional deterrence an unreliable policy and may lack the certainty of nuclear means. It is often tempting to extend this example to Southeast Asia, but the strategic culture and decision-making paradigms are sufficiently different to make direct comparison dubious at best.

The relevance of a balanced – nuclear and conventional – military force retains primacy in deterrence for military strategies. In many contexts, nuclear capability is required to back-stop conventional deterrence; but that may not be its only role.

**Deterrence by Denial**

One of the key elements of deterrence is changing the cost-benefit calculation of a threatening opponent. Credibly signalling – or proving – that an aggressive act will fail by building and demonstrating sufficient defence or resilience to resist aggression will deter an attack. Ballistic-missile defence is a good example of how this kind of capability changes the calculation in both financial and psychological terms. These considerations are likely to become more important in the future as the proliferation, speed and reach of weapons increases.

While deterrence is ultimately a cognitive state, it is possible to construct physical defences to deter aggression by others. The Maginot Line, for example, was built to protect the Franco-German border after the First World War. This extensive set of defences was designed to physically prevent German aggression. Ultimately it failed as the Germans invaded regardless by bypassing the line through the Ardennes forest. However, the strategic positioning of capabilities can offer a more mobile form of deterrence, and this less rigid approach might be an area of significant development in the twenty-first century as resilience, behaviours and changes in risk appetite become more obvious in relation to, for example, cyber-deterrence. There are some precedents for adopting the more fluid approach of deterrence by denial, such as the Israeli security barrier.
Cyber-Deterrence
As the world has become more interconnected by telecommunications, cyber-warfare has added an extra dimension to modern conflict. Cyber-deterrence requires a different approach from traditional methods due to its completely different nature. Cyber-warfare can affect the physical and digital domains while being covert, instantaneous and having few geographical constraints. The low barriers to enter cyberspace open opportunities to anyone. Unlike military capabilities that may only be procured by states or powerful non-state actors, cyber-capabilities are readily available to almost everyone. Some arguments suggest that non-state actors, for example, lack the intelligence capability which could expose weaknesses in a target network most likely to yield the desired impact. However, groups such as Anonymous have still achieved significant disruption at a national level.

It is important in the cyber-domain that critical national infrastructure is protected by strong defence. Maintaining effective barriers prevents many potential intruders from even attempting aggression and the majority of attacks can be repelled immediately. Ensuring this is done properly leaves a much smaller number of penetrative attacks to be traced and addressed.

When these intrusions into the system occur, they pose the problem of attribution – one of the major difficulties in successfully implementing cyber-deterrence. The anonymity provided by the cyber-arena makes it difficult to accurately trace an attack back to the perpetrator. Without knowledge of who has initiated an attack, how can one successfully retaliate and deter? Further, the low barriers to entry mean the work can be outsourced, meaning it is not enough to simply trace the attack back to a single computer. Rather, it is important to uncover a political actor, if there is one, so that it can be effectively deterred. In 2012 then-US Secretary of Defense Leon Panetta stated that ‘Potential aggressors should be aware that the US has the capacity to locate [attackers] and to hold them accountable for their actions that may try to harm America’.

The statement itself is an act of deterrence, attempting to signal that cyber-attacks against the US would be counterproductive. These words appeared even more credible as North Korean internet connectivity was severed immediately after a US presidential statement on unacceptable behaviour by Pyongyang in its attack on Sony Pictures in January 2015.


If it is possible to trace an attack, the next step may be to retaliate in some way. As with conventional deterrence, it must be decided what force and form the retaliation will take. A 2013 report by the US Defense Science Board highlighted that retaliation can extend beyond the cyber-domain – known as horizontal escalation. It may be effective to impose economic sanctions, undertake diplomatic and political actions or even use military force. Even if it is not possible to attribute an attack to a political actor, repercussions on the host state may force it to better police its population’s cyber-actions and prevent reoccurrences.

For deterrence to be effective, responses must be clearly demonstrated. Retaliation in the physical world is often very overt: if a state is attacked by missiles or soldiers, it is fairly evident. However, responding with a piece of malware can be much more subtle. It is therefore important that the message – that a cyber-attack is being carried out as a result of past actions – is relayed clearly. If the response is silent then it may not be attributed to the deterring power and deterrence cannot be upheld. Obtaining data on activities in the cyber-domain is difficult and many cases remain highly classified; the overt events that transpired in 2014 between the US and North Korea form a useful exception. While neither the attack on Sony Pictures nor the response to North Korea has been attributable to either state in an unclassified way, the actions taken clearly relate to messaging specific target audiences in the cyber-domain and have been widely interpreted as a statement of national intent and capability.

The difficulty of forensic attribution – with the aim to provide specific and irrefutable evidence of the originator of an attack – has previously been used to explain why deterrence in the cyber-domain is extremely complex and challenging. In this regard, there are similarities to the actions of non-state actors in the physical domain with whom it is difficult to associate specific acts. Responses to cyber-attacks are not impossible; they are merely more difficult and nuanced compared with state-based deterrence activities. In addressing this challenge, established legal frameworks and norms require a broader understanding of what may be the rational or irrational, and what may be proportionate and disproportionate, responses than currently exists. However, it must be acknowledged that by admitting a belief in the impossibility of cyber-deterrence, one invites a first strike in this sphere – a nonsensical and illogical position for a country in which to place itself.


An adequate cyber-response can still be executed without forensic attribution of the attacker; this may perhaps become more important in the future. A cyber-response does, however, require a greater appetite for risk than Western powers currently demonstrate and runs counter to contemporary British ethical and moral responses. The liberal, Western idealism of actors across Europe appears to seek less harsh, more refined military, economic and diplomatic reactions; cyber-responses are, in reality, exceptionally blunt tools. Avoiding drastic action and conducting only limited and nuanced activities – particularly when it is not possible to prove, legally, the identity of the attacker beyond doubt – can undermine broader deterrence postures. From the limited evidence available at lower levels of classification, a pattern may be emerging that, as with nuclear and conventional arms, deliberate and disproportionate cyber-responses support broader deterrence postures in a more effective manner.

Despite the challenges of cyber-deterrence, there is no evidence yet of a large-scale cyber-offensive that has cost lives or crippled infrastructure. Denial-of-service attacks – which overload a network to a point where it cannot cope with the traffic, causing inconvenience or disruption – are fairly common. An example of this kind of attack was the Russian state-sponsored attack on Estonia in 2007. Even the Stuxnet attack against Iranian nuclear facilities in 2010 – one of the most advanced cyber-attacks ever seen – caused fairly limited damage and was very specific in its intended purpose. This is not to say that a serious cyber-event will not occur. However, there seems to be an acceptable ceiling to cyber-warfare – most incidents are intrusions aimed at stealing information. These have been within the acceptable threshold that has not precipitated a serious response. One main reason may be that all cyber-powers rely on the same internet infrastructure, and hence any significant disruption could be self-harming. Also, the resources required to launch a truly large-scale cyber-attack are only available to leading cyber-powers. These are limited in number and hence the likely identity of the guilty party may not be as elusive as smaller-scale disruptions.

So far, cyber-deterrence appears to be effective in preventing large-scale attacks that could result in casualties. This is not entirely due to capabilities; challengers also understand that the destructive might levelled at such actors would be devastating. This assessment implicitly accepts the lack of published evidence demonstrating a desire by states to launch specific, large-scale cyber-attacks, although such evidence does exist in more classified domains. Continual advancements in technology and the low barriers to entry into the cyber-domain may change this situation in the future. If more states manage to obtain destructive cyber-capabilities, more lethal use of cyber-warfare may be seen. With such powerful capabilities, the problem of attribution may become more prominent. While the cyber-attribution problem complicates deterrence, the concept of swift, clear and targeted
retaliation still stands. Be this through cyber-weapons or physical means, it must be demonstrated that cyber-intrusion beyond the accepted norm will not be tolerated. The US just started to develop this policy area after the recent North Korean attacks on Sony Pictures in January 2015.

Deterrence and Non-State Actors
The rise of non-state actors with the power to influence global events has posed a challenge to the traditional understanding of the state system. Some of these non-state organisations possess military capabilities or the ability to inflict violence. A debate continues, however, over whether such groups can be deterred by military, economic, political or ethical means.

Those who believe deterrence can apply to such groups point to the cost-benefit calculation that is instinctive and common to all actors, albeit not easily estimated for some violent non-state groups. Their argument is that by tailoring deterrence to the actor in question, one can continue to influence its decision-making. Yet the evidence to support this view is not compelling. This does not disprove that non-state actors can be influenced; rather, it shows that understanding their decision-making is difficult and therefore that the means to influence them cannot be reliably developed.

Some argue that deterrence against non-rational actors – in other words, groups whose responses do not conform to Western interpretations of logical rationality – is impossible, since their response to triggers, threats or actions cannot be predicted.16

Many of the issues involved in using deterrence as a strategy for influencing non-state actors relate to making deterrence specific to that actor, rather than assessing their behaviour. Of course such specific deterrence requires an appetite to undertake activities in proving national resolve. This, however, means accepting the inevitability of tests and reaction to deterrence postures and policies. National audiences may not understand the requirement for actions that intend to affect future behaviour, as opposed to those which relate to current circumstances; this is nevertheless how some French theorists recognise the future of deterrence.17 They understand deterrence

as a strategic intimidation on a broad and grand scale. This approach is in stark contrast to the US school, which sees deterrence aimed at preventing an adversary’s specific military action, typified by the US air-sea battle doctrine directed against China.

**Law-Enforcement Strategies as Deterrence**

Law-enforcement models of deterrence can be adapted to a strategic context. One approach that can be applied is known as the ‘rules of the game’. In the domestic context, this model involves tolerating a low level of disruptive activity in society – but, on an implicit understanding that should the level exceed a threshold, it will trigger a disproportionate response.

This method has been adapted from law enforcement to grand strategy in Israel. Here, Hizbullah and Hamas continue to make low-level, irregular attacks against Israel which elicit little response – a demonstration of both tolerance and resilience from the Israeli state. Yet when the threshold – for example, of the number of rocket attacks – is exceeded the resulting military response is disproportionate (indeed, it may not even need to have a military objective per se beyond retribution). In addition, once a response has been triggered, the tolerance level is established at a lower level than before. Both these actions are supposed to dissuade actors from challenging the status quo. The events in Gaza during the summer of 2014 illustrate this approach. On 7 July, after a slow rise in activity between Israeli and Hamas forces, forty rockets were fired into Israel. This breached the tolerated level of activity and in response, on 17 July, the Israel Defense Forces launched a highly destructive retaliation into the Gaza Strip, which led to the deaths of some 2,200 people.\(^{18}\) While the achievability of the operation’s aims and objectives was debatable, the attack was actually a political response to a breach of the ‘rules of the game’ and resulted in a massive reaction. Although this strategy may work in the long term in the law-enforcement domain, its benefits may be less clear when translated into grand strategy.

---

Russia’s recent activities in Ukraine and the rise of Daesh in Iraq and Syria have posed a challenge to the Western model of deterrence. However, the problem is not entirely new, even in cases involving violent non-state actors (VNSAs). Despite the recent focus on the threat posed by VNSAs to the US and its allies, these actors have a long history of challenging established rules. They were notably brought to the public’s attention by the 9/11 attacks in 2001. In 2002, then-US President George W Bush claimed ‘Deterrence means nothing against shadowy terrorist networks with no nation or citizens to defend’. While this view may be broadly held, the recent rise of Daesh has nevertheless forced the West to rethink the way it approaches deterrence.

Israel presents a major case study in which deterrence techniques against VNSAs have been tried and tested over long periods of time. Indeed, Israel has faced problems of political violence and VNSAs since independence in 1948. The country has developed its methods of deterrence through years of Arab–Israeli conflict, fighting across contested borders, often against politically motivated non-state aggressors. Studying the evolution of these conflicts can provide valuable insights into how Israeli deterrence has adapted to counter non-state threats and can highlight areas of success and failure.

The Arab Revolt of the 1930s in the British-administered Mandatory Palestine sparked a belief that the only way to stop Arab attacks was to grow the Jewish community’s own military strength. Jewish defence militias, which would later integrate into the new state’s defence force, responded to violent threats. Much of their retaliation was borne of emotion, rather than planned and executed with the specific aim of deterrence. When Israel achieved independence, neighbouring Arab states saw the new state as an aberration. Syria, Egypt and Jordan turned a blind eye to terrorists based in their territory as they had a shared interest in destroying the Jewish state. As a young state with new borders, the attacks – which used to be an internal problem under the British-run mandate – now became an external problem for the state of Israel. It was not easily possible to pursue terrorists across borders into neighbouring states and Israel could not expect its neighbours to apprehend these groups. By the mid-1950s, it was commonplace for small, armed units of fedayeen to enter Israel from Jordan and launch violent attacks. Meanwhile, militant activity emanating from Gaza increased. This was supported by Egyptian troops which, by 1955, were even participating in raids. The attacks from Syria, Jordan and Egypt peaked in 1955 and Israeli

---

policy-makers saw this infiltration as an act of war. Hence, Israeli leaders felt it was necessary to dissuade the country’s opponents.

The then chief of staff of the Israel Defense Forces (IDF), Moshe Dayan, ordered a series of retributive raids to hit the *fedayeen* in their strongholds. He described the policy in November 1955:

> We cannot guard every water pipeline from explosion and every tree from uprooting. We cannot prevent every murder of a worker in an orchard or a family in their bed. But it is in our power to set a high price on our blood, a price too high for the Arab community, the Arab army, or the Arab government to think it worth paying.

Dayan hoped that the promise of cross-border retaliation would provide incentive for neighbouring states to discourage cross-border attacks on Israel. This led to seventy reprisal missions in three years, each one designed – in strength, certainty and speed – to fit the offence. These raids did not always have the desired effect and occasionally the severity of the retribution far exceeded the offence. Israel was forced to rethink its policy after a reprisal on Qibya, Jordan, in 1953. After a mother and her two children were murdered in the Israeli village of Yehud, Israel launched a reprisal that killed around a dozen Jordanian soldiers and more than fifty civilians. This raid caused international outrage and prompted Dayan to re-examine his policy: ‘Israel had learned that even when Arabs harm peaceful civilians, we must direct our retaliation against military objectives.’

New IDF guidelines were subsequently released at the end of 1953:

- Any confrontation will be evident and there will be no attempt made to hide it
- The principle of cleaving to the place and method of the crime is revoked. We shall hit the enemy where and how we choose, even if the objective does not exactly match the enemy’s crime
- The speed of the operation is decisive – the reaction must be as quick as possible and as soon as possible after the crime
- The targets chosen will be crucial objectives: military centres, camps, police stations, National Guard concentrations deep behind [enemy lines], the attack upon which will be as painful as possible.

---

This produced mixed results. On one hand, it resulted in one of Israel’s first successful acts of deterrence. Jordan, as a weak state, faced with anti-regime sentiment after heavy Israeli reprisals, began to work to prevent insurgents from infiltrating Israel. On the other hand, raids aimed at the Egyptian military escalated tensions, contributing to the full-scale confrontation in the Suez Crisis of 1956. For the following five decades, Israel continued to be involved in major conflicts. Insurgent attacks from various non-state actors continued during all of these conflicts.

Israel was ultimately victorious in every major war it fought, but its victories did not always successfully deter its adversaries. After Israel gained control over the Sinai Peninsula in 1967, Egypt launched a surprise attack against Israel in 1973 in the Yom Kippur War, briefly recapturing it. Egypt did not doubt that the IDF had greater military strength nor did it believe Israel lacked the will to retaliate. Israel was convinced that its capabilities and will were sufficient to deter an Egyptian attack. Nevertheless, because the Israelis lacked understanding of how important the peninsula was to Egypt, Israel was not prepared. The Egyptian attempt to reclaim the peninsula in 1970 should have displayed the significance of the issue to Israel. However, Moshe Dayan – at that moment Israeli defence minister – was surprised in both 1970 and 1973, believing the cost to Egypt of attacking Israel would far outweigh the benefits of retaking the lost territory.

Although the specific deterrence of Egypt failed, the Israeli display of strength and demonstration of superior capability during the Yom Kippur War resulted in a reinforcement of Israel’s general deterrence posture in terms of capability and intent, and ultimately led to a peace treaty with Egypt. This was a paradox of Israel’s general deterrence: failures of specific deterrence showed Israel’s escalation dominance, but were unsustainable. Each failure to deter led to further violence that built angst among Israel’s adversaries, ultimately resulting in further aggression, albeit through less overt means. Thus, while Arab neighbours have not invaded Israel since 1973, they have funded a wider insurgency against Israeli interests.

Israel finds itself in this problem today. The current strategy is to maintain the status quo – as Israel cannot eliminate the threat, it is necessary to manage rather than eradicate it. In recent years, Israel has used a mixture of compellence and deterrence to achieve this.

A good example of this was the withdrawal of the IDF from southern Lebanon in 2000. Israel believed that withdrawal would dissuade Hizbullah from carrying the fighting into Israel, as it would liberate southern Lebanon from Israeli occupation. It was believed that the Lebanese population in the south would no longer wish to fight the IDF once it had departed; in turn, this was intended to compel the Lebanese population to stop harbouring terrorists. At
the same time, Israeli President Ehud Barak announced that Syria would be held accountable for any Hizbullah attacks as it had a strong military presence in Lebanon. Hizbullah attacks were accordingly addressed by Israeli attacks on Syrian military infrastructure, such as radar bases, within Lebanon.

Yet as time passed, what seemed a relatively stable balance of conflict escalated. As Hizbullah had no state or citizens to protect, Israel faced more severe costs and losses, with soldiers taken hostage and civilians killed. With Hizbullah growing in capability, Israel feared what response an Israeli reprisal would draw. A miscommunication of threat from Israel, and Hizbullah’s misunderstanding of Israel’s will to retaliate, led to war between the two.

On 12 July 2006, Hizbullah launched a cross-border attack, killing eight Israeli soldiers and taking three as hostages. It did not anticipate the massive retaliation which killed around 1,200 Lebanese citizens as a result of a relentless, month-long air campaign accompanied by a ground attack. Despite an estimated 170,000 shells hitting Lebanon in a month, Hizbullah reportedly lost less than 1 per cent of its ground-launch platforms. Again, specific deterrence of Hizbullah had failed; on the other hand, the overall conflict restored general deterrence and, soon after, neighbouring Syria opened peace talks with Israel.

There is much to be learned from Israel’s troubled history of deterrence. Reprisals do not provide single acts that will deter or compel a state or actor. Instead, the responses to acts of VNSAs have built Israel’s umbrella of general deterrence. These acts maintain the general norm of behaviour of militant actors. When these small-scale reprisals fail to build sufficient deterrence and violent actors overstep what is seen as the tolerable level of conflict, Israel may retaliate with a single, intense spike of violence. While this strategy may strengthen general deterrence, it cannot defeat its opponents or eliminate attacks. Some argue that in this respect, Israeli deterrence cannot be seen as even marginally successful, as truly successful deterrence should not require escalation every few years. To successfully halt violence, Israel must instead pursue political moves which may lead to a more stable outcome.

While an interesting and well-tested case study, Israel has never achieved absolute deterrence. It follows a policy that merely strives to achieve a level of minimal acceptable violence based on an assumption of continuous and imminent conflict with an adversary. This might be the best a state can hope to achieve in a modern era of non-state actors, radical fundamentalism and weapons proliferation.


IV. East Asia Case Study

North Korea has posed a substantial security threat in East Asia since the end of the Cold War; similarly, the rise of China poses questions for regional security. In this context, a large part of US security policy in the region has been focused on extended deterrence in the form of the US ‘nuclear umbrella’ over its key regional allies: Taiwan, Japan and South Korea.

North Korea’s unpredictable behaviour and the strength of a growing China (both nuclear-armed states) are sources of regional tension for their neighbours. While China has a fairly well-established nuclear capability, North Korea does not: it is not believed to have miniaturised a nuclear warhead to the extent that it can be effectively delivered. However, even Pyongyang’s limited capabilities should not be dismissed, and its aggressive behaviour demands serious attention.

Yet the nuclear non-proliferation regime forbids the spread of nuclear weapons to allow neighbouring states to counter China and North Korea. To dissuade states from acquiring their own nuclear capability in this potentially unstable region, the US is willing to threaten with the use of nuclear weapons to protect its allies – in particular, Japan, South Korea and Taiwan. By maintaining confidence in this US capability and its reputation, Washington has managed to compel these countries to not develop their own nuclear capability.

South Korea
While currently under the US nuclear umbrella, the extended deterrence relationship with South Korea has not always been smooth – Seoul actually initiated its own nuclear programme in the early 1970s. In 1958, the US deployed nuclear weapons to South Korea to reinforce Washington’s guarantee. However, the belief in this guarantee faded in subsequent years and, in 1970, North Korea escalated tensions by capturing a South Korean naval vessel. Despite the rising worries over conflict with the North and objections from the South Korean government, the Nixon administration withdrew capabilities from the Korean Peninsula – without further discussion. This led President Park Chung-hee to pursue a stronger defence posture. Conventional deterrence was found to be too expensive – hence, a nuclear programme was started. South Korea no longer believed that the US would provide the promised security commitments due to Washington’s weakening image in the region.

To prevent nuclear proliferation, Washington threatened South Korea to withdraw more US troops and cut financial assistance. Park suspended some parts of the project, but continued nuclear-weapons projects in secret. The relationship between the US and South Korea deteriorated over the
decade until Park was assassinated in October 1979, and the US retracted its troop withdrawal plan under President Carter. From then on, relations improved and South Korea abandoned its pursuit of nuclear weapons. This is an important example that provides an argument for positive compellence as opposed to just negative deterrence: reinstating US troops earlier may well have forestalled South Korea’s nuclear activities. Eventually in 1992, the Joint Declaration of the Denuclearization of the Korean Peninsula was signed by both Koreas. In the document, they swore not to ‘test, manufacture, produce, receive, possess, store, deploy or use nuclear weapons’. Although the North has since violated this agreement, the promise of the US nuclear umbrella – and the confidence that it will be upheld – has deterred the South from restarting its nuclear programme.

In 2009, at a US-South Korea summit, Seoul raised doubts about the US security guarantee. To maintain a non-nuclear policy in South Korea, Washington allayed these fears by confronting North Korea over nuclear tests while maintaining close communication with its ally. Furthermore, the Obama administration echoed its commitments to Seoul in the 2009 summit statement, which reads that both parties ‘will maintain a robust defence posture, backed by allied capabilities which support both nations’ security interests. The continuing commitment of extended deterrence, including the U.S. nuclear umbrella, reinforces this assurance.’

This affirmation helped boost Korean confidence in the US’s resolve. However, there are still those in South Korea who believe that a sovereign nuclear capability should be established. As a result, the US must continue to meet any North Korean hostility quickly and seriously in order to maintain the credibility of its guarantees. The US is left with few options other than continuing to maintain large garrisoned forces on the Korean peninsula, with the associated financial and military resource implications.

Japan
Perhaps understandably, of all the allies that fall under US extended deterrence, Japan presents itself as the most anti-nuclear. Despite its position in a potentially unstable region, the memories of 1945 remain strong. Both progressive and conservative parties in Japan strive for nuclear disarmament. However, it must be remembered that the situation in Japan is unique: outside efforts to prevent Japan from procuring nuclear weapons have had very little internal opposition from the start. Japan is known to have covertly undertaken small amounts of research into nuclear weapons, but these proved costly – both financially and politically – and were therefore

ended. Instead, Tokyo has accepted the use of US extended deterrence, with Japan continually involved in discussions and planning in order to encourage the reaffirmation of US resolve and capability.

Regarding the threat from North Korea, the left in Japan has reasoned that should North Korea initiate conflict, it would not be for self-gain but out of a sense of weakness. Based on this understanding, the left argues that compellence (in other words, military presence) be used to reassure North Korea that it is not under threat, particularly from the US. If this policy were to be implemented, Japan would take a step away from the approach of deterrence that it has been adopting towards North Korea.

It is still the case that the majority of the Japanese public is opposed to the idea of a Japanese nuclear weapons programme and hence the US umbrella is an important part of Japanese security policy. Like South Korea, Tokyo seeks affirmation that the US will uphold the nuclear umbrella and come to Japan’s aid both conventionally and, if necessary, with nuclear strikes. In order to strengthen the US–Japanese bond, Tokyo has developed its own strategies of coercion: developing an organic amphibious force and naval capabilities that seek to overcome a Chinese policy of anti-access and area denial. Tokyo believes that by becoming more involved with US affairs, Washington will be compelled to assist Japan should hostility arise in Asia.

In the current situation, it is unlikely that Japan will pursue nuclear weapons. Anti-nuclear beliefs have become part of the national identity, and this should continue so long as the US keeps affirming that Japan is supported by the nuclear umbrella. Nonetheless, based on some predictions, if Japan were to pursue a nuclear programme, it could take as little as between two and ten years to develop.

Taiwan
The rise of the People’s Republic of China (China) and its emergence as a nuclear power triggered a nuclear programme in the Republic of China (Taiwan) in the late 1960s. It was thought that a Chinese nuclear capability would render Taiwan increasingly vulnerable. Alongside this, there was declining confidence in US guarantees – Presidents Kennedy and Johnson rejected President Chiang Kai-shek’s calls for intervention in China. These factors led to the Taiwanese nuclear programme and its acceleration in the 1970s. The US found evidence of this programme in 1974 and pressed Taiwan to dismantle several facilities and make a public declaration that Taipei would

not pursue nuclear reprocessing. The programme continued behind closed
doors until 1987, when a defector revealed its continued operation. Taiwan
was subsequently forced to terminate the programme due to pressure from
both the US and China.

Unlike Japan and South Korea, the US does not guarantee to defend Taiwan in
the event of hostilities with China. Yet, garnering US support is still important
to Taipei. Its leadership knows that if it pursues a nuclear option, Washington
will certainly abandon the country diplomatically and end military sales.
Taipei cannot afford to lose such US favour, even if there is no promise for
aid or any US involvement in a conflict scenario. In this way, Washington is
able to deter Taiwan from procuring nuclear weapons without the risk of
committing itself to a potential cross-strait conflict with China.

Implications for Nuclear Deterrence in East Asia
Taiwan and, especially, South Korea and Japan depend on US extended
deterrence. With this nuclear umbrella, Washington has been able to
dissuade these states from procuring their own nuclear weapons. Over the
last decades, however, the area has experienced escalating tensions, such
as disputes over the East China Sea and the unpredictable behaviour of
Pyongyang. The history of this region reveals some interesting consequences
of deterrence. In recent times, fears over the mentality and reputation of
the US have been reduced by the positive commitments to protect specific
countries with the nuclear umbrella. Leaders in the western Pacific have
expressed concern privately over the less strident US presence and military
activities in the region on a conventional force level. Despite this, statements
on US nuclear force deployment in the region and US national interests
have overcome some of the less formally declared concerns by these
governments. This is worth noting when looking to the future, as history
indicates that negative deterrence and threats will not succeed in keeping
states non-nuclear in East Asia: South Korea attempted to establish its own –
albeit stalled – nuclear weapons programme. If the current state of affairs is
to continue, Washington must instil belief and trust in its Asian allies through
close communication and presence, particularly in the face of threats from
North Korea and the growing power of China.

5. See coverage of comments by Philippine President Benigno Aquino and Japanese
Prime Minister Shinzo Abe in Michael D Swaine, ‘The Real Challenge in the Pacific: A
Response to “How to Deter China”’, Foreign Affairs (May/June 2015).
V. Conclusion

Strategies of deterrence encompass a vast array of activities and national philosophies. The concept has persisted since ancient times and remains useful today whether in its conventional or nuclear form. The practice of deterrence has adapted to new technologies, changing distributions of power and new kinds of threats by being sufficiently malleable. It is therefore naive to assume that the modern world – whether due to societal shifts or technological development – somehow makes deterrence irrelevant.

Modern examples of deterrence postures, activities and actions indicate their ability to remain viable concepts for defence and security. However, there is no single strategy of deterrence to counter threats and prevent conflict. Strategies of deterrence must be nuanced and contextualised to particular enemies, adversaries and geopolitical circumstances.

This is a facet that could change the utility of deterrence in the future. If leaders do not understand the construction and execution of deterrence within the societal and technological context of the problem, delivering it successfully will be challenging. Interestingly, it does not appear that misunderstanding of this concept comes from current, future or potential adversaries; rather, it is Western decision-makers and leaders who have not taken the time to actively consider the relevance of the concept in the modern world.

Activities and capabilities which underpin deterrence are not easy nor are they cheap. The investment in resources to deliver successful deterrence postures – militarily, economically and conceptually – is significant. Still, unlike many other national approaches to defence and security, it appears that deterrence will continue to be as relevant as it has always been. Those key requirements for successful deterrence can be summarised as follows:

- Viewing deterrence through the eyes of the adversary and not one’s own, including removing a Western perception of rationality from the risk calculation. This should also encompass an appreciation of, in some cases, the futility of dialogue and argument with some parties. Some term this detailed threat deconstruction\(^1\)
- Possessing (and demonstrating) sufficient capability and capacity for retaliation
- Forward positioning and regular, visible deployments of forces that would be required to take action for punishment, retribution or escalated response

---

• A political and social willingness to accept pain – whether financial, political, economic or loss of life – as a result of actions
• An ability to adapt responses allowing decision-makers to transform a state’s response from deterrence to coercion as individual situations dictate
• Humility in deterrence, which allows an adversary the opportunity to de-escalate each situation and escape the time and decision compression that frequently occur in testing scenarios
• Appreciating the link between resilience and deterrence and investing in both, particularly in military capabilities that provide greater resilience and therefore change the cost-benefit calculation for an adversary.
About the Authors

**Peter Roberts** is a Senior Research Fellow for Sea Power and Maritime Studies at RUSI. He researches and publishes on a range of subjects, including strategy and philosophy, sea power, command and control, naval weapons systems, C4ISR, military education and military use of cyber-warfare. He also oversees conferences, meetings and lectures in these areas. He retired from the Royal Navy in January 2014 after a career as a Warfare Officer, serving as both a Commanding Officer and a National Military Representative in various roles with all three branches of the British armed forces, the US Coast Guard, US Navy, US Marine Corps and intelligence services from a variety of other states. He has served as chairman for several NATO working groups and Five Eyes maritime-tactics symposia. While the latter part of his career was spent advising foreign governments on maritime strategy, his most recent military experience was within defence management and procurement with responsibility for military cyber-warfare, information operations, human and signals intelligence, and maritime ISTAR collection.

Peter has a Master’s degree from King’s College London in Defence Studies. He is a Visiting Lecturer in Strategy at the Portsmouth Business School at the University of Portsmouth and is a Fellow of the Chartered Management Institute.

**Andrew Hardie** is a visiting fellow at RUSI, and researched a number of subjects in the C4ISTAR and engineering domain while working with the Military Sciences team. He is currently a Senior Engineer at MBDA Missile Systems, specialising in guidance and control algorithms. Andrew holds a First Class MEng in Aeronautical Engineering from the University of Glasgow.
RUSI Membership

RUSI membership packages provide privileged networking opportunities and benefits tailored to meet the needs of both individuals and large organisations.

**Individual Memberships**
Individual memberships are suitable for those individuals who wish to join RUSI’s growing network of policy-makers and practitioners. Benefits include regular updates from RUSI, including invitations to members’ lectures and seminars, subscription to the *RUSI Journal* and *RUSI Defence Systems*. This package also offers members access to our renowned Library of Military History.

**Corporate Membership**
RUSI’s corporate-level membership packages, offering discounts to all RUSI conferences, are open to all organisations concerned with defence and security matters, and can be tailored to meet the business interests of both public and private sectors.

**Concessions**
Discounted student and young persons rates are available for those under the age of 35. Concessions are also available for those over the age of 65. We also offer online membership to those wishing to access RUSI’s content of analysis and commentary.

[www.rusi.org/membership](http://www.rusi.org/membership)