The 2020 Michael Quinlan lecture, 21 January 2020

Professor Sir David Omand GCB

The Future of Deterrence

It is an honour to have been asked to deliver the Michael Quinlan lecture about the future of deterrence. Especially here in King's College where Michael's papers are available to scholars in the Liddell Hart Archive.

Michael was a British civil servant from 1954 to 1992, finishing as Permanent Secretary to the Ministry of Defence. In MOD we saw him as our exemplar. He tutored me for example in the spare prose necessary in his day for writing White Papers. Not a word missing but not an unnecessary one left in either. Were he to read some of the publications of government today he would be sighing, O tempora, O mores!

Michael wrote of himself, "policy on nuclear weapons bulked large in several of my posts and I acquired over time a structure of concepts for tackling the issues it raised". He was Private Secretary to the Chief of Air Staff when the RAF had responsibility for the national deterrent, Director of Defence Policy at a time of intense interest in nuclear arms control, a key member of NATO's NPG Staff Group updating Alliance nuclear strategy as Defence Counsellor to NATO, and Deputy Under Secretary of State for Policy and Programmes when the UK decided to replace the Polaris system with Trident. I know from my own time as Private Secretary to several Secretaries of State for Defence, and later as Deputy Under Secretary of State for Policy, the influence of Michael's thinking.

Yet, as Michael wrote in retirement, "the need for policymakers to think hard and realistically about nuclear weapons did not end with the Cold War". And now we have serious cyber threats, creating a demand for fresh thinking about deterrence.

Michael believed the ideas behind nuclear deterrence should be accessible to the non-specialist. I shall therefore try to avoid what the late John Berger called mystification, 'the process of explaining away what otherwise might be evident', the critique of the cold remote vocabulary of the expert - in Berger's case on high art.

In plain words, we exercise deterrence every time we affect other people's behaviour through threatening to impose a potential cost or difficulty on them if they act in ways we do not want. Deterrence is about affecting behaviour – I shall ask how far that is possible in cyberspace.

How <u>do</u> we influence another not to act in a way we do not want?
We can expose their intentions to criticism,
we can try subliminal influence and nudging,
we can offer inducements and threaten to withhold them,
we can emphasise mutual inter-dependence,
we can threaten, including with consequences so awful as to dominate all other considerations.
There is a scale of D: from D minor, detection and exposure to disapproval, to discouragement, to deflection, to dissuasion and finally to D major, the formal structures of nuclear deterrence.

I had a homely example provided by two young grandchildren. They had been told to turn down the volume on the children's television programme they were allowed to watch. Various threats of switching off the programme, banning screen time for the next few days, as well as inducements for continued good behaviour during their stay with us, had been made.

As I watched them, a little hand crept towards the remote control and I could sense the internal calculation about whether we would notice, what they could get away with, and whether my signalling of the consequences of overt disobedience, and the value of the inducements that might be withheld, were for real.

Although they would not have known to frame the issue that way, part of what was going on was an internal debate about what really constituted a red line that must not be crossed. Signalling the existence of such a line should imply certainty that if crossed there will be consequences.

That is the rationale for the 70-year old mutual defence provisions of Article 5 of the NATO Washington treaty that would be triggered by an armed attack on the NATO area.

Nuclear deterrence is a serious matter surrounded by grave ethical issues, about which Michael Quinlan cared deeply. I do not know if Michael knew of the historical judgment of Hannah Arendt, "Those who choose the lesser evil forget quickly that they chose evil." Michael I am sure accepted that living with the guilty knowledge of having contributed to the capability for nuclear devastation is the price to be paid by those who desire to prevent

major war, but who know that in a world of nuclear powers that means being prepared in the last resort for the use of nuclear weapons. My grandparent example is not an attempt to trivialise those concerns, but to emphasise that the ideas behind deterrence, when it can be expected to work and when not, involve basic human psychology.

Now, setting red lines has consequences. Once a red line has been signalled we must expect the other party to creep close to it and try to achieve as much as they can of their objectives whilst staying just on the safe side of the red line. That is what we see with aggressive Russian cyber behaviour today, below the threshold of armed attack.

If behaviour is adjusted right up to the red line itself, it will leave little or no margin of appreciation for miscalculation or mistake. Trusted communication channels between the parties are therefore essential.

In October 1961, as the Berlin Wall was being built, Khrushchev ordered Soviet tanks, their engines revving, to be positioned right up to the Friedrichstrasse. General Lucius Clay, President Kennedy's special representative in Berlin, had his tanks lined up facing them to demonstrate Western resolve. All loaded with live ammunition. The slightest miscalculation could have escalated into armed hostilities.

President Kennedy felt it necessary to send a personal request to Khrushchev to withdraw his tanks out of sight - giving, we can assume, private assurances that there would be matching de-escalation on the Allied side. Bobby Kennedy, then US Attorney General, sent the message via his hotline, in fact through Col Georgi Bolshakov, known to be a GRU agent

who was posing as the Press Attache in the Soviet Embassy in Washington. It worked, but to add a historical footnote, the same Bolshakov of the GRU later assured Bobby Kennedy at the start of the Cuban Missile Crisis that of course the Soviet Union did not have nuclear missiles in Cuba. Hotlines can also deceive.

Now with my young grandchildren I would have had another deterrent avenue open to me if I had been able to lock the remote electronically at an acceptable maximum volume. That would have been deterrence by denial to make transgression harder. Not entirely to be relied upon, given the digital skills of the young today, but certainly raising the difficulty of transgressive behaviour.

Professor Joe Nye at Harvard has emphasised a third form of deterrence, that of entanglement, recognising the financial, economic and human inter-dependence of those involved. Both sides may have too much to lose to raise the stakes. I would like to think that would be true of grandchildren and grandparents – but emotion can lead to miscalculation.

Deterrence is thus context specific. It cannot be reduced to equations or algorithms. It depends upon who is issuing the deterrent warnings, who is supposed to receive and understand them, the credibility of the warnings, the value to the potential aggressor of what is being held at risk and crucially the past history of the relationship. There are multiple layers of credibility involved.

Extended deterrence, providing your deterrent umbrella to shelter someone else, adds complexity. NATO nuclear force posture has to ensure

coupling of the defence of NATO Europe to that of the United States in ways that are credible, including to NATO's domestic populations to avoid self-deterrence. At this point my analogy of the grandchildren runs out, perhaps with a cry of "just wait until your parents get home!" invoking their assumed greater deterrent power but leaving ambiguity about what then will happen.

We want sufficient strategic certainty but also some tactical ambiguity to discourage an adversary from gambling on being able to game the response.

Nor must either side come to believe that they could pre-empt the other's capability. Hence continuous-at-sea-deterrent Trident patrols by the Royal Navy are essential to the UK contribution to NATO deterrence strategy. Michael Quinlan elegantly demolished, as only he could, the arguments that surfaced from time to time of so-called 'existential deterrence' where nuclear weapons could be kept in base but not deployed operationally. Such a posture invites instability in a crisis. As Michael Quinlan wrote 'Nuclear weapons deter by the possibility of their use, and by no other route'.

Nuclear deterrence does not depend upon an assumption of chess master-like calculation. If the prospective penalty is sufficiently severe – and the damage that would be caused by any nuclear weapon, unlike that from cyber weapons, is very persistent - then much less than certainty of the punishment getting delivered is likely to deter. We have to be realistic that the prospect of a conventional or cyber response will not dominate the risk

calculation of an aggressor in that way. And hostile cyber activity is all around us.

Michael Quinlan insisted that the NATO democracies would never support the use of nuclear weapons in anger unless they were facing the loss of a major war of national survival. As the late Professor Herman Bondi was fond of saying. 'The definition of a nuclear armed state is one that you cannot afford to make desperate'.

That observation is pertinent to the Cold War worries of NATO being caught off-guard. Most surprise attacks occur because the weaker party has temporarily the advantage of choosing a time and place with favourable force ratios. But any such advantage would have quickly dissipated since the Major NATO Commanders have counter-surprise plans with the authority and fire power to be able to mount a robust defence. The situation thus facing an aggressor would have been that despite any initial success their attack would have triggered major armed conflict. The risks from escalation therefore far outweighed any potential gains the aggressor might have hoped to secure. Nuclear weapons do not serve just to deter the use of nuclear weapons.

Michael Quinlan nevertheless counselled a degree of humility in asserting that Cold War behaviour on the part of the Soviet Union in respecting the integrity of NATO territory could be explained entirely by deterrence, adding dryly that humility was not always evident in commentators on nuclear deterrence. That brings to mind the man who always stamped his foot on entering a room, which he said was too prevent the elephants from following him. But there are no elephants outside the room, you say.

Exactly, he replies, my strategy works. Professor Philip Bobbitt has drawn attention here to the danger of the Parmenides fallacy. We should not compare the present state of affairs with the past but compare the present with the worlds that would be actual today if we had not developed and deployed our nuclear weapons. A counter-factual judgement is needed about how much more likely war with the Soviet Union would have been without nuclear deterrence. The solid evidence available today, from East and West, bears out the conclusion that both sides held back with a genuine fear of *l'éngrenage,* of starting a conflict they could not control.

Russia today has to accept that - as reiterated at the NATO 70th anniversary meeting in London last month – the Alliance remains determined to defend its territory. That was what Michael Quinlan compared to the Copernican revolution in thinking about war. Wars between nuclear armed adversaries became far too dangerous to start, even if the initial intention of the aggressor was limited, and certainly did not envisage nuclear weapon use. The same argument cuts the ground from under 'no first use' declarations. Under the passions of a major war no country can be relied upon to stick to such peacetime declarations of intent, however well-meant at the time.

Nuclear deterrence strategy only solves one problem, of course – albeit a big one - taking major war out of the repertoire of statecraft between nuclear powers. What it cannot do is prevent States trying to achieve their security objectives through competition at lower levels of conflict and intimidation. During the Cold War, the West faced Soviet subversion that had three components. Intimidatory moves to get our attention. Propaganda to persuade us that compliance was in our interest, the international community that it should stand aside, and the Soviet

population that the regime was acting in their interest. And the third component was a repertoire of dirty tricks. Such behaviour continues today.

But, today, subversion can also be delivered digitally, more easily and at lower cost.
Intimidation through cyber-attacks, and trolling to drive unwelcome voices off social media.
Propaganda from TV and radio stations and Internet sites.
Dirty tricks from hacking and stealing emails and releasing them, from bogus social media campaigns, from the amplification of angry voices through automated bots, from deep fakes and all the rest.

Deterrence is, in the lapidary words of Michael Quinlan, "about operating on the thinking of others". That is the business model of the Internet, or, as it has been termed "surveillance capitalism", using our own personal data as feedstock for personalised marketing and political influence campaigns. It is the most impactful content that gets noticed, no matter how angry, how divisive, or how untrue. It should be no surprise to find the digital medium being exploited by Russia and others to launch cyberattacks, undermine confidence in democracy, exacerbate divisions in society and distract our governments.

Can aggressive digital activity be deterred through some combination of the three basic forms of deterrence?

1. Deterrence by credible sanction of punishment for unacceptable behaviour

2. Deterrence by denial, making it too hard for the adversary to secure their objective at reasonable cost.
3. Deterrence by entanglement where all parties have a shared interest in the relationship not becoming too fraught, with international norms of good conduct chilling bad behaviour by the consideration that we all have to coexist and do business together.

As I have illustrated, deterrence by threat of punishment requires sufficiently specific signals of intent backed up by credible capability to impose unacceptable consequences.

I cannot fault here the signalling of the Obama administration:

> "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means — diplomatic, informational, military, and economic — as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible".

NATO has therefore developed a Cyberspace Operations Centre to improve such cooperation between member states, and the UK has said it will declare its offensive cyber capability to NATO.

John Bolton, when US National Security Advisor, briefed that the Trump administration's new "National Cyber Strategy" had replaced Obama era restrictions on the use of offensive cyber operations. The new legal regime enables the US Defense Department and other relevant agencies to operate with a greater authority to penetrate foreign networks to deter hacks on U.S. systems. Describing the new strategy as an endeavour to "create powerful deterrence structures that persuade the adversary not to strike in the first place," Bolton added that decision-making for launching attacks will be moved down the chain of command from requiring the president's approval.

The *New York Times* reported shortly afterwards that US Cyber Command had planted malware potentially capable of disrupting the Russian electrical grid, something the Russian authorities admitted was conceivable. As signalling that is fine.

But in practice maintaining a 'trojan' capability of that sort is extremely difficult. Every patch to the target system, every change of configuration, has to be monitored in case it affects the malware, and can you really be sure that the owner of the system has not discovered the malware and how to disable it, so when it comes time to press the button nothing happens?

We also have to bear in mind that there can be unexpected consequences from offensive action. Russian attackers for example inserted the NotPetya worm into tax preparation software aimed at Ukrainian targets but it escaped into the wild and did well over a $1billion worth of damage to global companies and almost destroyed the world's largest shipping company, Maersk.

A digital attack that did leave many dead or that caused massive destruction, the cyber Armageddon beloved of thriller writers, would rightly be equated to the result of an armed attack. That possibility would justify a response under the inalienable right of self-defence. It might be a major cyber retaliation to persuade the aggressor to desist. But equally it might be a flight of cruise missiles. It is wise to dispel any illusions that there could be major cyber wars that would stay confined to cyber space.

The destructive capability of both conventional and nuclear weapons is obvious without revealing sensitive design details. Demonstrating highly destructive cyber capability is harder without revealing your hand in ways that might enable the potential adversary to reduce their vulnerabilities, or even to reverse engineer and turn the method back on you. Nevertheless, the British Government helpfully publicised that it has used offensive cyber capability against the jihadist propagandists of Daesh.

We need to ensure our response is calibrated to be necessary and proportionate whilst those attacking us will not be so constrained, But even if doubts exist about the realism of our being able to inflict a high enough level of punishment by cyber means to deter, sufficient conventional capabilities certainly do exist to respond to a major attack. I think it likely therefore that US and NATO statements aimed at deterring devastating cyberattacks are taken seriously.

Of course, you have to attribute responsibility for cyber-attacks. This is, like any intelligence-based assessment, a probabilistic judgment by the professionals, after weighing all the forensic evidence in the code used, the

methodology, past record and the secret intelligence available, for example considering the intentions of an adversary and shedding light if the real attacker is seeking to divert blame and create a conflict from which they can benefit. A political judgement is then needed of whether and how to act on the professional attribution assessment. There is greater room for misjudgement on the part of the aggressor that they might get away with a cyber-attack than an armed attack. We need therefore to bolster deterrence by investing in the upfront intelligence work to make attribution a faster, more reliable, process.

Most day to day malign cyber activity is, however, well below what might be considered the threshold of an armed attack.

I have an acronym: CESSPIT. **C**rime, **E**spionage, **S**abotage and **S**ubversion **p**erverting **i**nternet **t**echnology. It is hard to see how a threat of punishment can deter such persistent lower level CESSPIT activity by a multiplicity of State and non-State groups including international criminal gangs.

Cyber operations can nevertheless be used against CESSPIT targets by hacking back, penetrating and disrupting the networks and systems of the attackers, to create difficulty and discomfort and make attacks more costly. Such persistent engagement is therefore a contribution to deterrence by denial. It could be described as **forward active dissuasion (FAD),** like having police officers on the beat conducting stop and search. But it is unlikely to cause an actual cessation of such activity, just as the threat of long prison sentences certainly inconveniences the few criminals that are caught and takes them temporarily out of circulation but it does not stop

criminals trying to commit crime. Nor does it stop them improving their techniques to lower the risk of being caught.

We should see such active dissuasion operations as just part of a much wider whole-of-nation and allied effort at raising the cost and difficulty of malign cyber activity. I like the way that GCHQ/NCSC has adopted the term 'active cyber defence' as a form of deterrence by denial, raising the bar by actively seeking out and blocking malware, bad addresses, and dodgy websites.

Investing in good cyber security and cyber resilience makes us a harder target. As does basic cyber security with passwords, patches and multi-factor authentication, 24/7 intruder detection systems, statistical anomaly-based detection and sophisticated encryption.

One way to penalise attackers is to publicise bad behaviour and name and shame those involved. The Russian GRU and other hackers indicted by the FBI will be arrested if they try to travel to the West, imposing at least a modest cost on them, as did the UK attribution of the destructive NotPetya attack and exposing hacker groups like "Fancy Bear" as GRU stooges.

Attackers of course learn from their mistakes and innovate, such as using polymorphic malware that can detect the defensive measures and adapt accordingly. But the initiative here should not be left with the aggressor. We need to be ahead of their game.

In conclusion, we should not mislead ourselves by a false equation of nuclear deterrence to the risk management of persistent threats in cyberspace.

- We should, however, see the digital capability to interfere with adversary systems as a legitimate force multiplier for the Armed Forces when engaged in armed conflict, essential to minimise our casualties, and comparable to jamming and electronic suppression of earlier eras. We do not talk about offensive tanks or warships nor should we label military digital capability as offensive in that way.

- The possession of cyber weapons capable of interfering with critical adversary systems should be part of NATO's preparedness to respond to major cyberattacks that are comparable to a destructive armed attack against our civilian or military infrastructure. These are cyber weapons we do not wish to have to use. But by reserving the right to defend ourselves with means of our choosing, digital as well as conventional, and ultimately nuclear in the case of major war, we are harnessing the Alliance's full deterrent strategy to prevent major conflict from arising. But we should be realistic. For example, I do not imagine we might deter by threat of cyber punishment the rather capable North Korean cyber warriors since ours is a highly networked and therefore vulnerable society and theirs is not.

- Most of the persistent malign activity we experience, day in day out - the CESSPIT - is below that threshold of armed conflict. It cannot be deterred as can an armed attack (or its cyber equivalent) on NATO. But we can reduce the risk to us by a layered defence. We should

impose cost and difficulty on attackers by all the passive and active defensive means open to us, including disrupting their operations where we can, in what I called a Forward Active Dissuasion strategy. We should reduce the vulnerabilities of our systems and increase our resilience, and be prepared to manage the situation when attacks occur. And educate ourselves in critical thinking to reduce our vulnerability to the disinformation and deception to which we are subject on line.

- Finally, deterrence by entanglement has its place, for example as it does in managing the China cyber relationship. I think here of the agreement we and the US reached with China to cut down cyber espionage for the commercial advantage of national companies, a rare example of a practical cyber norm. We should continue to explore other norms for responsible state behaviour in cyberspace, recognising these are complements not alternatives.

Michael Quinlan wrote: "We should have a deep distrust of taking up, on grounds of advantage in political presentation, positions that rest on false strategic premises". Today when it comes to strategic premises for managing cyber threats we should have no illusions about the extent to which we can be sure of controlling the behaviour of our adversaries.

++++++++++++++++++++++++++++