Concerning SSBN Vulnerability - recent papers

John Gower CB OBE, former ACDS Nuc CB, Ministry of Defence

Two BASIC papers published in recent months[1,2] have asserted the UK's strategic nuclear deterrent is in danger of becoming vulnerable in such a way that it can no longer be relied upon to fulfil its primary role. They detail the threat to the submarines from future swarms of surface/underwater unmanned vehicles (but using the more eye catching descriptor of "drones") and the more general threat to the deterrent from a cyber threat, not specifically defined but "out there somewhere, clearly". I will try to offer a measured response to these charges based on my knowledge and experience.

The Management of UK Deterrent Vulnerability

Between late 2008 and late 2014 I was responsible for the annual report on the totality of the vulnerability of the broad range of systems, infrastructure, operations and processes which together constitute the UK's nuclear deterrent. The organisation whose purpose it is to monitor, audit, horizon scan and report, the Strategic Systems Performance Assessment and Analysis Group, worked for me. Clearly the detailed work which is their day to day bread and butter and the content of those reports are inappropriate material for this paper, but I was and remain confident that the scope is comprehensive, innovative and independent of policy imperatives.

There was and remains no place for complacency and their assiduous attention to detail reflected the broad scope of expertise: analytical, scientific and operational which exists across SSPAG. Thus, although I am clearly unable to quantify detail, I am confident that every element of vulnerability, actual or potential, is identified, analysed and reported upon.

Response to Concerns

I will cover the concerns in both reports, in the light of my assertions above, in order to give additional context and I am confident that the BASIC team sponsoring or compiling reports will recognise that I do not do so from a position of bland complacency, which the MoD has been "pre-accused" in both reports, but from one of informed judgement.

Firstly, the **Cyber** report.

The BASIC "Primer on Trident's Cyber Vulnerabilities" draws heavily on and extrapolates from a Jan 2013 US DoD Defence Science Board Task Force Report on "Resilient Military Systems and the Advanced Cyber Threat"[3]. Having studied the 2013 report in detail it is clear it does not identify a current vulnerability in the TRIDENT weapon system (indeed so much so that TRIDENT is not mentioned once). It does recommend - understandably and quite sensibly - that the DoD should audit its nuclear deterrent estate from end to end to ensure that it remains as robust and survivable under determined and sophisticated cyber attack as it is survivable

---

[1] The Inescapable Net: Unmanned Systems in Anti-Submarine Warfare
http://www.basicint.org/publications/david-hambling/2016/inescapable-net-unmanned-systems-anti-submarine-warfare

[2] A Primer on Trident's Cyber Vulnerabilities
http://www.basicint.org/sites/default/files/BASIC_cyber_vuln_mar2016.pdf

[3] http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

against nuclear attack. It should come as no surprise that similar audits form part of the SSPAG remit in the UK.

I am sure it was not the intent of the report's authors, but the loose use of the term TRIDENT to cover every aspect of the programme implies a vulnerability in the most critical areas which does not exist. Those less familiar with all the elements of the programme would be excused if from reading the BASIC report they were concerned that the weapon system (control elements, missile and warhead) had a cyber vulnerability. The report uses the fact that the SSBN command system is migrating to a Windows-based product to imply a consequent TRIDENT vulnerability to cyber.

The command system and the TRIDENT Strategic Weapon System (SWS) have no link and thus there is no path which a cyber attack on the windows-based systems in the SSBNs could exploit. There is simply no cyber pathway which could affect the safety and effectiveness or either initiate an unauthorised launch or prevent an authorised launch of the UK's deterrent.

That is not to say that other, less directly critical, elements of the deterrent wider infrastructure do not, in theory, have cyber vulnerabilities. Any of the computer systems used to design and acquire equipment, plan logistics, programme operations and so on will have some potential vulnerabilities to cyber attack. This is the same for any government or industry system. At the lower level of system which has approved internet connectivity through government gateways, resilience to such cyber attack is provided by software and hardware protection, personnel scrutiny and training and adherence to procedures designed to prevent the threat manifesting itself in a successful intrusion. At the higher level systems, where no outside connectivity exists, any vulnerability is countered by protocol, physical and personnel security. These are all subject to audit and regular review and there is no complacency; the threat is well recognised but does not represent an existential threat to the continuity of the UK's deterrent.

I cannot leave a response to the Cyber report without challenging the Implications section within which it seeks to question the continuing necessity for nuclear deterrence against nuclear threats. This section identifies a conclusion in the DoD report that the US is seeking a "sub nuclear cyber deterrence" option and speculates whether this could in time replace nuclear deterrence. It uses quotes on the potential for severe effects from a high level cyber attack to bolster this speculation that cyber capability could supplant nuclear capability as a deterrence against nuclear threat.

The DSB report indeed recommends that the US "*provide a non-nuclear but cyber survivable escalation ladder between conventional conflict and the nuclear threshold – that is to increase stability and build a new sub-nuclear red line in this emerging era of a cyber peer competitor delivering a catastrophic attack*". While it does not rule out a **nuclear** response to the most devastating **cyber** attack (something the UK has never yet considered in its declaratory policy) in no part of the report does it consider the possibility of a **cyber** capability being able to replace a **nuclear** deterrent against nuclear attack. Indeed, the potential for this was examined and rejected by the UK in the work leading up to the SDSR in 2010. I would argue strongly that the question asked in the implications section has been considered on both sides of the Atlantic and dismissed as there being nothing of sufficient devastating and immediate impact in any foreseeable cyber arsenal to deflect an adversary who is nearing, or who has passed, the nuclear employment decision.

Secondly, the **Unmanned Systems in ASW** report:

The author is a prolific writer on the subject of innovative technology and the weather and has a particular interest in drones. His book “Swarm Troopers” was published last year. In the 29 Feb paper through BASIC and again in several publications and via Twitter in late March he draws together a number of research activities, industrial product descriptions and imagined scenarios to weave a story of future near certainty of SSBN detection. While I would not begin to dismiss the potential for Unmanned Underwater Vehicles to add to the arsenal of those seeking either to find, or indeed hide, submarines, I think that on analysis the present whole is considerably less than the sum of its apparent parts.

I will briefly look at three areas in discussing the points raised in this paper:

- The continuing evolution in undersea warfare, particularly with respect to SSBN
- The challenges of scale and environment
- The problem of UUV stealth, and thus their own vulnerability

In setting the context it is worth examining the changing nature of both submarine and ASW operations over the past forty or so years to understand the forces which are bringing UUV slowly to the “party”. A particular and most challenging subset of this is SSBN and counter-SSBN operations, the nature of which has seen the greatest shift. In the early days of threat SSBNs which were noisy submarines with relatively short range missiles, the emphasis was on detection, tracking and if necessary marking, in order to be able to neutralise their threat on the commencement of hostilities. As submarines quietened, and patrol areas widened, this became both more difficult and less strategically relevant as it became increasingly uneconomic to develop capabilities for activities which would be seen as increasingly escalatory. In addition, assets designed to prosecute SSBN have seen their roles and utility across the spectrum of warfare - at sea and on the land - multiply. Thus through a combination of stealth, challenge and a gradual evolution in strategy the emphasis has shifted from prosecution of the adversary SSBN to a much wider range of roles, including protection of the patrol areas for one’s own SSBN. While never explicitly acknowledged, prosecution of SSBNs in peacetime has evolved from a core component of nuclear strategy to an activity which may now be seen as unnecessarily escalatory. Although there is no guarantee that this will remain the case should UUVs identified in the paper move from concept to genuine fielded capability, I believe that it should also not be assumed that a return to peacetime SSBN prosecution is a given.

Apart from the reduction in the ability and strategic ambition to conduct peacetime anti-SSBN activity, the challenge of scale and environment will complicate the introduction of relatively low cost UUV. The problems differ in the inshore, choke points and open ocean, but the scale advantages of the first two are diminished by the even more hostile environment. Firstly, the open ocean. While no-one outside the programme can know the exact areas which UK SSBN patrol, they are assuredly vast. Even if you consider the open ocean segments of just the North Atlantic and Norwegian Sea you have a search area of around 4.5 million square nautical miles. With a generous detection range against a modern allied SSBN, acoustically and through other fieldable sensors of 1km in all directions, this would demand nearly 5 million UUV. That would be clearly unworkable, so you would employ fewer sensors patrolling a smaller area. A detailed

analysis of search plans, return rate against a desired detection probability and ability to maintain track and ultimately prosecute would be required to calculate a number of UUV required to make the investment worthwhile. I would be surprised if a viable search and detection plan could be conceived for the open ocean with fewer than high tens of thousands or low hundreds of thousands of UUVs, which I would assess as still unworkable. So the operating area becomes identifiable choke points.

It is no secret but simply geography that SSBN deploying from the UK have to pass either north or south of Ireland to enter deep water. On the face of it these offer attractive choke points at which to station sensors, including UUV, to detect the passage of an SSBN. Indeed, during the majority of the Cold War, the Soviet Union placed intelligence ships upon the choke points and deployed submarines close to them in order to do just that to both deploying and returning UK and US SSBN. That they were unsuccessful points not only to the relative stealth advantage of allied SSBN but also to the significant difficulty in conducting ASW in a noisy inshore environment. UUVs would face the same challenges, with the additional one of being gathered and rendered inoperative by the many trawlers which criss-cross both areas. Submarines, while taking great care to avoid trawlers and their gear, usually consider them a challenge, not an ally. In the case of drifting or swarming UUVs, for once, the trawlers would be unknowing allies. Indeed, should the deployment of such UUV barriers become known then a perfectly valid and relatively low cost counter to them would be to employ a few trawlers to sweep the choke points when required.

The choke points also do not fully remove the challenge of scale. Even a relatively small "barrier" search in the two choke points would require several hundred UUV assuming the maintenance of a detection range of 1km (itself even more optimistic inshore); a more realistic (but still optimistic) inshore detection range of 500m would require around a thousand UUV. The operation of large numbers of UUV in these areas assume that the ships, submarines or aircraft deploying the UUV do so undetected or interdicted within or close to the UK's territorial waters.

While the NATO exercise DYNAMIC MONGOOSE, referred to in the article, showed successful utility of UUV detecting submarines in coastal Norwegian waters, the challenges of controlling and networking multiple UUV, let alone a thousand or more, have not yet been demonstrated and should not be underestimated. I have listened to and read the opinion of Kevin LePage, the NATO scientist in charge of the experiments in this series of exercises. Setting aside his rather oxymoronic conjunction of "tactical strategic" and that he appears to be referring to UUV deployed **from** a submarine, I see no evidence yet to support the last sentence in his statement, "*I think now miniaturizing the technology that the submarine is deploying, miniaturizing the sensors and having large numbers of sensors, we can start to own the underwater battlespace in a way that makes it less attractive. Takes away the tactical strategic advantage of the submarine*." It is certainly an ambition of those who continue to work the ASW problem, yet if there has been one constant in the changing ASW battle over the last forty years it has been that each decade someone has confidently predicted that the submarine's advantage was to be short lived and that "in the next decade the oceans will become transparent."

UUVs have been considered in a variety of ASW roles since their inception, primarily as an aspiration to reduce costs in a man and technology heavy enterprise. Yet ASW is evidentially much more of a human art than it is a science in a way that is vastly different from the relative certainties of the air-land battle. Even though increasingly capable computer algorithms have

improved the assistive technology for its protagonists no-one has yet been able to take the intuitive mind out of the loop with success. It is probable that advances in AI may in the future allow the human interaction to take place more remotely and perhaps ultimately not require the networking and data transfer from the UUV to a manned centre but even in the most optimistic advertising the next generation of UUV will not yet offer that.

Therefore these UUV will have a physical presence on or under the sea surface, and a detectable data transfer system to send their data to processors capable of analysis and ultimate classification. In addition, to threaten the SSBN, there would need to be some sort of additional prosecution capability. All of these: the physical UUV, the communications systems and the prosecution capabilities would have exploitable vulnerabilities which would vary depending on the chosen battlespace, but would be at their most vulnerable to interdiction or disruption in the inshore or choke point areas.

In conclusion, there is no doubt that those in acquisition continue to strive to introduce UUV into the underwater battlespace in as meaningful a way as the UAV has over land. That we are still years away from this after at least 20 years of ideas, promises and trials speaks volumes for the challenges yet to be overcome, and for the immutable differences in the environments in which UAV and UUV operate. In parallel to this the nature of ASW itself has changed. As nations have extended their SSBN missile range, their patrol areas have increased in scale and complexity and some have ceased operating SSBN in waters readily accessible to adversaries. Thus even searching for SSBN is a much more escalatory activity than it has been in the past, even should the technology become capable in the future. So the choice to employ UUV against SSBN, particularly in the coastal or territorial waters of the SSBN owner state is not simply a highly challenging technological one, it introduces political and strategic implications. In the open ocean, a realistic scale of effort is likely to be physically and economically unviable.

I am only too aware that a likely response from those who make claims of ocean transparency, or SSBN vulnerability is “prove that it is not so”. However annoying it may be to those who seek an open debate on issues of vulnerability of the UK nuclear deterrent, such a debate will not happen.

The research, analysis, investment in stealth and counters to emerging threat technology is quite correctly conducted within the highest classifications. My successor, and his successors, will brief as I did, a wide range of decision makers - senior military, civil servants and Ministers - on their assessments and recommendations, including parallel work, where shared, with key allies. Ministers will take decisions and make recommendations based on the conclusions of this work. While there is no room for complacency or spin, there is equally no room for conspiracy theories or “dossier loading” speculation - furthermore, any such unfounded allegations insult those men and women for whom this is daily business and who have no means to reply.

From my personal experience, I can assure that those involved, supremely conscious of the investment of blood and treasure in the deterrent and of the importance our successive Governments have placed on it for the security of the UK and of its allies and vital interests, take their responsibility extremely seriously. They would no more countenance ignorance of a potential risk to SSBN vulnerability than they would sharing their work outside those with a need to know.

UUVs are just one of the potential threat technologies on the radar of SSPAG and of those on both sides of the Atlantic for whom SSBN security is their daily bread. Notwithstanding the claims and extrapolations in the original article there was nothing in these technologies or their prognosis which caused me undue concern when I handed over my responsibilities in Dec 2014. Should that change, then I am confident that measures will be taken to exploit their own vulnerabilities and weaken any risk to an acceptable level, as has been the case since SSPAG analyses commenced with the first Polaris patrol in 1968.

There is certainly nothing in the current or projected technology which would materially alter the comprehensive government and other studies between 2006 and 2013, all of which recommended the replacement of the Vanguard class with a new class of SSBN as the only viable and economic means of maintaining the deterrent necessary for the ultimate security of the UK and her Allies in the current and foreseeable security environment.