Is Trident safe from cyber attack?

Article prepared exclusively for the European Leadership Network

February 2016

Dr Andrew Futter, Senior Lecturer in International Politics, the University of Leicester[1]

Last year, former UK Secretary of State for Defence, Des Browne, warned that UK nuclear weapons could "be rendered obsolete by hackers", and that without a comprehensive assessment of this risk to the Trident system, a future Prime Minister may not be certain they had a "reliable deterrent" that could be used when needed.[2] Lord Browne's comments, which were based on personal experience and a 2013 report from the US Defense Science Board,[3] have been met with a diverse reception; for some Trident is inherently safe from hackers because it is "air-gapped" from the wider Internet when the submarine is on patrol under the surface of the ocean; while others claim that cyber attacks could make the UK nuclear weapons system obsolete before work on the successor submarine even begins. Either way, the fact that Trident[4] relies on numerous computers, complex software and endless lines of code means it must be assumed to be vulnerable to interference in some way, and this new challenge seems set to play an increasingly important role in the forthcoming debate over renewal, and raise serious questions about the longer-term efficacy of the UK nuclear deterrent. As such, it is important to consider what we actually mean by "the cyber threat", what exactly might be vulnerable, in what ways, and to whom, before we can put the challenge presented to UK nuclear weapons in context.

First, **cyber is a fundamentally contested term**, which means different things to different people, and is not – or at least, should not be - considered as merely synonymous with the Internet. Instead, perhaps a better way to think of cyber is as involving the "command and control of computers",[5] and therefore to conceptualize cyber attacks as all efforts to disrupt, deny, degrade, distort or destroy the information that they rely upon, store, process and generate. While Trident is

---

[1] This article is the sole responsibility of the author, and does not necessarily reflect the position of the European Leadership Network or any of its members. To contact the author, Dr Futter, email ajf57@le.ac.uk.

[2] "Trident could be rendered obsolete by hackers", BBC News, (24 Nov 2015), http://www.bbc.co.uk/news/uk-politics-34903327

[3] United States Department of Defense, Defense Science Board, "Task force report: resilient military systems and the advanced cyber threat", (January 2013), http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

[4] Trident is used throughout the piece to refer to the entire system, which comprises; the Vanguard class submarine, the Trident D5 missile, the W76-class warhead, as well as support facilities ashore.

[5] This is the definition used by leading cyber expert Martin Libicki.

not connected to the Internet in any meaningful sense, the submarine, missile, warhead and all the various support systems rely on networked computers and software, and each of these have to be designed, written/ manufactured, incorporate new information, and be regularly upgraded, altered and patched.

Applied to the UK nuclear weapons context, this means we need to consider new vulnerabilities and challenges for; the submarine (such as stealth), systems aboard the submarine (such as the nuclear reactor or those needed for navigation), software that controls the missiles and the warhead (such as fire control, targeting and the yield/ type of detonation), as well as secret design or operational information about all aspects of the submarine, its weapons and those who operate them (indeed, humans remain a fundamental part of the cyber challenge). We also need to think about what certain adversaries may be trying to achieve through cyber, and how this may vary for example between traditional state-based foes (likely to seek to disable or undermine Trident) and other non-state or third party actors (who may wish to cause a crisis, miscalculation or accidental nuclear launch). Viewed in this way, the cyber threat to UK nuclear forces is actually more diverse and nuanced than perhaps it might first appear, and requires a little more unpacking than has often been the case in recent reporting.

By far the biggest fear and worst-case scenario is that hackers somehow compromise or sabotage the submarine or the weapons it carries. While advances are being made in technologies to "jump the air gap",[6] and UK submarines receive regular radio-transmissions from ashore that could theoretically be attacked (such as weather updates needed for targeting and the regular *FamilyGram*), this will almost certainly involve malware introduced during the procurement phase while the submarine/ missiles/ warheads are being built, or when the submarine is in port for maintenance, refurbishment and software updates. Likewise, while it may be possible to remotely activate certain pre-installed malware programmes while the submarine is on patrol, it is more likely that malware be pre-programmed to activate at a certain time or under certain conditions.[7] Given that the UK is likely on the cusp of building the next generation of nuclear-armed submarines, this challenge, and guarding against threats to the supply chain and overall maintenance, is particularly relevant now.

[6] See for example, Geoffrey Ingersoll, "US Navy: hackers 'jumping the air gap' would 'disrupt the world balance of power", *Business Insider,* (19 November 2013), http://www.businessinsider.com/navy-acoustic-hackers-could-halt-fleets-2013-11?IR=T

[7] Or it could simply be through the introduction of "doctored" hardware and software, such is rumored to have been the case with the huge explosion of a gas pipeline in Russia in 1982 as part of "Operation Farewell". See, Thomas Reed, "At the abyss: and insiders history of the Cold War", (New York, Presidio Press: 2007)

The most likely type of attack from a traditional state-based foe would presumably aim to disable or interfere with key systems on the submarine; for example, malware could be introduced to compromise its stealth (either software or some type of signal emitting beacon hidden in the hardware), the working and safety of the nuclear reactor (a fear that has been magnified by the reported success of the Stuxnet attacks against Iran[8]), or undermine the fire control systems[9] that manage the missile and the warhead so that they do not work, or at least do not work as expected.[10] That said many other systems could be targeted that would also cause considerable trouble for the submarine – the fresh water supply or sanitation system for example. All of these systems rely on computers and complex code, and all could theoretically be tampered with, causing the submarine to return to port and thereby end its deterrent patrol prematurely (particularly acute perhaps should the UK opt for three rather than four replacement submarines). However, it is highly questionable whether an adversary would be confident enough in the success of such malware to use it as a basis for an attack on the UK.

A second concern is that new cyber techniques might be used to interfere with communications to the submarines; either jamming or preventing the exchange of messages and data, or "spoofing" the submarines with misleading or incorrect information. The worst-case scenario here would be that unauthorized actors either managed to order nuclear use directly (perhaps through stealing and transmitting "go-codes" to the submarine – possibly acquired through cyber-espionage), or that cyber capabilities were used to mislead either the submarine or the UK government into thinking an attack was underway and that nuclear weapons should be readied for firing. This would most likely be the type of attack perpetrated by third party hackers or "cyber-terrorists", perhaps through so-called "false-flag" attacks (a major concern due to the problems of cyber attribution).

Given the relatively relaxed status of UK nuclear weapons when on patrol (aided by the stealth of the submarine and the requirements of UK nuclear posture), such interference would be unlikely to cause any major problems during periods of relative peace and security, but would perhaps, become much more acute during times of crisis. Indeed, cyber interference could well

[8] See Kim Zetter, *"Countdown to zero day: Stuxnet and the launch of the world's first digital weapon",* (New York, Crown Publishers: 2014)

[9] The Fire Control System is actually several different systems all with their own coding and software. Only the targeting code is written in the UK (the rest is produced by the United States). Flight data for missiles is stored in the Fire Control System outside the missile, once the missile is powered up and in flight, data goes from the missile to the warheads. For an excellent overview of this, see John Ainslie, "The future of the British bomb", (London, The WMD Awareness Programme: 2006), http://www.swordofdamocles.org/pdf/future.pdf

[10] While Trident SLBM's are astro-interial guided (by the stars), this still requires software and code.

compress the escalation ladder and make it increasingly difficult for all those involved to understand what was going on (particularly if this also involved denial of service attacks). While the risk is far greater for states with highly alerted forces (such as the US and Russia[11]), the chance of miscalculation, misperception, or unauthorized use due to "spoofing" remains a possibility- albeit perhaps a distant one. It is also conceivable that cyber capabilities might be used to undermine and hinder communications with UK submarines. In fact, there is evidence that hackers have attempted to compromise the extremely low frequency radio communications used to send launch approval messages to US nuclear-armed submarines in the past[12], and it must be assumed that the same is true for the communications hub for British SSBN's based at Northwood in the Chiltern Hills. Again, this would likely be manageable during normal operations, but would present new challenges during a crisis, especially given the fact that UK nuclear forces could likely be used in conjunction with NATO, and would therefore need to coordinate and communicate fairly widely, especially on attack plans with the US. That said, electronic warfare techniques and the threat of "jamming" have been around for decades.

Finally, perhaps the biggest challenge – although not as directly catastrophic as the other possible scenario's discussed above – is that sensitive design or operational secrets related to the UK nuclear weapons system (and those that operate it) be stolen through cyber espionage. Arguably the biggest threat is that highly classified details of the submarine, its key systems (such as stealth or navigation), the missile, the warhead, or its general area of patrol[13] (all likely stored on computers) might be stolen through cyber espionage. This could compromise the invulnerability of the submarine, or allow adversaries to develop countermeasures, anti-missile defences, and/or better anti-submarine warfare (ASW) techniques aimed at undermining the deterrent.

Such attacks might also be used to "map" out systems as a precursor for future attack and possible sabotage. The past is littered with attempts to steal secrets in this way, including against contractors involved in building the new successor submarine – a piece of malware known as the Zeus information stealing Trojan.[14] Defence laboratories and contractors in the US involved with

---

[11] "De-alerting and stabilizing the world's nuclear force postures", Global Zero Commission on Nuclear Risk Reduction, (April 2015), http://www.globalzero.org/files/global_zero_commission_on_nuclear_risk_reduction_report_0.pdf See also, Andrew Futter, "*War Games* redux? Cyberthreats, US-Russian strategic stability, and new challenges for nuclear security and arms control, *European Security,* 24 (2016), http://dx.doi.org/10.1080/09662839.2015.1112276

[12] Jason Fritz, "Hacking nuclear command and control", International Commission on Nuclear Non-proliferation and disarmament, (2009), www.icnnd.org/Documents/Jason_Fritz_Hacking_NC2.doc;

[13] While the area that SSBN's can patrol is vast, it is also limited by several factors, notably whether that part of the ocean has been fully surveyed and mapped.

[14] Richard Norton-Taylor, "Chinese cyber-spies penetrate Foreign Office computers", The Guardian, (4 February 2011),

manufacturing and maintaining the Trident missile and its software (which the UK relies on) have also been targeted by hackers looking for sensitive nuclear-related secrets,[15] and one must assume the same is true for the Atomic Weapons Establishment (AWE) in Berkshire where UK nuclear warheads are designed and maintained. It is also important to note that the majority of the code for the Trident missile and its fire control system is written in the United States – indeed, it is at least conceivable that US technicians have included coding that would prevent the missiles being targeted at the US, or possibly, without US authorization.[16] Again, it is unlikely they would ever admit this or make it public.

While Lord Browne is undoubtedly correct to point towards cyber as a major – and largely unknown – challenge for UK nuclear weapons, one must not forget that **those in charge of the UK nuclear weapons complex are not just standing idly by** while adversaries seek to cause havoc. In fact, concern about the possible compromise of computers used in nuclear command and control (C2) can be traced back to the 1960s,[17] and certainly to the 1983 Hollywood blockbuster *War Games*. All UK nuclear infrastructure, and especially the computers, software and coding in the submarine and various subsystems and weapons will be subjected to the highest levels of security, and be amongst the best protected against outside interference of any kind. Indeed, according to one source, the MoD regularly "red teams" various aspects related to the cyber and information security of UK nuclear weapons, and cyber concerns are one reason why the submarine, missiles and warheads regularly go through such rigorous testing and inspection routines. That said, the recent decision to use a windows-based operating system for UK submarines rather than the more expensive, but purportedly more secure Linux system used by the United States,[18] has caused concern amongst computer security experts.[19] However, for obvious reasons the UK MoD is reluctant to give any details about cyber attacks against various aspects of the UK nuclear weapons complex, and thus it is only possible to speculate on the nature and extent of potential vulnerabilities.

It would however be wrong to consider the cyber threat to the current Trident system and its likely successor in isolation. Other advanced technologies are also increasingly presenting

---

http://www.theguardian.com/world/2011/feb/04/chinese-super-spies-foreign-officecomputers

[15] Jason Koebler, "U.S. nukes face up to 10 million cyber attacks daily", *USNews,* (20 March 2012), http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily

[16] Ainslie, "The future of the British bomb".

[17] Gordon Corera, "Intercept: the secret history of computers and spies", (London, Weidenfeld & Nicolson: 2015) p.71-2

[18] While software is shared for the missile and fire control systems, the UK and US have different operating systems for their respective submarines.

[19] Lewis Page, "Royal Navy completes Windows for Submarines rollout", The Register, (16 December 2008), http://www.theregister.co.uk/2008/12/16/windows_for_submarines_rollout/

challenges to the current and especially the future UK nuclear deterrent system, and many of these augment and complement the new threats associated with cyber.[20] The spread and mounting capability of ballistic missile defences (BMD) as well as advances in ASW (such as underwater drones[21]), make guarding secrets about stealth technologies, patrol areas, missile and warhead specifics and performance data as important as ever, while the ever-increasing complexity and lines of code on which the submarine, missile and warhead rely, makes security of the supply chain and particularly software updates of paramount importance too. In sum, we are moving toward a more demanding techno-military deterrence environment in which cyber is a key - but not the only - part, and this will play an increasingly influential role in UK nuclear decision making in the years ahead.

The United Kingdom bases its small but highly sophisticated nuclear weapons capability on stealthy submarines somewhere under the ocean surface because this is believed to be the most invulnerable, credible and reliable platform available. **But it will never be possible to say that the UK nuclear deterrent is entirely safe from cyber attack**, or that it cannot be compromised or undermined in some other way in the future. The potential for an adversary of the UK to discover the patrol area of British submarines or the specifics of the boat, missile or warhead through cyber-espionage, the possibility of interfering with key systems in the procurement or maintenance phase, or the prospect of lacing targeting or fire-control software with malware, combined with better ASW and BMD capabilities, is clearly a serious issue.

However, while these challenges are undoubtedly significant, and a comprehensive assessment right across the UK nuclear weapons enterprise is clearly a must, **cyber threats do not necessarily mean that the programme should be scrapped**. Rigorous testing, security practices, and professionalism[22] should help mitigate the worse-case cyber scenarios described above, while many of the other challenges will simply have to be managed as we move into a more complex future nuclear deterrent environment. Ultimately, neither the UK nor any adversary can ever be completely confident about the invulnerability of the nuclear system, but the credibility of the deterrent rests less on the confidence of decision makers in the UK about cyber attack, and more

[20] See for example, Andrew Futter, "Trident Replacement and UK Nuclear Deterrence: Requirements in an Uncertain Future", 160:5 (2015), http://www.tandfonline.com/doi/pdf/10.1080/03071847.2015.1102548

[21] David Blagden, "What DARPA's naval drone could mean for the balance of power", *War on the Rocks,* (9 July 2015), http://warontherocks.com/2015/07/what-darpas-naval-drone-could-mean-for-the-balance-of-power/ and Paul Ingram, "Will Trident still work in the future?", *BASIC Policy Brief,* (22 January 2016), http://www.basicint.org/publications/paul-ingram-executive-director/2016/will-trident-still-work-future

[22] Notwithstanding the recent concerns raised by Trident whistleblower William McNeilly. See Heather Williams, "Britain's Trident, and the need to support nuclear personnel", *Bulletin of the Atomic Scientists,* (1 June 2015), http://thebulletin.org/britain's-trident-and-need-support-nuclear-personnel8363

on whether possible future opponents think the system can be undermined. Given where we are, it seems highly unlikely that any foe would take this risk.

The opinions articulated above represent the views of the author, and do not necessarily reflect the position of the European Leadership Network or any of its members.

The European Leadership Network (ELN) works to advance the idea of a cooperative and cohesive Europe and to develop collaborative European capacity to address the pressing foreign, defence and security policy challenges of our time. It does this through its active network of former and emerging European political, military, and diplomatic leaders, through its high-quality research, publications and events, and through its institutional partnerships across Europe, North America, Latin America and the Asia-Pacific region. It focuses on arms control and political/military issues, including both conventional and nuclear disarmament challenges inside Europe, and has a particular interest in policy challenges arising in both the eastern and southern peripheries of the continent.