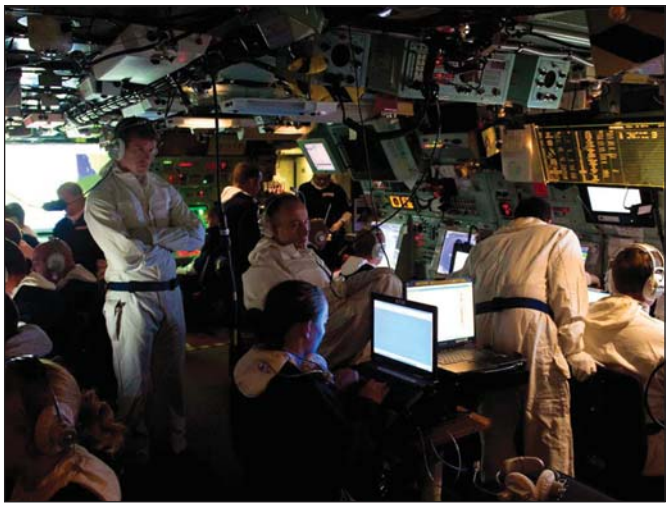
A Primer on Trident's Cyber Vulnerabilities

Parliamentary Briefings on Trident Renewal
Briefing No.2
March 2016

Aleem Datoo and Paul Ingram

Summary

Cyber threats impact both critical civilian infrastructure and all military systems dependent upon digital control and communications. Trident systems must be seen as a valuable cyber target for adversaries keen to neutralise any nuclear threat against them. If they can have some confidence of preventing a Trident launch, where does that leave nuclear deterrence? Cyber vulnerability also raises critical questions of strategic stability. Trident, intended for strategic deterrence, risks becoming a dangerous, destabilising liability.



Crew members of HMS Westminster in training scenario
Photo: Dan Rosenbaum, Royal Navy Media Archive

The Threat

Cyber comprises all the components and systems that provide digital information, including hardware, processors and software. Cyber warfare could involve attacks on critical civilian infrastructure or military systems. The United States, Russia and China have heavily invested in offensive cyber capabilities likely to be used alongside other capabilities in any conflict (as the Russians did in Georgia 2008 and Ukraine 2014). It is impossible to secure against such attacks with strong confidence.

> ***'The United States cannot be confident that our critical Information Technology (IT) systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities (a "full spectrum" adversary).'***
>
> **Defense Science Board Final Report, *'Resilient Military Systems and the Advanced Cyber Threat'*, January 2013, Opening sentence to the Executive Summary.[1]**

Contrary to claims often made, the so-called 'air-gap' between a patrolling submarine and other digital systems does not make it invulnerable to cyber attack. Malicious code or hardware can be introduced at the point of construction, overhaul or maintenance between patrols. It can even be vulnerable to the insider threat whilst on patrol, and could in future be vulnerable to electromagnetic or other forms of penetration in close proximity to the submarine.

A UK government Cyber Primer refers to a Ukrainian cyber worm that in 2008 penetrated all Windows network systems around the world, including the Royal Navy, MoD's administrative systems and the House of Commons in the UK.[2] The Trident system may not have been impervious to this attack: the Vanguard submarines operate on a submarine Windows system.[3]

An adversary penetrating military sites, contractors or sub-contractors, could gain access to highly sensitive information about Trident, from the specifications of the engineering behind the weapon, to communication on its location, patrolling patterns and doctrine. A more significant attack could sever communications, or corrupt or manipulate data.

A strategic nuclear system that is vulnerable to cyber-attack is one that could be neutralised at a critical moment. An opponent could penetrate the system and the code sit there for years, and the operators of the system know nothing about the intrusion until the code is executed. In particular, this could prevent firing. This could compromise confidence in Trident's ability to deliver a near-certain assured second strike capability.

Countermeasures

Tests can identify flaws and vulnerabilities of a system. But when millions of lines of code are involved in multilayer systems and attackers can craft a specialised attack that accounts for the various protection systems in place, it is never possible to assure complete security of a system.[4] That is not a reassuring situation when nuclear deterrence is involved.

Cyber-security to protect high-value targets can be far more expensive to implement than any particular attack they are designed to repel. The January 2013 US Defense Science Board (DSB) report found that "most of our [nuclear deterrent] systems have not been assessed against a [higher] tier cyber attack". It estimates the annual cost of addressing the more obvious cyber vulnerabilities would be $500 million.[5]

Since the DSB report, the Director of National Intelligence has named cyber attack as the highest strategic threat to the United States, ahead of terrorism. Significant investment has been allocated to resilience against cyber attacks, and to developing an offensive cyber capability for deterrence. The Third Offset Strategy in early 2016 appropriated $1.7bn over five years exclusively for cyber warfare.[6]

"DoD red teams, using cyber attack tools which can be downloaded from the Internet, are very successful at defeating [strategic DoD] systems"
2013 DoD DSB Report

The US Defence Science Board Report on cyber resilience in January 2013 concludes that:

- The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War
- DoD red teams, using cyber attack tools which can be downloaded from the Internet, are very successful at defeating our systems
- US networks are built on inherently insecure architectures with increasing use of foreign-built components
- With present capabilities and technology it is not possible to defend with confidence against the most sophisticated cyber attacks
- It will take years for the Department to build an effective response to the cyber threat to include elements of deterrence, mission assurance and offensive cyber capabilities.

Sonar Technicians conduct passive acoustic analysis training in sonar control room Photo: US Naval Forces

The key strategy is to upgrade weapon systems to qualify as High-Assurance Cyber Military Systems (HACMS), strategically designed to better withstand a cyber attack.[7]

The UK acknowledges the gravity of the threat in its 2013 Cyber Primer and its 2015 National Security Strategy and Strategic Defence and Security Review.[8] The latter promised £860 million for the creation of a cyber security strategy, but this primarily addresses cybercrime and security in the civilian sphere.

The advantages to a putative adversary from neutralising nuclear systems are obvious, so we could expect them to devote significant resources to doing so. Unfortunately it means that if systems are to be fielded with confidence, then major investments are required to plug vulnerabilities, rather than complacent assurances that systems are safe because they are insulated from the internet.

HMS Ambush Arriving at HMNB Clyde
Photo: Defence Images

Implications

Nuclear systems have only ever been one particular (and highly controversial) capability in the delivery of a credible strategic deterrent. States do not require identical capabilities against a particular threat to achieve stable deterrence, they simply need to be sufficiently credible in their efforts to dissuade opponents. The United States is now looking to create a non-nuclear "sub-redline" cyber attack force that can itself cause catastrophic results on an adversary as a primary deterrent.[9]

Sonar Technician and Republic of Korea Navy line officers during an anti-submarine warfare exercise. Photo: Naval Surface Warriors

Presidential Policy Directive 20 (2012) sets out the framework for America's offensive cyber posture, to be considered within the context of any other offensive capabilities.[10] It begs the question, is strategic cyber deterrence an option for the US President specifically to deter cyber attack, a means to expand the suite of deterrence capabilities into a new sector, or could it eventually replace nuclear capabilities that may become less reliable as a result of cyber vulnerabilities and the complexities created from nuclear proliferation?

Some theorists believe that offensive cyber capabilities are unlikely to deliver the same quality of strategic deterrence that nuclear weapons are claimed to have done up to now, largely because of the uncertainty of lasting effect.[11] However, recent US leaders leave no doubt as to the potential impacts from a major cyber attack. Former Chairman of the Joint Chiefs of Staff Mike Mullen, said "[t]he effects of a well coordinated, state-sponsored cyber attack against our financial, transportation, communications, and energy systems would be catastrophic."[12] When compared to the dwindling assurance from nuclear deterrence, offensive cyber capabilities may come to offer an attractive alternative strategic deterrent.

Could strategic cyber deterrence eventually replace nuclear capabilities that may become less reliable as a result of cyber vulnerabilities and nuclear proliferation?

Mutual cyber deterrence presents a host of worrying implications for strategic stability.[13] Some leaders may have greater confidence in their ability to prevail in any conflict, where it may appear more beneficial to strike first with a cyber attack out of the blue. Deterrence may be unsettled as the boundaries between the steps in the escalation ladder become more fuzzy, where attribution for an attack is unclear, and where the impacts may be global. Though PPD20 outlines a US commitment to work to establish international consensus for the control of cyber capabilities, there have not yet been any attempts to establish international cyber rules of engagement (bar a bilateral agreement in principle between the US and China that is completely unverifiable).[14]

It is clearly premature to conclude that states will see cyber capabilities as a more effective alternative to nuclear weapons to achieve strategic deterrence. But the uncertainty of the situation today for the future impact of emerging cyberwar is clearly relevant for leaders weighing up the decision to invest in expensive, long-lead, long life nuclear weapon systems such as Trident that could end up contributing to future strategic uncertainty rather than dampening it.

Endnotes

1 http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

2 *Cyber Primer* , Ministry of Defense, December 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360973/20140716_DCDC_Cyber_Primer_Internet_Secured.pdf pp. 223

3 Windows for Submarines, Microsoft UK Government Blog, 17 December 2008 http://blogs.msdn.com/b/ukgovernment/archive/2008/12/17/windowsforsubmarinestm.aspx

4 The DoD Cyber Strategy, 2015, p.34; *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* Defense Science Board, January 2013, p. 31

5 *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, Defense Science Board, Department of Defense, January 2013, p. 12 http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

6 New US Defense Budget: $18 Billion for Third Offset Strategy, Franz-Stefan Gady, The Diplomat, February 2016, http://thediplomat.com/2016/02/new-us-defense-budget-18-billion-for-third-offset-strategy/

7 High-Assurance Cyber Military Systems (HACMS), Dr. John Launchbury, Defense Advanced Research Projects Agency DARPA, http://www.darpa.mil/program/high-assurance-cyber-military-systems

8 The DoD Cyber Strategy, Department of Defense, April 2015, p. 9, http://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf ,

9 *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* Defense Science Board, January 2013, p. 41

10 Presidential Policy Directive 20, October 2012, p. 9, https://fas.org/irp/offdocs/ppd/ppd20.pdf

11 'Deterrence, Influence, Cyber Attack and Cyber War', Paul K. Davis, *International Law and Politics* , Vol. 47:327 http://nyujilp.org/wpcontent/ uploads/2015/11/NYI203.pdf

12 Posture Statement of Admiral Michael G. Mullen, USN, Chairman of the Joint Chiefs of Staff Before the H. Armed Serv. Comm.,112th Cong. 17 (2011)

13 'Deterrence, Influence, Cyber Attack and Cyber War', pp. 344-350

14 Is it time for a Geneva Convention on cyberwar?, James O'Malley, Little Atoms, 8 December 2015, http://littleatoms.com/world/genevaconventioncyberwar; PPD 20, October 2012, p. 17

About BASIC

BASIC seeks progress on the vision of a secure world free from the threat of nuclear weapons, involving a global move away from reliance on nuclear weapons within national security doctrines, leading to worldwide nuclear weapons disarmament, strong international measures to assure non-proliferation, and stronger international conditions and public opinion that underpin this.

3 Whitehall Court
Westminster
London
SW1A 2EL

E: **basicuk@basicint.org**
T: **+44 (0)20 7766 3461**
W: **www.basicint.org**

BASIC set up a three year review of Britain's current nuclear weapons policy in 2011 led by Sir Malcolm Rifkind MP, Lord Browne and Sir Menzies Campbell MP. The Commission comprised eminent members of the British political, security, diplomatic and scientific community, which completed a final report agreed by consensus, published in July 2014. The report was intended to inform the debate, not close it down. Commission members unanimously expressed their belief that this is a critical issue in its own right, and that the issues needed further consideration.

This series of briefings is intended to update Parliamentarians of critical, relevant issues in a year when the government intends to bring the issue of Trident's posture and the project to renew the system to a vote in the House. They are made possible by a generous grant from the Mulberry Trust. The briefings adopt the spirit of the Trident Commission, highlighting the need for Britain and other nuclear weapon states to consider more seriously the 'glide path' down the nuclear ladder.

Paul Ingram
BASIC Executive Director