Could Trident be hacked?

Aleem Datoo, British American Security Information Council (BASIC), outlines just how vulnerable the UK's nuclear weapons system is to cyber security threats.

Following global trends, UK military operations are increasingly dependent on a range of interconnected cyber networks. Cyber security for these military systems needs continuous assessment. The UK's Trident system[1] is particularly susceptible as a high-value target to a potential adversary and its elaborate design. All military systems have cyber vulnerabilities, and Trident is no exception.

The term 'cyber' comprises all components that relay digital information including both software and hardware and the human control, and a cyber attack is one that disrupts cyber dependent systems. Contrary to popular belief, the short history of cyber warfare has already proven[2] that 'air gapping'[3] a system is no assurance of invulnerability. A cyber attack can involve the introduction of malicious software or hardware at any point during operation, construction, overhaul or maintenance. A particular piece of malware can lay dormant and undetectable by the operators until it is activated by time delay, algorithm design or remote trigger.

The diversity of infection points, the vast number of computers, lines of code and pieces of hardware that form Trident's cyber system mean the vulnerability is real. A Cyber Primer published by the British government reported that in 2008 that a cyber worm from Ukraine penetrated all systems using Windows operating systems including those in the Royal Navy, the MoD's administrative systems and the House of Commons.[4] Royal Navy submarines use 'Windows for Submarines',[5] significantly more susceptible to malware than a bespoke system based upon Linux.[6]

The Trident system receives regular maintenance and patch-ups involving updating both the software and hardware, and this is when it is most vulnerable to the introduction of malware. This vulnerability will extend to the Successor submarines – now named 'Dreadnought' – whilst their software programs are written and hardware components are being designed by several private companies. Infiltration may not be immediately apparent and would likely involve remote or pre-programmed activation,[7] making an attack both difficult to identify and defend against. The effects that malware could have are varied. Its purpose could be to gather information, such as design details or the location of the submarine (rendering its stealth qualities futile). It could even impact or neutralise the basic function of the submarine or missiles.

Countermeasures are not simple. It is possible to build rigorous software defences against penetration and use 'red teams' to identify holes to be patched, but dealing with millions of lines of code based on a stock Windows system it is impossible to guarantee the system.[8] It is possible to reinforce the security of hardware design and maintenance, but much of this is conducted outside the UK or within private organisations not explicitly accountable for UK Trident's cyber security.[9]

According to the US Defense Science Board (DSB), the annual cost of reinforcing its cyber vulnerabilities is $500 million.[10] In a 2013 report, they claimed "most of our [nuclear deterrent] systems have not been assessed against a [high] tier cyber attack," and will look to address the military cyber vulnerabilities through the Third Offset Strategy.[11]

UK Defence Secretary Michael Fallon's attempts to give assurances in the context of growing concerns around cyber security for Trident in early 2016 rang somewhat hollow. "As for cyber-attack, while deployed, submarines operate in isolation. It is hard to think of a system [Trident] less susceptible to a cyber-attack."[12] Despite the UK's 2015 Strategic Defence and Security Review that promised £860 million for cyber security,[13] and despite the tests and inspections conducted on Trident systems by the Royal Navy,[14] Fallon's comments suggest a lack of understanding around the nature of cyber vulnerabilities.

States are directing significant resources into their offensive and defensive cyber capabilities. This, coupled with a critical lack of rules of engagement and mechanisms of attributability, necessitate an attention for all nuclear armed states to invest heavily in cyber defences for their systems, though it will never be possible to provide complete cyber security. The UK needs to conduct continuous and thorough assessments of the vulnerabilities to Trident, and the cyber dimension feature more in its decision making over the Successor Program. The danger that Successor submarines could become a significant security liability for the UK is real.

Aleem Datoo is a researcher with BASIC, and lead author of a briefing on Trident's cyber vulnerabilities.[15]

Notes and references

1. Referring to the Trident missiles, nuclear warheads and the Vanguard Class Submarines.
2. Manjoo F (2010). Don't Stick It In: The dangers of USB drives. Slate. October. http://www.slate.com/articles/technology/technology/2010/10/dont_stick_it_in.html
3. Physically segregated and incapable of connecting with other computers or network devices.
4. pp.2-23 of: Ministry of Defence (2013). Cyber Primer. December. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360973/20140716_DCDC_Cyber_Primer_Internet_Secured.pdf
5. Microsoft UK Government Blog (2008). Windows for Submarines. https://blogs.msdn.microsoft.com/ukgovernment/2008/12/
6. Borger J (2016). 'Trident is old technology': the brave new world of cyber warfare. The Guardian. January. https://www.theguardian.com/technology/2016/jan/16/trident-old-technology-brave-new-world-cyber-warfare
7. Futter A (2016). Is Trident Safe From Cyber Attack? European Leadership Network. February. http://www.europeanleadershipnetwork.org/medialibrary/2016/02/04/d2106a19/Is%20Trident%20safe%20from%20cyber%20attack.pdf
8. p.31 of: Defense Science Board (2013). Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. Department of Defense. January. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf
9. Farmer B (2016). Trident Upgraded to Protect Against Cyber Attack. The Telegraph. March. http://www.telegraph.co.uk/news/2016/03/29/trident-upgraded-to-protect-against-cyber-attack/
10. p.12 of: Defense Science Board (2013) – as note 8.
11. Gady FS (2016). New US Defense Budget: $18 Billion for Third Offset Strategy. The Diplomat. February. http://thediplomat.com/2016/02/new-us-defense-budget-18-billion-for-third-offset-strategy/
12. MacAskill E (2016). MoD Showing Contempt for the British Public Over Trident, says Labour. The Guardian. March. https://www.theguardian.com/uk-news/2016/mar/23/classified-analysis-says-trident-will-not-become-obsolete-says-fallon
13. p.40 of: HM Government (2015). National Security Strategy and Strategic Defence and Security Review 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
14. As note 7.
15. Datoo A, Ingram P (2016). A Primer on Trident's Cyber Vulnerabilities. BASIC. July. http://www.basicint.org/publications/aleem-datoo-paul-ingram-executive-director/2016/primer-trident%E2%80%99s-cyber-vulnerabilities