HACKING UK TRIDENT:

A Growing Threat

BASIC

JUNE 2017

BASIC

Stanislav Abaimov and Paul Ingram

British American Security Information Council (BASIC)
3 Whitehall Court
Westminster
London SQ1A 2EL

Charity Registration No. 1001081

T: +44 (0) 20 77663465
www.basicint.org

Disclaimer

Only publicly available information has been used in the research behind this publication. No classified information has been disclosed. We have been careful not to include a level of detail that could be of use to any group that might be motivated and capable of compromising the security of the operational systems concerned. Any cyber-attacks that have any hope of success could only be mounted by a highly-sophisticated group probably with the backing of a major state. This report will have no impact upon the awareness or capabilities of any such group.

We have included in this report a number of scenarios to illustrate the type of threat this report is discussing. The stories, characters and incidents portrayed in those illustrations are fictitious. No identification with actual persons (living or deceased), specific subcontractors, hacking groups or foreign entities is intended or should be inferred.

The Authors

Stanislav Abaimov is a PhD researcher in Cyber Security and Electronic Engineering in the University of Rome, Tor Vergata. He has earned a degree of MSc in Information Security, Royal Holloway, University of London, an Academic Center of Excellence in Cyber Security, certified by EPSRC and GCHQ. He is also a graduate of the Moscow State Institute of Electronics and Mathematics, faculty of "Automated Systems and Informatics in Control Systems". During his Master Studies Stanislav conducted his research in the field of Advanced Persistent Threat, security testing, digital forensics, and cyber warfare and defence. His Ph.D. research focuses on CBRNe cyber security and Industrial Control Systems in Critical Infrastructure. Stanislav is supporting research in SCADA systems in CBRNe and Critical Infrastructure, ICS malware and his interests vary from cyber security in ICSs and Autonomous Weapons Systems to Wireless Communications, Threat Modelling, Network Analysis, and Cyber Defence.

Paul Ingram is BASIC's Executive Director. Paul has authored numerous BASIC reports and briefings covering a variety of nuclear and non-nuclear issues since 2002, including cyber security and emerging vulnerabilities of SSBNs. He has extensive media experience and formerly hosted a weekly peak-time talk show on IRINN (Iranian domestic TV News in Farsi) from 2007-2012, addressing issues relevant to global security. Paul also taught systems approaches on the flagship Top Management Programme at the UK Government's National School of Government from 2006-2012.

British American Security Information Council (BASIC)

BASIC is a think tank based in Whitehall in London, taking a non-partisan, inclusive and dialogue-based approach to encourage stable global nuclear disarmament, arms control and non-proliferation. The organization works to facilitate constructive engagement between siloed communities on traditionally sensitive or complex issues of nuclear policy, to create space for new and diverse perspectives to grow from those interactions. Over the 30 years since the organization was founded, in 1987, BASIC has developed institutional expertise across a number of transatlantic issue areas, including the UK-US nuclear relationship, the UK's Trident programme, the politics of disarmament and arms control in the UK Parliament, NATO nuclear weapons in Europe, the Middle East, the evolving role of responsibility in nuclear governance, and expanding technological threats to SSBN platforms.

Executive Summary

This paper reviews the growing potential for cyber-attack on the UK's operational fleet of Vanguard-class submarines armed with nuclear-tipped Trident II D-5 ballistic missiles, and some of the implications for strategic stability.

A successful attack could neutralise operations, lead to loss of life, defeat or perhaps even the catastrophic exchange of nuclear warheads (directly or indirectly). But the very possibility of cyber-attack and the growing capability to launch them against SSBNs, could have a severe impact upon the confidence of maintaining an assured second-strike capability and therefore on strategic stability between states. Recent suggestions that the fleet is vulnerable have sometimes been met with complacency and claims that the isolated 'air-gapped' systems cannot be penetrated. Whilst we recognise that it is important not to be alarmist, these claims are false.

In a time of global interconnectivity and enhanced accessibility to cyber tools, cyber warfare has already become a vital component of conventional warfare, a new military domain in its own right. We are not talking about a lone wolf teenager in a basement hacking into the controls of a missile and warhead and starting a nuclear war. Rather, we consider the most significant threat by some margin originates from the expanding investments by leading states in their offensive cyber capabilities, alongside their exiting intelligence networks. The exponential growth in the complexity of cyber-attack techniques outmatches the defensive capabilities, a trend that can only continue partly because any defensive operations have to anticipate all possible attack vectors before they are mounted, and partly because the most effective form of defensive cyber operation involves offensive cyber intelligence (hacking into one's opponents' systems to glean information on what it is they are attempting to penetrate and why). This has a transformative impact upon all forms of warfare. But there is a particular danger associated with nuclear weapons by virtue of their destructiveness that demands policy makers and those responsible for managing the systems to consider more seriously the dangers involved when deploying nuclear weapon systems in an ever-changing technical and strategic environment.

Malware injection during manufacturing, mid-life refurbishment or software updates and data transmission interception allow potential adversaries to conduct long-term cyber operations. BASIC has already highlighted the future potential for emerging technologies to deliver high confidence in global detection of submarines.[1] Future weaponized underwater drones may facilitate close proximity kinetic and cyber-attacks on ballistic missile submarines (SSBNs). Advanced nano and bionic technologies such as implantable and subdermal data storage and communication devices may be smuggled into the vessel and activated autonomously, manually or remotely.

This report considers the major electronic network and communication systems associated with the UK Trident system to identify its level of exposure to modern and future cyber-attacks. It reviews the submarine systems architecture and its *modus operandi*, and identifies potentially applicable cyber-attack techniques and scenarios. As it is based upon publicly available sources, its conclusions cannot be considered final or definitive.

The report provides illustrative attack vectors aimed at disrupting, destroying or endangering operations. On the other hand, it also confirms that it takes sophisticated, well-resourced and sustained cyber-attacks to exploit the vulnerabilities in remote submarine subsystems. These attacks are beyond the scope of all but the most well-resourced and extensive non-state groups. Essentially, the principal threat comes from other states' cyber operations alongside extensive and highly sophisticated intelligence activities.

The overall submarine network architecture is physically isolated from the internet and any civilian network, thus severely limiting the possibility of real time external access into the command network by remote hackers. This does not prevent attacks from inside the submarine or the prior injection of malware into submarines, missiles, warheads or other infrastructure at the manufacturing, construction and maintenance stages. Regular radio-transmissions from ashore could be used for limited bandwidth cyber-attacks, spoofing or activating pre-installed malware programmes. Such highly covert, adaptive and targeted programmes could be designed to trigger in response to particular events. This was the case in the advanced malware used in the so-called 'Stuxnet' or 'Olympic Games' attack on Iran's centrifuge systems, a cyber-physical attack that was delivered into Natanz by unsuspecting subcontractors.

The report concludes that the vulnerability to cyber-attacks is real. It can be reduced by significant, vigilant and continuous cyber protection, but cannot be eliminated. It is therefore essential that in addition to significant investment in cyber defence, those responsible also need to consider strategies that build resilience within the systems, and to incorporate this threat into broader assessments relevant to the choice of weapon systems, platforms and broader defence and security strategies.

"In addition to significant investment in cyber defence, those responsible also need to consider strategies that build resilience within the systems, and to incorporate this threat into broader assessments relevant to the choice of weapon systems, platforms and broader defence and security strategies."

The challenge of maintaining covert and secure patrols under reliable operational control is of utmost importance to an effective nuclear deterrence posture based upon submarines. The continuous and rapid development of new cyber technologies will inevitably result in some loss of confidence in future patrols, with negative results on strategic stability. It is crystal clear that the highest level of priority must be given to cyber protection at every stage in the construction of the UK's Dreadnought class, across the whole supply chain, if the UK is to contain this hit on confidence. This will inevitably have major implications for the programme budget, with uncertain success.

1. David Hambling, *The Inescapable Net: Unmanned Systems in Anti-Submarine Warfare*, British American Security Information Council, (13 July 2016), http://bit.ly/1RC55KE

FICTIONAL SCENARIO 1:

A strategy to acquire Dreadnought-class SSBN designs

Memo Dated: 17 March 2012

From: [Foreign] Naval Intelligence, Unit 6B

Mission: To steal Successor-class SSBN Designs for the purpose of ascertaining its capabilities, likely patrol characteristics, weaknesses in its stealth, and for developing naval capabilities to seek and destroy the Dreadnought once it is on patrol.

Objective: Attack the network systems of Gyro Instruments Ltd (GI), a UK-based sub-contractor involved in design and development, and the supply of components.

Method: *Remote access to GI's network. Failing that to deploy intelligence assets to conduct direct physical intrusion on site.*

Using acquired and/or developed tools, our arms-length cyber-team *DEVCOM_2* will perform remote reconnaissance, enumeration and vulnerability scanning, weaponization (acquisition and preparation of tools), exploitation (including zero-day exploitation) and initial breach.

If GI has air gapped a number of its systems or a network segment from the internet, *DEVCOM_2* will investigate options for gaining authorised access to those systems. It may be that there are indirect means to enter via third-party network connections, using lateral movement techniques and acquired credentials during the operation, and then ensuring our code propagates to the primary target.

If the target network is completely isolated from the internet or other networks *DEVCOM_2* will report back and we will activate Secret Intelligence Service sleeper operatives (KL56 and NU7) currently based in Leeds, about 50 miles from the site. They will gain access to the target network as contractors or employees using physical devices supplied by the team (we are still exploring possibilities, but could include nano-routers, antennas, microcomputers, etc.). This will enable the *DEVCOM_2* to bypass what perimeter defences may be in place. Once they have access and have acquired the designs these will be forwarded to the forensic team in Unit 61 for analysis. They will explore options to maintain continuous and permanent surveillance throughout the supply chain, manufacture and operation of UK Successor submarines.

Contents

1. Introduction 8

2. The Origin of the Cyber Threat 11

3. Command and Control of the Trident System 16

4. Attack Vectors on Trident 18

4.1 Air gapping 18

4.2 Potential attack vectors on the whole system 19

4.3 Supply chain and construction 19

4.4 Patrolling 20

4.5 Maintenance 20

5. Vanguard's Electronic Vulnerabilities 21

5.1 Communications to and from the submarine 22

5.2 Internal submarine networks 23

5.3 Navigation 25

5.4 Life support 26

5.5 Reactors and power supply 26

5.6 Command and control of missiles and warheads 26

5.7 Advanced persistent threat 27

6. Implications of These Vulnerabilities 30

7. Counter Measures 31

8. Future Related Trends 33

9. Conclusion 36

1. Introduction

Cyber threats have co-exited with the emergence and ubiquitous use of computers to control critical systems.

Cyber warfare has also been with us for some time but has achieved a scale that matches the highest priority military programmes only recently. In the context of this report, the principal threat arises from state hacking capabilities, principally because it is states that possess the necessary resources, intelligence and motivation to target nuclear weapon systems.

Trident, based upon a fleet of four Vanguard class ballistic missile submarines, is the only nuclear weapon system operated by the UK. In 2016, the UK Ministry of Defence stated its purpose as to "deter the most extreme threats to our national security and way of life [nuclear attacks by other states], which cannot be done by other means".[3] Each of four submarines when on patrol carries forty independently-targetable thermonuclear warheads on eight Trident ballistic missiles. They are based at the Clyde Naval Base near Glasgow, Scotland, and operate a continuous patrolling posture. Relying as it does upon numerous computers, complex software and endless lines of code, the Trident system is undeniably vulnerable to cyber interference.

It is obvious, but needs to be stated clearly, that cyber-attacks are not exclusively limited to those conducted over the Internet. They can target the command and control of computers and network connected devices, and therefore refer to any efforts to steal, disrupt, deny, degrade, distort or destroy the information that these systems rely upon, store, process and generate.

Trident's sensitive cyber systems are not connected to the internet or any other civilian network. Nevertheless, the vessel, missiles, warheads and all the various support systems rely on networked computers, devices and software, and each of these have to be designed and programmed. All of them incorporate unique data, and must be regularly updated, upgraded, reconfigured and patched.

"We take our responsibility to maintain a credible nuclear deterrent extremely seriously and continually assess the security of the whole deterrent programme, as well as its operational effectiveness, including against threats from cyber."[2]

Spokesperson for UK Ministry of Defence, 30 March 2016, apparently in response to articles in the Guardian and Independent suggesting there existed a serious cyber threat to Trident.

Applied to the UK nuclear weapons context, this means we need to consider ever-emerging vulnerabilities and challenges for the following:[4]

- the vessel (stealth, submerged state, etc.);
- systems aboard the vessel (the nuclear reactor, navigation, life support, etc.);
- control software for the missiles, the warheads and the torpedoes; and
- secret design or operational intelligence about all aspects of the submarine, its payload, the crew and the directives.

The House of Commons voted on 18th July 2016 by a large majority to proceed with building a replacement fleet of Dreadnought-class submarines to be operational by the early 2030s, thereby extending operations to at least the 2060s.[5]

Recently leaked classified data from the US Central Intelligence Agency (CIA) disclosed numerous malware and exploits used for cyber offensive operations and surveillance.[6] They include, among others, technologies able to remotely connect to consumer communication devices (iPhones, Android phones, smart TVs, and Microsoft Windows, MacOS and Linux (multiple) operating systems). The Guardian alleges that the thousands of leaked documents focus mainly on techniques for cyber operations and reveal how the CIA cooperated with British intelligence to engineer a way to compromise smart televisions and turn them into improvised surveillance devices. A programme called Weeping Angel describes how to manipulate a Samsung F8000 TV set so that it appears to be off but can still be used for monitoring. A CIA attack system called Fine Dining provides 24 decoy applications for CIA spies to use for covert operations that require physical presence of the agent inside or outside the

The WannaCry cyber attack

The ***WannaCry* ransomware cyber worm attack** is an ongoing cyberattack targeting the Microsoft Windows operating system. It started on 12 May 2017, having infected more than 230,000 computers in 150 countries with the software demanding ransom payments in the cryptocurrency bitcoin in 28 languages. The attack has been described by Europol as unprecedented in scale. The systems affected by the *WannaCry* attack around the world included hospitals, doctors' surgeries, banks and ATMs, transport systems, trains and airlines, ticket sales, car production plants, telecoms firms, power providers, logistics firms, schools and universities, and the Russian Interior Ministry.

Virus Name: *WannaCrypt, WannaCry, WanaCrypt0r 2.0, WCrypt, WCRY*

Vector: All Windows versions prior to Windows 10 are vulnerable, if not patched with the MS-17-010 update. The malware exploits the *EternalBlue* MS17-010 vulnerability to propagate (discovered by the NSA and stolen by the cyber-criminal group Shadow Brokers).

Ransom: $300 to $600.

Backdooring: The worm loops through every RDP session on a system to run the ransomware as with user-level privileges. It also installs the *DOUBLEPULSAR* backdoor. It corrupts shadow volumes to make recovery harder. (source: Malwarebytes)

Kill switch: If the website: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com is up the virus exits instead of infecting the target (source: Malwarebytes). This domain has been reregistered, removing the access to command and control of the malware. This action that stopped the spread of the worm.

Legacy: A minor variant of the virus has been found, with the kill switch edited out (disallowing the remote shutdown of the malware), allegedly not created by the original malware author. The ransomware module is corrupted, however, and does not work – the worm only propagates. Yet the encryption keys and the bitcoin addresses are the same.

Microsoft issued its first patch for Windows XP since 2014.

target facility.[7] Multiple instances of the disclosed developed and improved malware are able to jump air-gapped security systems (over USB drives, local wireless networks, etc.).[8]

The recent global attack that hit on 12 May 2017 involved the *WannaCry* worm. This was reported to have originated from a sophisticated cyber weapon developed by the US National Security Agency (NSA) that exploited vulnerabilities in Windows operating systems they had identified. This had been stolen by the hacker group, the Shadow Brokers, and released online. Microsoft had distributed the patch MS17-010 to address this vulnerability a month before it was stolen by the hacker group Shadow Brokers. However, those systems whose operators did not download the patch remained vulnerable and the worm attacked two months later.[9] The Shadow Brokers claim to have a large number of other cyber weapons they have acquired, and are threatening to release them regularly.

Whilst there has been much talk of the development of offensive cyber capabilities across many sectors, and growing investment by governments in these techniques and the means to combat them, there has been surprisingly little consideration given in public to the resulting emerging vulnerabilities to the Trident system and similar nuclear weapon systems. One notable exception to this is the excellent report, *Cyber Threats and Nuclear Weapons,* authored by Andrew Futter, published by the Royal United Services Institute in July 2016.[10] Futter explored amongst other things in that occasional paper the exposure of nuclear weapon systems to cyber espionage and sabotage, and the wider implications for strategic stability. This report picks up and expands on a some of the themes in that report and applies them specifically to the UK systems around existing Vanguard and future Dreadnought submarines.

2. UK Ministry of Defence, *Defence in the media – Wednesday 30th March 2016*, Ministry of Defence, (30 March 2016), http://bit.ly/2qAbVaJ
3. UK Ministry of Defence, *UK Nuclear Deterrence: What You Need to Know,* Policy Paper, (24 March 2016), http://bit.ly/1WRHC83
4. The Defense Technical Information Center, *Universal Joint Task List*, (16 May 2017), http://bitly/2ruAyWd
5. BBC, 'MPs Vote to Renew Trident Weapons System', (19 July 2016), http://bbc.in/29Q4eDl
6. Wikileaks, 'Vault 7: CIA Hacking Tools Revealed', (7 March 2017), http://bit.ly/2naI1Id
7. Ewen MacAskill, 'WikiLeaks publishes 'biggest ever leak of secret CIA documents', *The Guardian*, (7 March 2017), http://bit.ly/2lYPxou
8. Swati Khandelwal, '10 Things You Need to Know about "Wikileaks CIA Leak"', *The Hacker News*, (8 March 2017), http://bit.ly/2n75w4E
9. Warwick Ashford, 'Businesses Urged to Apply Windows Patch to Avert WannaCry Attacks', *Computer Weekly*, (15 May 2017), http://bit.ly/2rjqizZ
10. Andrew Futter, 'Cyber Threats and Nuclear Weapons', *RUSI Occasional paper*, (July 2016), http://bit.ly/2qvhgBP

2. The Origin of the Cyber Threat

Cyber warfare involves "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption",[11] but other definitions can sometimes encompass non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists and transnational criminal organizations.

Considering the range of motivations behind cyber-attacks and the capability of groups to conduct them enables better assessment of the threat and the prediction of which systems have to be secured.[12] On both counts, in the context of Trident systems, it seems most likely that attackers will be states.

When a UK Trident crew member went public in 2015 with his many concerns about lax security and poor safety at the Faslane naval base and on board the Vanguard submarines themselves, his prime expressed concern was that terrorists could gain access to the system.[13] His evidence notwithstanding (and it included some surprising and alarming claims), there are so many vulnerable systems that would deliver the desired effect that it seems unlikely terrorists would target Trident systems. Hacktivists and cyber criminals currently do not possess sufficient capability to conduct operations of the required scale and sophistication relevant to penetrating Trident systems, as far as we can judge. So the principal threat, and the one considered in this report to be most relevant, comes from other states, particularly those that have the potential to emerge as strategic competitors to the United Kingdom and its allies.

Industrial espionage and backdoor injection during manufacturing allow adversaries to conduct long-term cyber operations that may operate for years before they are discovered. Cyber-attacks are also used for military surveillance, warfare support and in recent years, for full-scale operations in their own right. Over the past decade, cyber warfare has become a vital part of conventional warfare and a new military domain.

States have a strong incentive to discover the patrolling locations of other states' submarines, their design and detailed capabilities, their defences, tactics and other operational details and acquire an edge in the naval military contest or even to neutralise a nuclear threat. This can be achieved either by using this intelligence in combination with its more physical naval assets, or by deploying cyber tools directly to degrade an opponent's ability to hide and deliver nuclear warheads on target. The suite of tools available for cyber intrusion is rapidly proliferating and improving.[14] When used in combination with other intelligence assets (such as rogue officers, crew members, maintenance and other personnel), the capabilities of states to infiltrate are significant.

Those responsible for defending against cyber-attacks can attempt to isolate critical systems and anticipate the numerous possible methods of attack, whilst minimising inconvenience for their authorised users. Cyber intrusions are covert and virtually impossible to attribute if conducted with expert-level operational security. They vary based on motivation of the attackers, targetable assets and the activities conducted by attackers.

Malware and attacks involve malicious software used to disrupt computer or mobile operations, gather sensitive information or gain access to computer systems. Malware injection requires prior knowledge of the software and hardware architecture and a delivery mechanism and can sometimes grant virtually full control over the target system or even network.

Some relevant cyber incidents

One of the earliest publicly announced events related to the CBRN infrastructure vulnerability to cyber attacks occurred in January 2002. The Slammer worm successfully breached the perimeter network defences at Ohio's Davis-Besse nuclear power plant (employees claim the network was protected by a firewall), infiltrated a private computer network and disabled a safety monitoring system for nearly five hours.

The 2010 *'Stuxnet'* event in Iran confirmed that information technology could be used not only to trigger remote CBRN attacks, but also could be seen as a direct threat to physical CBRN ICS equipment. *Stuxnet* was the first malware to infiltrate and cause physical and tactical disruption in multiple ICSs in a CBRN facility (the uranium enrichment plant) and numerous other facilities over two years with similar equipment. But it also infected computer networks across the global internet, and the cyber security community and CBRN defence experts united in their attempts to neutralise its spread and protect the integrity of global digital systems.

In 2011, the Trojan *'Poison Ivy'* was used to collect intellectual property from 29 international chemical companies. It was one of the largest acts of industrial espionage in history, raising the awareness of cyber security specialists in the topic of cybersecurity of critical infrastructure.

In an attack attributed by some as a retaliation for *Stuxnet,* the Malware *'Shamoon'* in 2014 wiped 30,000 workstations in Saudi Aramco's corporate network, raising concern over cyber-attacks that can bypass firewalls and intrusion detection systems to physically affect operations technology networks in a large scale.

In 2014, 13 different types of malware disguised as ICS/SCADA software updates (such as Siemens Simatic WinCC, GE Cimplicity and Advantech) were detected in spear-phishing emails. After a due forensic investigation, the malware was identified as the re-purposed banking Trojan, aiming to collect private information and credentials. This event confirms the capabilities of ICT malware to be used against industrial networks.

The world's first proof-of-concept PLC worm was presented at BlackHat 2015 conference (August 2015), showcasing the malware that can replicate itself directly from one PLC unit to another, attacking ICS firmware and hardware.

In December 2015, the Denial of Service in a power plant and multiple substations in Ukraine triggered a power outage. In February 2016, it was acknowledged that BlackEnergy malware was used for the cyber attack.

DATE	MALWARE	SCOPE	CYBER TOOL(S) USED	ANNOUNCED
2007	BlackEnergy (First generation)	Targeted Denial of Service on 54 communications, finance and government websites in Georgia	HTTP-based DDoS botnet	2008
2009–2010	Stuxnet	Centrifuged compromised in Natanz Nuclear Facility	ICS override	2010
2010	BlackEnergy2	Cyber-Fraud in Ukrainian and Russian banks	Rootkit, credentials capture	2010
2011	Duqu	Espionage in the Middle East (scope unknown)	Information gathering about ICS, Keylogger	2011
2012	Flame	Espionage in the Middle East (scope unknown)	Modular malware	2012
March 2015	BlackEnergy3	Power outage in Ukraine, impacting 225,000 customers	Modular malware, ICS override	December 2015
2015	Irongate (First generation)	Detected on VirusTotal by FireEye*	Man-in-the-Middle attack, Sandbox evasion	2016
2017	WannaCry	Over 300 000 Computers and systems running Windows operating systems infected and held for ransom	Ransomware	2017

"Sabotage can involve the introduction of autonomous malware during the development, procurement or configuration phase while the submarine, missiles, warheads or any other internal system, are being built, or when the submarine is in port for maintenance, refurbishment and software updates."

Of course, UK Trident submarines, once commissioned, are only out at sea around 30-45% of the time. Sabotage can involve the introduction of autonomous malware during the development, procurement or configuration phase while the submarine, missiles, warheads or any other internal system, are being built, or when the submarine is in port for maintenance, refurbishment and software updates. Remote radio transmissions to the submarine could be used to activate any covert dormant malware in one of the systems on board (if the malware has access to the receiving software/ hardware, or the activation signal is properly relayed to the malware process). It is more likely, however, that malware would be pre-configured to activate in response to a particular event (such as the order to launch a missile).

Autonomous Denial of Service (DoS) of the internal systems, delivered by pre-installed malware (hardware or software), may cause inconvenience, distraction or severe disruption of any affected systems (even auxiliary). This may be a primary or a secondary goal of the attackers, to orchestrate a chain of events and carry out a sophisticated multidimensional attack.

A cyber-attack may target the submarine, command and control, or the missile launch system. It can attempt to disrupt or change launch coordinates to divert the original course of the missile, or to disrupt or neutralise the warheads themselves.

11. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st edition, HarperCollins, (2011)
12. Tyler Moore, Cyber War, Wellesley College, (6 December 2010), http://bit.ly/2pXmjbk; Tavish Vaidya, '2001-2013: Survey and Analysis of Major Cyberattacks', *Georgetown University*, (July 2015), http://bit.ly/2ruP0wF; Arthur Beesley, 'EU Suffers Jump in Aggressive Cyber-attacks', *Financial Times*, (8 January 2017) http://on.ft.com/2i9gR3T
13. William McNealy, 'The Secret Nuclear Threat', (May 2015), text available on Nuclear Information Service website, http://bit.ly/2qVpYKW
14. Col Williams J. Poirier, Maj James Lotspeich, 'Air Force Cyber Warfare: Now and the Future', *Air & Space Power Journal*, (September-October 2013), http://bit.ly/2p4t9OA

FICTIONAL SCENARIO 2:

A possible strategy to infiltrate UK SSBN Command and Control

Memo Dated: 23 February 2018
[Foreign] Naval Intelligence, Unit 6B

Mission: to develop the capability of disrupting and neutralising UK and NATO SSBN Command and Control via remote access.

Objective: to infiltrate and compromise the network of the UK submarine command Northwood HQ, UK and establish ability to launch Denial of Service or other cyber-attacks at a time of our choosing and without detection.

Method: Establish remote access to Northwood's network and on-going hardware and operations surveillance using APT tactics and a variety of cyber tools that deliver the ability to neutralise communications to patrolling SSBNs. To trigger the intelligence asset on site and additional assets in London with established ability to access secure facilities as contractors, and to insert unauthorised hardware and software facilitating the objective.

The mission will commence by commissioning our arms-length cyber-team DEVCOM_2 to assess network exposure, and scope out options to determine the components of an extended APT operation on the facility network. This will require an audit of suppliers to the facility with the purpose of identifying vulnerable systems to act as entry nodes into the secure network.

We need to make early contact with the intelligence asset already inside Northwood to establish possible entry points and requirements. At the same time, to operationalise commercial assets in London to establish technical credentials and cover stories for future entry. At the right time we need to transport preconfigured hardware into the operation, for connection into the Network. This could then facilitate system error and/or force the unscheduled reboot and prevent normal loading process (disable certain services), enable us to bypass the authentication and possibly to load system-level privileges for remote access by DEVCOM_2.

3. Command and Control of the Trident System

UK nuclear weapons are predicated on the idea that they guard the nation against nuclear attack or blackmail.[15] Trident is designed to be a stealthy, invulnerable system, almost impossible for an enemy power to eliminate before an attack, and would consequently be able to retaliate in the event of any nuclear strike against the UK.

The Royal Navy's four Vanguard Class nuclear-powered submarines carry Britain's Trident nuclear deterrent.

Under the practice of Continuous At-Sea Deterrence (CASD) at least one submarine is always on patrol. Another submarine is usually undergoing maintenance and the remaining two are in port or on training exercises. Four submarines enable some latitude for unforeseen events. The submarine patrols at depth within a series of planned topographical "boxes" measuring several thousand square miles, but the exact location and route is known to only three or four people on board the vessel. The submarine will only make contact with naval command in an extreme emergency, as communication from the submarine could give away its location. Intelligence is usually relayed to the vessel by low frequency and very low frequency radio, and more occasionally by higher frequency bands using satellites, giving known details of shipping movements and potentially hostile aircraft or submarines in the area.[17]

Only the Prime Minister can authorise the launch of Trident ballistic missiles. These orders would likely be issued from the PINDAR command bunker under MoD Main Building in Whitehall, central London, with strict protocols in place to confirm her identity, though she can issue these orders from elsewhere. This order would be conveyed directly in person over secure link to the CTF 345 operations room in Northwood, the only facility with direct communications between the Prime Minister and the Vanguard commander on patrol. Two officers on board the submarine are required to authenticate each stage of the process, using the codes that are stored inside two safes opened with keys held by the ship's executive and weapons engineering officers. The submarine commander is responsible for the activation of the firing trigger.[18]

If the commander has a reason to believe that the government has ceased to function and has been destroyed, the letter of the last resort would be retrieved from a safe bolted to the control room deck and its instructions followed.[19] The letters of last resort are four identical handwritten letters from the serving Prime Minister to the commanding officers of each Vanguard-class submarine, orders on what action to take in the event that an enemy nuclear strike has destroyed the British government.

15. Peter Cannon, 'The Necessity of Nuclear Deterrence', *The Henry Jackson Society,* (18 June 2012), http://bit.ly/2qv7cZo
16. http://bit.ly/1Q50BtP
17. UK Ministry of Defence, 'Strategic Defence and Security Review published', Ministry of Defence, (19 October 2010), http://bit.ly/2ridwVm
18. International Court of Justice, 'Legality of the Threat or Use of Nuclear Weapons', (1996), International Court of Justice, http://bit.ly/1hW3TeQ
19. The process by which a Trident submarine commander would determine whether the British government is functioning includes, among other checks, establishing whether BBC Radio 4 continues broadcasting. This was first described in Peter Hennessy, *The Secret State: Whitehall and the Cold War*, (Allen Lane, 2003).

UK Vanguard submarines specifications

Length: 492 ft

Displacement: 15,900 tonnes

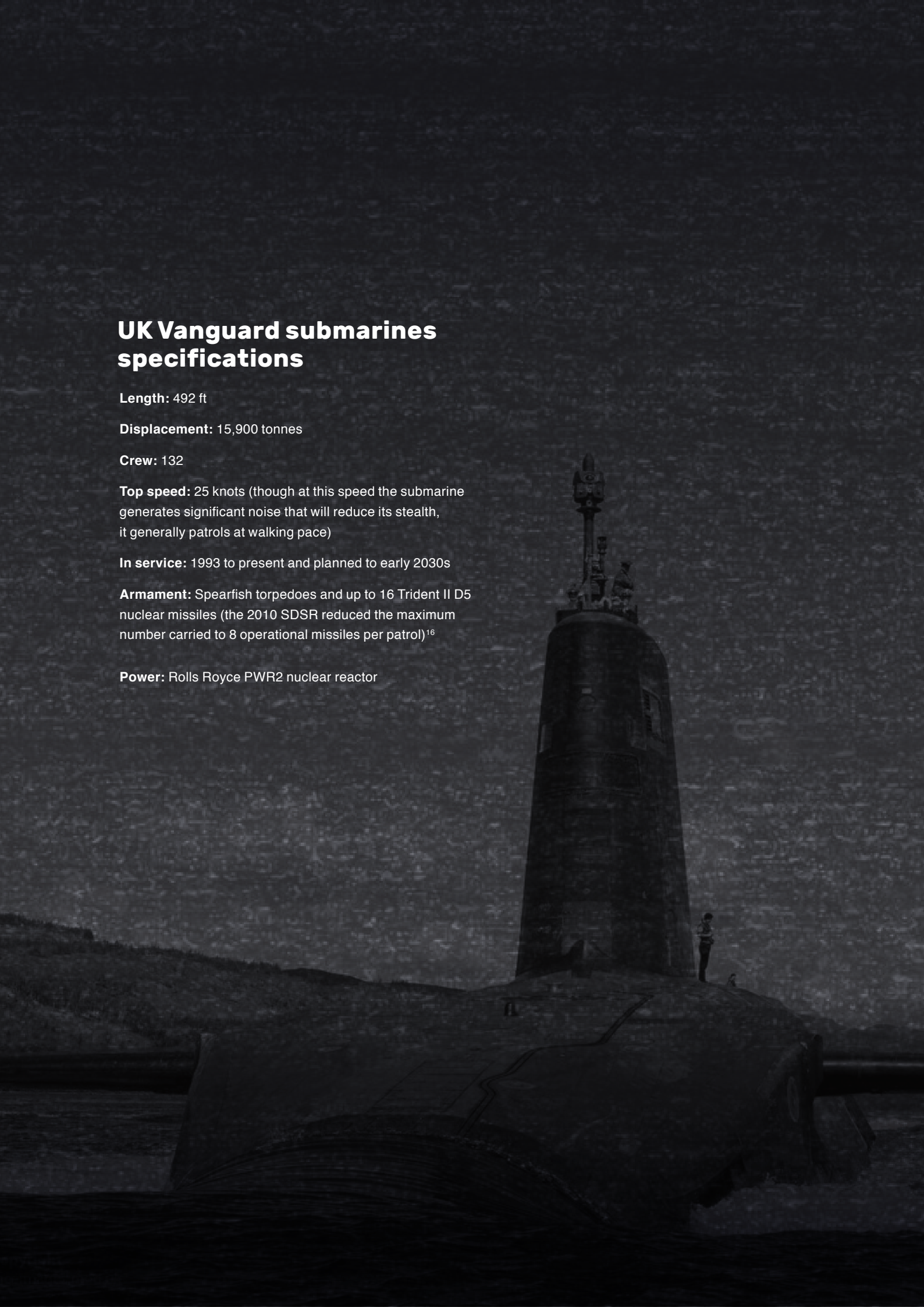
Crew: 132

Top speed: 25 knots (though at this speed the submarine generates significant noise that will reduce its stealth, it generally patrols at walking pace)

In service: 1993 to present and planned to early 2030s

Armament: Spearfish torpedoes and up to 16 Trident II D5 nuclear missiles (the 2010 SDSR reduced the maximum number carried to 8 operational missiles per patrol)[16]

Power: Rolls Royce PWR2 nuclear reactor



4. Attack Vectors on Trident

The nuclear ballistic missile submarine is perhaps the most sophisticated naval vessel ever built, with a great deal of interdependence between systems. Whilst there are many protections and back-up systems, sub-system malfunction and failure can conceivably trigger the collapse of the submarine's operation and neutralise its primary purpose.

Cyber-attacks may be mounted in concert with more conventional sabotage or military attack. A particularly effective attack could enable enemy access to the submarine's command network. Remote communication and passive reconnaissance (using long range antennas to monitor wireless transmissions) could enable attackers to capture encrypted information or to distort it without an initial breach into the system. Cyber-attacks are difficult to control and many of their effects likely unanticipated. They may have an intended effect on a particular sub-system but then have broader unintentional impacts on the wider system.

4.1 Air gapping

A secure computer network is said to be air gapped when it is physically isolated from other insecure networks, particularly the public Internet or any insecure local area network. Networks that employ dedicated cryptographic devices that tunnel packets over untrusted networks while avoiding packet rate or size variation are also considered air gapped, as there is no ability for computers on opposite sides of the gap to communicate. Submarines on patrol are clearly air gapped, not being connected to the internet or other networks, except when receiving (very simple) data from outside. As a consequence, it has sometimes been claimed by officials that Trident is safe from hacking. But this is patently false, and complacent.

Protocol may ban the introduction of storage devices during operation, and include a ban on wireless connections or similar restrictions on electromagnetic leakage from the secure network through the use of a Faraday cage or some other form of EmSec (security measures to prevent electromagnetic radiation leaking data).

A number of recent events (such as *Stuxnet*, *Duqu* and *BlackEnergy3*) prove that air gapping and network segmentation cannot be considered an effective defence against all cyber-attacks. Every electronic system inevitably has a means for new code to be introduced, be it by USB memory stick or some more sophisticated method, particularly at more vulnerable times.

Efforts to develop methods to penetrate an air-gapped network have been the focus of much research over many years. The viability of acoustic signalling in defeating air gap isolation was demonstrated in 2013.[20] In 2014, researchers introduced *AirHopper*, a bifurcated attack pattern showing the feasibility of using a mobile phone to achieve data exfiltration from an isolated computer, using FM frequency signals.[21] In 2015, *BitWhisper*, a covert signalling channel between air-gapped computers using thermal manipulations achieved Proof of Concept. *BitWhisper* supports bidirectional communication and requires no additional dedicated peripheral hardware. Later in 2015, researchers introduced *GSMem*, a method for exfiltrating data from air-gapped computers over cellular frequencies.

The transmission, generated by a standard internal bus, enables the computer to operate as a small cellular transmitter antenna.

ProjectSauron malware, discovered in 2016, demonstrates how an infected USB device can be used to remotely leak data off from an air-gapped computer. The malware remained undetected for five years and relied on hidden partitions on the USB drive not visible to Windows as a transport channel between the air-gapped computer and a computer connected to the internet, presumably as a way to share files between the two systems.[22]

Sophisticated malware can clearly exploit various hardware combinations to broadcast sensitive information from air-gapped systems. These hardware combinations use a number of different mediums to bridge the air-gap, including: acoustic, light, seismic, magnetic, thermal and radio-frequency.

4.2 Potential attack vectors on the whole system

An attack vector is a path or means by which a malicious actor can gain access to a computer or network server in order to deliver a payload or a malicious outcome. Attack vectors enable attackers to exploit system vulnerabilities, including hardware, software and the human element.

It is often said that the weakest link in any complex system are the human beings responsible for managing it, and they are often targeted by cyber-attackers. It is estimated that 80% of global cyber-attacks originate from social engineering and spearphishing. The famous hacker Kevin Mitnick describes himself more as a social engineer focused on exploiting human weaknesses. It does not matter how strict the systems are; unless everyone involved is on continuous high alert, they are highly vulnerable to manipulation or misdirection.

When in May 2015 Able Seaman William McNeally outlined his numerous security concerns about the operation of Vanguard submarines, his principal focus was on the poor levels of security on shore at the Faslane base and on board during patrol, and the general inability of personnel to keep to protocol and commanders to enforce protocols effectively.[23] His account of security lapses is sobering to anyone sceptical about the possibility of the delivery of a cyber weapon into the Trident system. He attested, 'it's harder to get into most nightclubs than it is to get into the ['highly secure'] Green Area' at Faslane. He also claimed that as a junior crewman, he and many others frequently went onto base and into the submarine without their bags being checked.[24]

The recreational computer network on board is one of the more vulnerable systems that could be used as a cyber entry point. Malware can be introduced and even written on board the vessel using one of the personal computers, and then the malicious code could be introduced into the control systems network using available data transfer capacities (USB drives, SD cards, etc.).

4.3 Supply chain and construction

The procurement and operation of the submarines involves several stages: research and development, manufacturing, assembly, sea-trialling, weaponization, deployment and maintenance. Security flaws can be introduced deliberately or inadvertently at the manufacturing, assembly and maintenance stages, to be potentially exploited in the future. Otherwise, malware may be uploaded into a component or a network of components, for it to lie dormant ready to activate at a predefined moment or under specific circumstances.

Cyber espionage may be used prior to or during construction to acquire highly classified design information or operational secrets, enabling competitors to develop their capabilities to track the Trident submarines.[25] Bear in mind that the design and operation of the reactor is treated as a higher classification than the warhead design itself, because of implications for submarine stealth and efficiency.

Such intrusions might also be used to enumerate and identify systems as a precursor for future attack and possible sabotage. The hacker group thought to be behind the release of the WannaCry worm in May

2017, the Shadow Brokers, claimed on 16 May to have data relevant to nuclear and missile programmes in several countries that they could release publicly in the coming months.[26] Defence laboratories and contractors in the United States involved with manufacturing and maintaining the Trident missile, its software and its fire control systems (upon which the UK relies) have been targeted by hackers looking for sensitive nuclear-related intelligence in the past.[27] We can assume the Atomic Weapons Establishment in Berkshire, where the UK nuclear warheads are designed and maintained, is also a highly desirable target, as well as the primary submarine contractors in the UK, BAE Systems, Rolls Royce and Babcock, and companies within their supply chains.

Protection against intrusion at every level of the supply chain is a monumental task, one it is hard to believe the industry is up to. Security can never be guaranteed even in the most secure facilities of a prime contractor, but those facilities for secondary contractors are unlikely to be any match for a concerted and resourced group of attackers, particularly with the resources of state intelligence services behind them.

4.4 Patrolling

Among all potential intentional attack threats to a patrolling submarine in communications receive mode only, there are three major vectors: malware injected before the patrol, insider threat (infiltration) and external radio transmission to the submarine. Until new technologies emerge, the vessel is less vulnerable to real-time external electronic and communication attack when submerged (VLF radio simply does not have the bandwidth to receive malware), though it is more vulnerable to attacks from inside the submarine. If compromised while underwater, systems failure might lead to critical malfunction, decompression and loss of the vessel and strategic payload.

One possible attack vector may include spoofing or false orders from hacked radio transmission facilities. Though rare and requiring special equipment and conditions, radio frequency attacks on communication devices can be conducted during any stage of the submarine operation, including on patrol.[28] It is generally easier to spoof communications from satellites.

4.5 Maintenance

Maintenance involves replacement, remodelling, reconfiguration, update and upgrade of systems. During this process systems interact with external networks and devices. Malicious software could be uploaded deliberately or unwittingly onto the vessel subsystems using storage devices, giving access to design or operational intelligence. It could also potentially sabotage or damage the missiles, missile control or any other onboard system. This does not necessarily require the presence of a malign human actor anywhere near the submarine, missile or warhead facilities, or in the facilities of any contractor. Maintenance, like the construction stage, has a less secure supply chain that is vulnerable to external or internal attack.

20. John Leyden, 'Hear that? It's the Sound of BadBIOS Wannabe Chatting Over Air Gaps', *The Register*, http://bit.ly/2quYGKa
21. Guri, Mordechai; Monitz, Matan; Mirski, Yisroel; Elovici, Yuval, 'BitWhisper: Covert Signaling Channel Between Air-Gapped Computers Using Thermal Manipulations', IEEE 28th Computer Security Foundations Symposium, (April 2015), http://bit.ly/2pZWGpM
22. BBC, ''Project Sauron' malware hidden for five years', (9 August 2016), http://bbc.in/2aWpx9K
23. William McNealy, 'The Secret Nuclear Threat', (May 2015), text available on Nuclear Information Service website, http://bit.ly/2qVpYKW
24. Symantec Corporation, 'Internet Security Threat Report 2014', Volume 19, (April 2014), http://symc.ly/1kmEX7O
25. Andrew Futter, 'Is Trident safe from cyber attack?', Article prepared exclusively for the European Leadership Network, (February 2016), http://bit.ly/1LxfDKf
26. See blog, *'OH LORDY! Comey Wanna Cry Edition'*, available in: http://bit.ly/2qmLzLa
27. Lockheed Martin, 'Lockheed Martin-Built Trident II D5 Missile Achieves 130th Consecutive Successful Test Flight', *PR Newswire*, (28 December 2009), http://prn.to/2qwGwry
28. Kim Zetter, 'How Attackers Can Use Radio Signals and Mobile Phones to Steal Protected Data', *Wired*, (11 March 2014), http://bit.ly/2qvlOrX

5. Vanguard's Electronic Vulnerabilities

All critical systems in a vessel are automated and controlled by its computer systems. As military infrastructure is heavily guarded and segmented, one of the most effective means to attack these systems would be the use of malware.

Table 1 outlines two main network structures vulnerable to malware injection: those on board the submarine and those within the command and control facility on land.

Activity	Critical system	Examples of possible consequences
Malware injected into one of the systems on board the vessel	Communications (remote)	• Engaging emergency protocols; • interception and misdirection of communications from HQ, spoofing or loss of communications.
	Communications (internal), and any computer in the facility	• Loss of coordinated operation; • increased vulnerability of the vessel; • decreased mobility and response capacity of the vessel; • malware propagation across the facility network from the most vulnerable system to the most critical, with potentially multiple effects.
	Navigation	• Decreased mobility; • confusion around location; • the vessel might be forced to surface to periscope depth.
	Life support	• Threat to human life and operation of the vessel.
	Reactor	• Loss of control; • overheating and core meltdown; • irradiation, area contamination; • at extreme, vessel destruction.
	Control of missile and warhead operations	• Confusion over communications between missile and control; • missile abort or misdirection; • premature explosion of warheads.
Malware injected into a system in the C&C facility	Interception of communication system	• Interruption of communications, preventing smooth C&C.
	Distortion or substitution of communication system, leading to false orders and information	• False orders could include: • notice to fire; • taking submarine off alert; • ordering the vessel to prematurely return to port.
	Human-Machine Interface (false reading on the system about the submarine status and location)	• False sense of security; • false alarms; • false orders.

5.1 Communications to and from the submarine

Possible attacks against digital communication systems include:

- Interception – unauthorised capture of transmitted data, encrypted or not;
- Spoofing – impersonation of the transmitted data, faking its origin and context;
- Bit flipping – compromising the integrity of the transmitted data by damaging the transmitted encrypted data, causing scrambled date or false interpretation;
- Jamming – blocking the data transmission in a particular area or over a certain channel.

The chance of miscalculation, misperception or unauthorised use due to "spoofing attacks" and electronic impersonation remains a possibility, and there are protocols in place when on patrol to guard against these possibilities. Of course, these depend upon crew members sticking to protocol, and in any case, are not guarantees for success. It is also conceivable that cyber-attackers could target UK radio communications, just as they have in the past US submarine radio transmissions.[29] This would present particularly acute challenges during the time of crisis and time-pressure, when the need for quick and clear coordination and communication is paramount. Details of the communication systems in Vanguard-class submarines are of course classified, but the technology they rely on is not. Modern radio frequency attacks can target not only data in transit, but also the transmitters and receivers, and their internal software.

External communication to the submarine transmits data (such as targeting and battlespace information, and brief messages from families to the crew) over very low frequency (VLF) and low frequency (LF) radio without using satellites, picked up by a long antenna trailing in the water behind the submarine.[30] Data is transmitted using an internet protocol (IP) system, and uses a US-UK common military grade encryption system at both ends of the communication. Extremely low frequency (ELF) systems have been in use in the past, enabling communication whilst the submarine is at maximum depth, but require huge transmitters, a great deal of energy, and can only transmit very low bandwidth. They have largely been abandoned.

VLF can penetrate to a depth of around 20 meters below the surface and can transmit at roughly 300 bit/s, translating to around 450 words a minute. Submarines can sometimes use a submerged buoy at this depth with an antenna, so that the vessel can remain at greater depth. VLF can be affected by salinity gradients in the ocean and natural sources of VLF radiation, but the quality of data transmission is not strongly influenced by environmental conditions and is therefore useful for reliable global communications. The US Navy's VLF systems serve as a back-up for global communication use during hostilities when nuclear explosions may disrupt higher frequencies or satellites and other transmitting equipment may be destroyed by enemy actions.

The transmission antennas need to be large, to the point that they can cover a site of several square kilometres, so this is a one-way communication from shore-based command centres to surface ships and submarines. Its range can be extended by broadcasting to several satellites at once. The British use a VLF transmitter at Skelton near Penrith, but other NATO and US transmitters can also be used to communicate with British submarines.[31]

A review on Very Low Frequency (VLF) submarine communication methods by the Pentagon in the mid-1990s unearthed a firewall vulnerability that could have enabled hackers to gain control of naval radio communications "for broadcasting nuclear launch orders to Trident submarines".[32] The investigation showed that cyber terrorists could potentially infiltrate this network and insert false orders for launch, or to neutralise such orders, sidestepping the chain of command. The investigation led to "elaborate new instructions for validating launch orders" from two independent instructions to fire, which will have been replicated by UK protocols.[33] Whilst this will have made spoofing and other attacks more challenging, they remain a possibility.

Submarines can also receive data from satellites at higher frequency when on or near the surface (with an antenna raised). This uses UHF, SHF and more recently EHF radio communication for faster bursts of data transmission, as well as for communications from the submarine to itself.[34] This form of communication does leave the submarine vulnerable to detection, and satellite communications to conventional cyber-attacks, as they use encrypted but generic network protocols for data transmission and security (including TCP/IP, NetBIOS and RDP).[35]

5.2 Internal submarine networks

Network connectivity inside the submarine uses internal wired radio and computerized systems which transmit data from sensors to the monitoring stations to inform decisions and control the submarine. Effective command and control requires correct and timely tactical data delivery, and is fully dependent on this network infrastructure.

In common with many military systems, the electronic systems involved in SSBNs are based on legacy technology onboard (both hardware and software), that is bespoke and highly classified. This has ambiguous implications for security. The search for vulnerabilities requires a great deal of reverse engineering and study. Yet the operating systems, software and hardware for the Trident submarines are designed with weak legacy architecture, with only a limited number of engineers involved in their development and security. Whilst the code is often old and may be unfamiliar to today's hackers, and many cyber hacking tools will be inappropriate to it, there are more likely to be many potential vulnerabilities lurking within as fewer people will have been involved in creating and testing it. Those vulnerabilities will have been around for a long while, and active external support often suspended enabling potential hackers to develop back-doors, trojan horses and other tools to compromise the code. As the victims of the *WannaCry* worm over the weekend of 12-15 May 2017 discovered, older operating systems that may not have universal support from the suppliers can be more exposed.

There are multiple isolated local area networks inside the submarine. The networks controlling the submarine are separated from that of weapons systems, as well as from the recreational network. However, emerging developments deliver the ability to bypass the physical isolation of networks. The notorious cyber-attack on the Natanz Nuclear facilities, labelled *Stuxnet* (Iran, 2010), is an illustration of airgap-jumping malware, that can propagate via USB storage devices carried by unsuspecting and authorised users. In this case, it is believed that malware was written in the United States and Israel, delivered by USB by contractors and subcontractors within Iran responsible for maintenance.[36] The virulence of the code was such that it rapidly spread to computers worldwide, but it is believed only had physical impact upon the specific target: Siemens controllers connected to the Iranian centrifuges.

Backdoor, a malicious process that facilitates access or code execution by an attacker without proper authentication, may be introduced during the development of the software by intention (including the scenario when the attackers infiltrate the network of a defence contractor or sub-contractor further up the supply chain) or by accident, when the backdoor may be introduced during the debugging process implemented by the developers and not removed.

The Submarine Command System (SMCS) was first created for the Vanguard-class submarines as their tactical information and torpedo weapon control systems.[37] It has a long and complex pedigree. Its updated versions are based upon a version of Windows XP and known colloquially as 'Windows for Warships'. These have now been installed on all active Royal Navy submarine classes.

Both Windows-based and Linux-based operating systems hold the legacy of vulnerabilities from the original systems, even though they operate on obscure and classified equipment and run bespoke programmes.

Prior to the Vanguard class, Royal Navy ships and submarines had command systems built by Ferranti using custom-built electronics and specialised proprietary processors. Soon after the decision in 1983 to proceed with the Vanguard programme, an

open competition for the command system was won by Gresham-CAP, who proposed an innovative distributed processing system based on commercial off-the-shelf processors, and with a modular software architecture largely written in the Ada programming language.

Each set of the Initial Phase SMCS equipment had multiple computer nodes. At the centre of the system there is an Input/Output Node (providing interfaces to weapons systems and sensors) and a Central Services Node (conducting fast numeric processing). Each central node is duplicated ("mirrored") to create a fault-tolerant system which is dual modular redundant. The human-computer interface is provided by multi-function consoles and some additional terminals. The dual redundant central nodes are linked to each other and to the consoles via a dual-redundant fibre optic network connection. Most processing was done by Intel 80386 single-board computers, each with its own Ada run-time environment. CAP Scientific (later part of Sema Group) created a complex layer of middleware to link the many processors together. SMCS was the largest Ada project to date. As a result, the SMCS project encountered many challenges with the large-scale use of Ada compilers, Ada development tools and the special characteristics of the Ada 83 programming language.

By 1991, the SMCS project was owned by BAeSEMA, a joint venture between Sema Group and British Aerospace. The decision was taken to migrate SMCS to the Solaris operating system on UNIX, running on SPARC (single-board) computers. To limit risk, only the control consoles were converted to Solaris; the central nodes were kept in the same form as the Initial Phase equipment. This threw up particular problems arising from a mixed architecture of Intel and SPARC, such as endianism.[38]

By 2000 the SMCS project was fully owned by BAE Systems. In its 2003 Defence White Paper, the government agreed numerous improvements for Royal Navy submarines, but no changes to the Vanguard-class submarines or to the Trident missile system.[39] It was assumed that the SMCS equipment, maintained under a support contract with Ultra Electronics, would outlast the service life of the Vanguard fleet into the 2020s. The programmes in place for other submarine improvements were mainly for new sonar equipment.[40]

In 2002, it was proposed to convert SMCS to run on standard x86 hardware redesigned specifically for naval command systems. The plan was to convert the SMCS infrastructure and applications to run on the Microsoft Windows operating system and known as SMCS-NG ("Next Generation"), or "Windows for Warships".[41] This is based upon a variant of Windows 2000 and Windows XP. SMCS-NG was retrofitted into all Royal Navy submarines by December 2008. The software is supplied as a universal release configured for the sensor and weapon fit of each submarine.

Windows has an entangled monolithic structure, as opposed to a modular architecture.[42] It is therefore impossible to change the proprietary operating system by means of reconfigurations and third-party modules. This structure of the consumer-friendly operating system exposes potentially vulnerable services and features that might not be required for the adequate functioning of the submarine.

Defence Minister Adam Ingram later gave assurances to parliament in 2004 that this was a low risk use of Microsoft Windows, on the basis that it was more likely to have long-term product support.[43] There was no mention of its security features, and it is worth noting that Microsoft has ceased general product support for both Windows 2000 and Windows XP, one of the reasons why the *WannaCry* worm spread to so many personal computers and commercial and public networks in May 2017. MoD negotiated an ongoing bespoke Custom Support Agreement with Microsoft when general support ended, but it remains unclear how this arrangement is in patching the systems.

However, other suppliers have taken a different path. The consoles for the new Sonar 2076 supplied by Thales Underwater Systems for the Astute class submarines, and which may be retrofitted to other classes, are built with the Linux-based operating system rather than Windows.

5.3 Navigation

Electro-magnetic radiation (light, infra-red, radio waves, wifi, etc.) does not generally penetrate far into water unless it is particularly long wavelength (extremely low frequency) radio, and submarines therefore cannot always rely upon it for accurate navigation, avoiding obstacles and to detect threats. When on the surface, a global positioning system (GPS) can accurately determine latitude and longitude, but this system cannot work when the submarine is submerged below periscope depth. Underwater, the submarine uses inertial guidance systems (electric and mechanical) that keep track of the ship's motion from a fixed starting point using gyroscopes. The inertial guidance systems are accurate to 150 hours of operation and must be regularly realigned by other navigational systems (GPS, radio, radar, celestial or sea bed navigation, as listed below). With these systems onboard, the crew can accurately navigate to within several tens of metres of the intended course.

To locate a designated target, a submarine can use active and passive sound navigation and ranging system (SONAR). Passive sonar involves listening to sounds generated by the target. Active sonar emits pulses of sound waves that travel through the water, reflect off the target and return to the ship. By knowing the speed of sound in water and the time for the sound wave to travel to the target and back, the instruments can quickly calculate direction and distance between the submarine and the target. Active sonar risks giving away the presence of the submarine to other vessels listening in, though its direction of emission can be controlled, particularly when navigating (directed at the sea bed), limiting the spread of the sound wave and the chances of being picked up. Sonar systems can also be used to realign inertial navigation systems by identifying known ocean floor features, and make more precise real-time location calculations.

On the surface or at periscope depth, submarines can use these methods to fix their position:[44]

- Satellite navigation: global positioning system (GPS).
- Terrestrial radio-based navigation systems.
- Radar navigation, normally used in friendly waters while entering and exiting ports. Radar can be directed to reduce the chances of detection by third-party sensors.
- Active sonar (similar to radar, active sonar systems are easily detected).
- Pilotage — conventional system of navigational aids in coastal and internal waters, (buoys, navigational markers, lighthouses, etc.), utilizing the periscopes when near the surface to obtain lines of position to plot a course.
- Voyage Management System: utilizes digital charts and data streaming from sensors and navigational devices to establish the vessel's position. Other information may also be entered in manually to improve the quality fix or position.

At depths below the periscope depth submarines determine their position using:[45]

- Dead reckoning from the ship's gyrocompass, estimating speed and local ocean currents.
- Inertial navigation system is an estimated position source based upon acceleration and deceleration, pitch and roll as data sources.
- Bottom contour navigation may be used in areas where detailed bathymetry data has been charted and there is adequate variation in sea floor topography. This may use directed sonar or an electronic gravimeter that accurately measures the minute variations in gravity caused by changes in the sea bed.

To calculate precise readings, submarine systems need to be synchronised. Should the malware be introduced during development or maintenance of the navigation components, it could disrupt internal synchronisation data (such as time and date, bathymetry data, calculations or sequence numbers). Ultimately this could confuse navigation, divert the submarine from its original course or cause collisions.

5.4 Life support

Life support systems include air filtering, water purification (the distillation system), temperature regulation and sanitization systems on board the vessel. They are critical for personnel survival and sustaining health over the longer term. Compromise and damage to those systems could have severe impact upon the crew and its operation of the submarine.

5.5 Reactors and power supply

Nuclear submarines use propulsion systems that include a nuclear reactor, steam turbines and reduction gearing to drive the main propeller shaft.[46] These systems also provide the electric power to operate the equipment on board and to power up the storage batteries. These systems are managed and monitored by sophisticated electronics and software, including programmable logic controllers (PLC) and computers, interconnected as a single logical network.

Attacks on the nuclear power plant have the potential to be the most dangerous of all on an SSBN. Malware can propagate over the network of interconnected PLCs, corrupt data from sensors and can even deny access to infected systems. Damage to any of these systems could have devastating consequences.

- An attack could result in changes to power generation, or even reactor overheating.
- If the entire power battery unit is disabled, the vessel's systems will rely directly and exclusively upon the reactor.
- An attack on the propulsion systems could lead to a variation in the power output, or could interfere with the navigation of the vessel.

5.6 Command and control of missiles and warheads

The United States and UK draw their Trident II D5 missiles from a common pool at Kings Bay, Georgia. These missiles and their electronic components are built and maintained in the United States by contractors working with a complex web of subcontractors, any one of which may be the victim of human intelligence and penetration. The security and maintenance of the missile pool and its associated systems is therefore under the sole control of the United States. The UK Trident warheads are maintained, refurbished and stored by the UK Atomic Weapons Establishment at Aldermaston and Burghfield in Berkshire. They are transported over land by road to Royal Naval Armaments Depot Coulport where they are stored and loaded onto the Trident submarines prior to patrolling. The missiles and warheads are vulnerable to cyber interference at each stage of this process.

The US Navy installed Permissive Action Link (PAL) devices on all its ballistic missile submarines near the end of the Cold War to prevent unauthorised launch. Missile launch requires a code sent by the Chiefs of Staff on behalf of the US President. The US posture involves preparation for a nuclear exchange in which the President or his deputies remain in charge and in communication with launching crews at the moment of release. In contrast, the UK Ministry of Defence chose not to install PALs on Vanguard-class submarines because the system is designed to threaten a devastating second strike response in the event that the capital and government has been eliminated. This is the purpose of the letter of last resort, the idea being that an adversary would not seek to destroy the UK and its government in the first place, knowing that the capacity to respond in retaliation exists after destruction.

It is important to point out that the electronic missile control systems are entirely separate from those running the submarine. The mechanical trigger that launches the Trident missile is modelled on a Colt 45

Peacemaker pistol. This mechanical component ensures the standard launch procedure itself is secure from cyber spoofing. However, there is scope for spoofing on the communication and chain of command side of the firing chain, and also on the other side of the launch, between the trigger and the missile. If the control software of the missile or the warheads is compromised there could be an unauthorised launch, premature detonation inside the launch bay or during missile flight, corruption of the flight control data, unauthorised retargeting or simply interruption of launch.

Missiles are deeply complex and involve a large number of electronic components, including guidance systems, firing and rocket control systems and the electronics involved in the re-entry vehicles and warheads themselves. With missiles, even more so than for submarines, if any one of these components malfunctions it could cause a catastrophic failure. Rocket science is highly complicated. All missile development programmes have involved significant failures in their early years. When a missile fails, there are any number of explanations.

The speculation, first broken by David Sanger and William Broad in the New York Times in March 2017, that a US cyber hacking programme could have been behind the recent spate of failures in the North Korean missile tests, has been controversial.[47] Several analysts have disputed the claims on the basis that the failure rate with the new missiles is consistent with the record in other missile programmes, and the challenges the United States has experienced in penetrating the North Korean programme.[48] However, this story highlights the exposure of all states' missile development programmes to foreign cyber interference.

When HMS Vengeance in June 2016 completed its shakedown exercise off the coast of Florida after mid-life refurbishment, it fired a D5 missile recently picked up from the common pool in Kings Bay. Just a few weeks after the shakedown the UK Parliament voted in favour of renewing the system. But it was only in January 2017 that the incident was made public by the Sunday Times.[49] It was reported that the telemetry data from the missile contained anomalies and the missile had to be destroyed.

Those familiar with the systems following the developments speculated that the most likely cause was a failure in the guidance systems that are being replaced as part of the Life Extension Programme of the missiles. [50] But the failure could have several explanations, including the aging of the guidance components or failures in the new, under-tested components. It was also consistent with the injection of malware into the failing component or into the system transmitting telemetry data from the missile. In other words, if there had been a hack, this is possibly what it would have looked like. There is no strong evidence that has been presented either for or against such a conclusion.

5.7 Advanced persistent threat

An advanced persistent threat (APT) is a set of stealthy and long term continuous cyber-attacks. These would need to be performed by an organized and well-funded group of high level cyber experts, if they are to affect Trident's operations. APTs, being costly and requiring a high degree of secrecy over a protracted time period, usually target critical private or public entities for big business, political or military motives. "Advanced" signifies sophisticated techniques using malware to exploit vulnerabilities in systems. "Persistent" signifies continuous monitoring of the external command and control system and extracting data from a specific target. "Threat" indicates human involvement with particular intent.

Recognised APT attack vectors include infected media, supply chain compromise and social engineering (exploiting group psychology weaknesses), to place custom malicious code on one or multiple computers for specific tasks and to remain undetected for the longest possible period while collecting data and readying for a future attack.

In a typical civilian scenario, attackers seek to obtain unauthorised access to confidential data, cause denial of service, collect valuable information, banking credentials databases, in some cases even to cause physical damage to systems and facilities. Unauthorised access to systems can be also obtained by exploiting bugs, errors, invalid inputs, misconfiguration, default settings, etc. Using

sophisticated APT techniques, intelligent intruders may remain undetected within an organisation's systems for months, concealing their presence with the noise of a busy network. Insiders are particularly difficult to spot because many of their operations may be legitimate, while a small but significant part of their activity is harmful.

Attribution is a sophisticated challenge, particularly as attackers often confuse by using another country's language or deliberately mashing up their English.[51] Images, text files with specific quotes, IP addresses or hardware brands could all be calculated to mislead investigators and plant the blame elsewhere. Successful false flag operations could trigger conflict or war directed at states uninvolved in the original cyber intrusion.

APT threats to the UK Trident command and firing chain could override security protocols, potentially transferring some control of communications in a crisis to the attacking state without the prior knowledge of Royal Navy command. One of the more sophisticated scenarios would be to create a series of false readings on the Human-Machine Interface and jamming of communications, leaving the commanding officer of the vessel blind.

29. Jason Fritz, 'Hacking Nuclear Command and Control', International Commission on Nuclear Non-proliferation and Disarmament, (2009)
30. VLF is defined as 30 - 300Hz, a wavelength of 1000 to 10,000 km. LF as 300 - 3000Hz, a wavelength of 100 to 1000 km.
31. John Ainslie, *The Future of the British Bomb*, WMD Awareness Programme, (October 2005), p. 85
32. Scott Peterson, 'Old weapons, New terror worries', *The Christian Science Monitor*, (15 April 2004), http://bit.ly/2pOR729
33. Bruce Blair, 'Rouge States: Nuclear Red-Herrings', *The Defense Monitor*, Vol. 33, No. 1, (January-February 2004); Bruce Blair, 'Why Our Nuclear Weapons Can Be Hacked', *The New York Times*, (14 March 2017), http://nyti.ms/2ruWTD2; Rosetta in the UK, 'The Open University Joins Forces with BAE Systems to Harness Rosetta Know-how for UK's Newest Submarines', http://bit.ly/2pOXt1e
34. Ultra High Frequency (UHF) is between 300 MHz and 3 GHz; Super High Frequency (SHF) between 3GHz to 30 GHz; and Extremely High Frequency (EHL) is 30GHz to 300GHz
35. Zhuo Jiang, Qian W, Hewu Li, 'NTCP: Network Assisted TCP for Long Delay Satellite Networks', 2016 IEEE/CIC International Conference on Communications in China, (27-29 July 2016), http://bit.ly/2rv15SN
36. Nate Anderson, 'Confirmed: US and Israel created Stuxnet, lost control of it', *Law and Disorder*, (1 June 2012), http://bit.ly/2n7OGWE
37. BAE Systems, 'Submarine Command System Next Generation', http://bit.ly/2pXfvdR
38. Intel architecture is little-endian and SPARC is big-endian. Endianism refers to the conflicting methods by which hexadecimal memory is stored in the memory as bytes.
39. House of Commons Defence Committee: Written Evidence, Session 2002-03, http://bit.ly/2q06Cj1
40. Ministry of Defence, T*he Royal Navy Handbook*, Conway Maritime Press, (2003)
41. Lewis Page, 'Royal Navy Completes Windows for Submarines Rollout', *The Register*, (16 December 2008), http://bit.ly/2rd0gyo
42. Bill Gates, as Microsoft's Chief Software Architect, had given sworn testimony under oath to the US Courts on this point. Civil Action No. 98-1233 (CKK), Direct Testimony of Bill Gates, Defendant's Exhibit 1507, (22 April 2002), paragraphs 207 to 223.
43. Adam Ingram MP, in an answer to Mike Hancock MP, Written questions, House of Commons, 200036, 428 c165W, (01 December 2004)
44. 'Navigation and Operations', University of Kansas, Naval Reserve Officer Training Corps (2006)
45. S. E., Hamn, 'Coastal Piloting: Bottom Contour Navigation (Seamanship)', T*railer Boats*, (1995); see also *Undersea Warfare*- journal, No. 51 (June 2013)
46. Rolls-Royce, 'Submarines Capability', http://bit.ly/2q07WSS
47. David E. Sanger and William J. Broad, 'Trump Inherits a Secret Cyberwar Against North Korean Missiles', *New York Times*, (4 March 2017), http://nyti.ms/2lJUOQA
48. Jeffrey Lewis, 'Is the United States Really Blowing Up North Korea's Missiles?', *Foreign Policy*, (19 April 2017), http://atfp.co/2ooa4E9
49. Sunday Times, 'No. 10 Covered up Trident Missile Fiasco', *Sunday Times*, (22 January 2017), http://bit.ly/2rv8LUW; see also Ewen MacAskill, 'How did the Trident test fail and what did Theresa May know?', *The Guardian*, (23 January 2017), http://bit.ly/2jhLVyW
50. Sunday Times, 'Revealed: Trident's faulty guidance', *Sunday Times*, (29 January 2017), http://bit.ly/2qvFr33
51. See a blog from someone claiming to be from the Shadow Brokers, *'OH LORDY! Comey Wanna Cry Edition'*, available in http://bit.ly/2qmLzLa

FICTIONAL SCENARIO 3:

Disrupting UK SSBN operations directly

Memo Dated: 6 January 2017

From: [Foreign] Naval Intelligence, Unit 6B

Mission: To compromise the operation of the submarine, gather intelligence data, divert the submarine from its original course or disable its ability to fire

Objective: Infiltrate the submarine, and establish the means to interrupt operation

Method 1: Introducing malware into the submarine's systems, its controlling computer network and the systems controlling missile firing. One of the options we have is to create a "Backdoor" that could be activated via a communication link (or under predefined circumstances) and transmitting a radio signal through covert channels (e.g. injecting hidden bits of data into the standard radio messages in both directions). For this to function we will require a receiver ("listener" - a malware in the communication facility on land) to relay data to Naval Intelligence in Transnistria. We should also aim for the capability to transmit commands to the submarine through covert channels to provide the capability to control our malware remotely, alongside packet data [the original communications] transmitted to the submarine by the Royal Navy. This method will require hardware to be added, or for our agents to modify hardware destined for incorporation into the submarine during maintenance or overhaul.

Naval Intelligence assets in the UK will need to infiltrate suppliers in order to maximise our chances of compromising the Dreadnought programme early in its manufacture stage.

Method 2: Any personal computer may have a compiler installed (If the operating system is based on Windows. Unix/Linux based systems already have compiler installed by default). Our intelligence asset within the Vanguard gold team will need training up with instructions on writing the code. He will be able to design, compile, deliver and deploy the malware inside the vessel whilst on patrol, and be able to control and monitor the malware. This method can be used to map the patrol course of the submarine using the data from the infected internal network, giving us valuable intelligence for future patrols.

Method 3: Physically introducing long term malware into control systems, similar to Stuxnet, that could distort data from the sensors in a controlled manner to confuse submarine command, communications, navigation and missile targeting, or be triggered when the submarine engages in activity consistent with a launch sequence.

The malware that targets control systems matching with those onboard the submarine (any system connected to critical control systems), can be used to infect control systems within the vessel. Sophisticated cross-platform malware may operate on multiple control systems and multiple operating systems.

6. Implications Of These Vulnerabilities

Perhaps the most likely form of attack would target critical systems on the submarine: reactor operations, missile control or the stealth of the submarine. Other systems could be targeted, such as internal communications control stations, water purification systems, oxygen level controllers or sanitation systems, to neutralise the submarine's operation.

Cyber-attack techniques might be used to interfere with communications to and inside the submarines, or to broadcast from the submarine and thereby give away its position; they may either jam (or otherwise prevent) the exchange of messages and data, or create misleading or incorrect information. The worst-case, though highly unlikely, scenario would be unauthorised missile launch (by stealing and transmitting launch authorisation codes to the submarine), or spoofing a nuclear attack. This type of attack would require the most sophisticated, highly skilled and resourceful hackers working in combination with an extensive intelligence operation, probably including a so-called "false-flag" operation (a major concern due to the problems of attribution of cyber-attacks).

When on operations, submarines are generally prone to infiltration and covert surveillance, and in war and crisis they are vulnerable to being disabled, damaged or retargeted by surprise. In other words, submarines could be widely compromised in peacetime without anyone knowing, and their operations explicitly impacted only during conflict. Any electronic interference in the middle of a crisis could be highly destabilising, not least because crisis involves stress, confusion and often poor decision making. Indeed, cyber interference could make it increasingly difficult for all those involved to separate malfunction from alerts or attack (particularly if this also involved denial of service attacks), and incentivise early missile launch.

The cyber threat to the Vanguard and Dreadnought submarines cannot be considered an isolated challenge. Technologies are advancing at a rapid and unpredictable pace and present numerous challenges to current UK military doctrine and equipment, a problem that can only get worse. Many of these augment new threats associated with the cyber domain. The spread and mounting capability of ballistic missile defences, as well as advances in automated and autonomous robotics and engineering (such as underwater drones, aerial drones with diving capabilities, etc.), make guarding classified intelligence about stealth technologies, patrol areas, missile and warhead specifications and performance data as important as ever and more difficult. The ever-increasing complexity and sophistication of the control systems upon which the submarine, personnel, missiles and warheads rely, makes security of the supply chain and particularly software upgrade and updates of paramount importance.

Submarines have been assumed to be the most secure, stealthy, credible and reliable platform available since the 1960s. With the latest emerging malware propagation techniques, the security of UK submarines on patrol is less assured. They may already have been compromised, but in future confidence must surely be more uncertain.

7. Counter Measures

Rigorous cyber defensive measures are an essential response to the growing threat; at every point of operation and intervention: development, construction, patrol and maintenance. They require very expensive state of the art detection technologies and simulation exercises to respond to all potential cyber-attack scenarios.

Cyber security is no trivial task when there is a complex network of hundreds of private commercial suppliers, many of which it must be assumed have weak security controls in place. The problem for those that are responsible for cyber security is that they have to anticipate every possible vulnerability, and engage in offensive cyber operations themselves against potential attackers in order to gather prior intelligence concerning methods, intention and attack vectors. It rapidly becomes a continuous and active cyber conflict in which all sides attempt to penetrate each other's systems.

The first step is to assess and classify the vulnerabilities. Vulnerability is all about the intersection of three elements: the existence of a system susceptibility or flaw, an attacker gaining access to that flaw, and then an attacker developing their capability to exploit the flaw. Vulnerabilities are classified according to the asset class they are related to:[52]

- Hardware (e.g. susceptible to humidity, dust, soiling, unprotected storage);
- Software (e.g. insufficient testing, lack of audit trail);
- Network (e.g. unprotected communication lines, insecure network architecture);
- Personnel (e.g. inadequate recruiting process, inadequate security awareness);
- Physical site (e.g. area subject to flood, unreliable power source);
- Organizational (e.g. lack of regular audits, lack of continuity plans, lax security protocols).

Any risk management processes entail prioritisation. The Common Vulnerability Scoring System is an open framework for communicating the characteristics and severity of software vulnerabilities.[53] Vulnerabilities can be categorized in order to develop an adequate response by severity, as exploitable and non-exploitable, or as server side and client side. Responses include adding a patch, mitigating the risks and remedying the vulnerability.

Access to the internet and the use of wifi and bluetooth on board during patrol is strictly forbidden for all crew members. Computer systems and networks devoted to morale, welfare and recreation are isolated from mission critical systems and protocols in place to minimise the chances of cross-infection between systems. Personal computers and phones are not allowed on board, and only specifically designed devices are in use.[54] Ideally. But if the revelations of crew member McNally in 2015 have any truth to them, such protocols may only operate on paper. Maintaining high vigilance and security priority on patrols that last several months and where trust builds up within crews is a very tall order.

"Cyber security is no trivial task when there is a complex network of hundreds of private commercial suppliers, many of which it must be assumed have weak security controls in place... It rapidly becomes a continuous and active cyber conflict in which all sides attempt to penetrate each other's systems."

The next generation of SSBN will require a team of cyber security experts, employed both remotely and on board, who perform 24/7 monitoring and control. They will need to monitor all external and internal communication. The internal protocols for routine internal checks while on patrol will need to be updated regularly.

If a communication channel is encrypted and bi-directional, an attacker can actively eavesdrop by intercepting an open key exchange message (during the initiation of the communication channel) and retransmit the message while replacing the requested key with his own. As the submarine does not broadcast communication signals, this type of attack is only applicable in systems that go through the process of establishing the full communication channel (protocol procedures, such as "handshakes" and key negotiations) in the Command and Control Centre. When this happens, it leaves a trace. For example, when attackers perform ARP (Address Resolution Protocol) spoofing to send or receive communications, trace elements are left on the routing devices. It is then possible when detecting these traces to conduct counter offensive cyber operations against the attacker.

52. ISO/IEC, "Information technology -- Security techniques-Information security risk management", ISO/IEC FIDIS 27005:2008
53. FIRST, 'Common Vulnerability Scoring System, V3 Development Update', (10 June 2015), http://bit.ly/1L4hNz7
54. Though there have been reported breaches of these protocols; Colin Daileda, 'U.S. Navy Debuts E-Reader Without Wi-Fi, Which Is Perfect for Submarines', *Mashable UK*, (May 7 2014), http://on.mash.to/2pXADR3

8. Future Related Trends

The maritime world is moving towards a more demanding techno-military strategic environment for submarines in which cyber is a key part, and this will play an increasingly influential role in decisions over the UK nuclear deterrent in the years ahead.

Military systems will be highly networked to communicate, intercept and control vast swathes of territory, at sea and in cyberspace; stealthy submarines will be an anomaly attempting to remain 'off the grid'.

Development, procurement, testing, deployment and installation of SSBN systems, including electronic control systems, take years before the submarine starts its first patrol. The Blair government announced its decision to start the concept phase of SSBN replacement in December 2006, stating that the process would take 17 years and that the first submarine would be available on patrol in 2024.[55] The Initial Gate, when teams started detailed designs for the system, was four years later in 2011.[56] A decision was announced in the November 2015 Strategic Defence and Security Review that the submarines would be constructed in a modular manner, and physical work to being constructing the main body of the first submarine commenced in the Autumn of 2016.[57] This submarine is not now expected to start patrolling until the early 2030s, a full quarter century after the decision was first taken to move on this project, and 15 years after the designs were finalised and construction on the submarine began.

Very basic versions of the predecessor to today's smart phone were only just coming onto the market 15 years ago. The iPhone 6, launched in September 2014, can process instructions 2000 times as fast as the computer on board a state of the art US F22 Raptor aircraft, the most sophisticated fighter aircraft on combat duty in the US Air Force today. Each generation of smart phone is overtaken by the next in the space of a year or two.[58] Technology involved in the smart phone is highly relevant to military technology, including robotics and sensing, that could enable interception and tracking of submarines. The development of civil technologies is starting to outstrip and determine the application of technology on the battlefield, largely because the market and related investment in R&D is so massive.[59]

Work on the bespoke software for a submarine's command and control system is developed alongside the hardware choices made throughout the design and construction of the submarine. By the time the submarine starts active service the technologies on board will be out-dated by a number of generations, and may already have a large number of vulnerabilities discovered by others despite their classification. These discoveries can be made by attackers when penetrating other (less secure) operating, software and hardware systems using similar code (programming language, framework, kernel, etc.), or more directly by attackers targeting the SSBN systems themselves. Maintenance, updates and upgrades require further time and funding, and themselves become sources of vulnerability and a means to penetrate the cyber systems upon which the SSBN depends.

Maintaining strategic superiority in an age of mass surveillance and data sharing, and rapid development and proliferation of technology and processing power across civil and military sectors, is a major challenge fraught with uncertainty and complexity. Information that previously was available only by the means of military reconnaissance is now

publicly available to any person with any communication device. Military reconnaissance itself has developed extraordinary capabilities that improve year by year. Its ability to detect and neutralise submarines, using a network of capabilities including satellites, aircraft and other maritime platforms; unmanned vehicles in the air, on the surface and under water; and a variety of static and mobile sensors and communication relays is also rapidly developing, using networks of small and cheap platforms deployed at scale and quickly replaced by newer technologies. It may at some point in future, for example, be possible to deliver proximity transmitters and hacking devices to the hull of the vessel to infiltrate the submarine onboard network even under water.

Underwater communication relays and networks are being deployed that will increase the interconnectivity of the military systems and facilitate detection and interception of submarines, including by cyber-attack.[60] The submarines themselves may be able to communicate more frequently with command facilities ashore, but this will expand the possibilities for cyber-attacks, and making it more difficult to apply countermeasures against remote hacking.

Communications based on optical data transmission (fast-blinking LEDs) can detect undersea vessels.[61] Communication will continue to be a vulnerable part of command and control, relying heavily on interconnectivity and network architecture. Radio frequency interception remains a possibility, as does spoofing. The submarine may become increasingly vulnerable to radio frequency interception, or possibly even the use of sonar to steal or inject data.[62]

The construction, assembly and maintenance of submarines is ever more automated and robotized, and a far greater proportion involves complex electronics. The nuclear reactors themselves are becoming more sophisticated and rely on complex interconnected devices and electronic networks.

Polymer electronics and 3D printed weaponry, undetectable by metal scanners, will require specific security measures. Nano technologies are being developed to improve surveillance, espionage and warfare. Advancing nano and bionic technologies, implantable and subdermal data storage and communication devices, all offer means to covertly infiltrate the vessel. Surveillance nano drones, nano microphones and communication devices, miniaturization of computer systems that can fit in a watch, ultra-high capacity data storage devices will bring multiple benefits, but also increase the threat of interception and unauthorised manipulation.

When the Chinese seized a US underwater drone in the South China Seas in December 2016 the incident surfaced a rapidly-expanding arms race in underwater surveillance and combat capabilities.[63] Aerial Drones with diving capabilities are in development.[64] A number of sensing and communications technologies are rapidly improving and will be deployed on unmanned vehicles across the maritime space in a system of systems that will have game-changing impact upon the ability to hunt submarines.[65] This technology will be further developed for rapid underwater payload delivery or underwater payload exfiltration from any location in the world, threatening the viability of future submarines.

55. Ministry of Defence, 'The Future of the United Kingdom's Nuclear Deterrent', Defence White Paper (December 2006)
56. Ministry of Defence, 'The United Kingdom's Future Nuclear Deterrent: the Submarine Initial Gate Parliamentary Report', (May 2011)
57. National Security Strategy and Strategic Defence and Security Review 2015, (November 2015)
58. David Hambling, *The Inescapable Net: Unmanned Systems in Anti-Submarine Warfare*, British American Security Information Council, (13 July 2016), http://bit.ly/1RC55KE
59. David Hambling, *Swarm Troopers, how small drones will conquer the world*, Amazon (2015)
60. The DARPA tactical undersea network is one example; Shelby Sullivan, 'Tactical Undersea Network Architectures (TUNA)', http://bit.ly/2rvbiP3
61. Kate Yandell, 'The Navy's New Underwater Internet', *Gizmodo*, (3 July 2014), http://bit.ly/2qvxdbc
62. Martellini M., Abaimov S., Gaycken S. and Wilson C., *Information Security of Highly Critical Wireless Network*s, Springer, (2017); Geoffrey Ingersoll, ' US Navy: Hackers "Jumping the Air Gap" Would 'Disrupt the World Balance of Power', *Business Insider*, (November 2013), http://read.bi/2qWhfbF
63. Ben Blanchard and Steve Holland, 'China to Return Seized U.S. Drone, Says Washington "Hyping Up" Incident', Reuters, (18 December 2016), http://reut.rs/2q0lnIR; http://bit.ly/2r0jTNn; http://bit.ly/1SPtBJ9
64. http://bit.ly/2r0Akta; Navy League 2017, NRL furthers Flying Sea Glider effort, IHS Jane's 360, http://bit.ly/2pXiPpw
65. BASIC and Pugwash have several publications in production in mid 2017 by Miguel Batista. See also David Hambling, *The Inescapable Net: Unmanned Systems in Anti-Submarine Warfare*, British American Security Information Council, (13 July 2016), http://bit.ly/1RC55KE

FICTIONAL SCENARIO 4:

Disrupting guidance systems for Trident missiles

Memo Dated: 21 December 2015
From: [Foreign] Naval Intelligence, Unit 6B

Mission: To develop a capability with multiple dimensions to disrupt communications and guidance of Trident II D5 missiles.

Objective: Complete satisfactory infiltration of the D5 supply chain, insert our hardware and software into components, and set up a mixed system of autonomous and remote triggers to disrupt, perhaps even control.

Method 1: Disrupt guidance and telemetry signals using autonomous malware. Naval intelligence has operatives in two key sub-contractors involved in the design and supply of components for the guidance system as part of Lockheed Martin's life extension programme for the D5. These components are in the middle of testing and integration, and our operatives have been successful in injecting new forms of malware that are under development under the guidance of our DEVCOM_2 team. We are now ready to test the operation of this installed malware in a forthcoming Trident II D5 test by switching to a green light. Should this test be successful, we plan to expand operations in this direction in order to have multiple means of disrupting launch, trajectory and warhead separation, and to explore options for disrupting the fusing of the warhead itself.

Method 2: intercept signals to confuse communications, perhaps even to take control of the missile. Once the missile leaves the water our malware on board can communicate via satellite or maritime assets [ships, aircraft, unmanned vehicles] with naval command. Malware currently in development and connected to the guidance system on board the missile will, on launch, trigger a transmitter using variable, cloaked frequency that will enable remote control via satellite or assets nearby. This will enable naval command to alter the trajectory of the missile, block or disrupt communications between the missile and US Naval Command and the Trident submarine, or trigger the warhead fuse into premature activation.

9. Conclusion

This report clearly demonstrates that the UK's Trident system, though benefiting from the highest classification of security and attempts to shore up weaknesses, remains vulnerable to cyber-attack.

The potential cyber-attack vectors cover three life stages of submarines: construction, patrol and maintenance. Each of these stages contains specific vulnerabilities to be investigated, assessed and monitored. The defensive measures should include physical and cyber-security solutions with the use of the state of the art detection technologies and simulation exercises to respond to all potential scenarios.

In the development stage, one of the attack scenarios is that the sensitive design, or operational secrets related to the UK nuclear weapons system, could be compromised through cyber espionage. The construction period also entails probability of the malware being installed into the electronic devices to be activated in patrol. During the manufacturing and assembly of the submarine and internal systems, predetermined security flaws may be introduced, to be potentially exploited in the future. Otherwise, malware may be uploaded into a device or a network of devices, for it to conduct an attack autonomously at a predefined moment or under specific circumstances. The patrol phase relies on internal and external communication and network of systems, which are vulnerable to internal cyber-attacks. The submarine can be infiltrated with autonomous malware when undergoing maintenance or delivered via storage devices or even via remote communication channels.

Another risk is connected with the high speed of technology development. Any electronic device installed in submarines today is soon outdated. A team of permanent cyber-security experts will be needed online strengthen defence both internally and externally. Updates of software and hardware should be implemented on a regular basis, as well as rigorous testing and inspection routines, simulation exercises and "offensive" security tests of various aspects related to the cyber and information security. All this also acknowledging that such activities themselves can also be the source of cyber-threat. False economies when choosing operating systems, software and hardware should be avoided.

It was announced in the 2015 Strategic Defence and Security Review that the Successor submarines would be constructed in a 'staged investment programme', or a modular fashion, which may give greater flexibility in the manufacturing.[66] Maintaining maximum adaptation in these phases will be critical, but is a huge challenge. There is also a challenging trade-off between nimble, flexible and responsive systems, and the essential security, including cyber-security, that could reduce the risk of infiltration or theft. Among the myriad potential threats which need to be continually assessed throughout are wireless communication technologies, networks of unmanned maritime vehicles capable of detecting submarines and possibly delivering electronic payloads, nano devices, polymer electronics and 3D printed weaponry.

There should be no doubt that whilst the issues outlined in this report have strands of both continuity (anti-submarine warfare, attempts to compromise the operations of adversaries' military activities, ever-unfolding technological change) and disruption (emerging dominance of cyber as a form of warfare and disruption, re-emergence of doubt around the ability of leading nuclear weapon states to deliver their nuclear payloads on an adversary), there are some crucial uncertainties over the consequences emerging for nuclear doctrine, deterrence and stability.

This report has focused on the cyber vulnerabilities of the UK's nuclear submarines, but of course, cyber insecurity is relevant to all forms of military equipment, and particularly for other nuclear weapon delivery systems. It has been said that because of the operational air gap, submarines are relatively more secure than other platforms. This may be true, but there are particular consequences for ballistic missile submarines because of their mission as an assured second-strike capability. These have been assumed to be effectively invulnerable to first strike attack, and to have stabilised strategic relations between the United States and the Soviet Union, then Russia, for over half a century. If confidence in these platforms is harmed then this could have unpredictable consequences upon strategic stability, and crisis instability that need to be studied more closely.

When an attacker successfully penetrates a nuclear weapon system they may have knowledge of that achievement and the nature of the compromise when defenders do not. It may mean that one state thinks its adversary's nuclear deterrent is successfully compromised in the run up to a crisis, when that adversary believes it is operational. One excellent example of this was the reported use of Suter by Israel to compromise Syrian air-defences and enable the attack on the Syrian reactor in 2007.[67] Incomplete knowledge in the cyber domain could encourage overconfident state leaders overplaying their hands in a crisis.

Commanders may be less confident of the readings of their instruments, and experiencing denial of service attacks, may be more reluctant to move to alert status and fire when presented with what appears to be a nuclear attack or orders from their commander in chief. This may strengthen the informal nuclear taboo that has developed since the Cold War, with uncertain impact upon the salience of nuclear deterrence. More likely is that the pressures on commanders to fire early whilst they still have control of their systems will add instabilities in crisis situations and the likelihood that leaders will fear strategic surprise.

The greater uncertainty may mean that states relying upon nuclear deterrence decide to deploy more systems with greater variety in order to maintain reliability. On the other hand, it could have the opposite effect, leading states to conclude that increasingly expensive nuclear deterrent systems requiring ever more sophisticated cyber defences may be replaced by other means to achieve deterrence and other objectives that lie behind deployment.

Just as in counter-terrorist operations, recognising the nature and scale of the cyber threat, systems managers have to consider deterrence, resilience and mitigation as well as prevention. When developing civilian cyber security systems, it is often deemed good practice not only to strengthen protection but also to assume that the network is already compromised and act accordingly. In other words, as well as having in place a first line of defence by prevention, network architecture and protocols need to be robust. This may involve back-up and recovery procedures, responses to intrusions, contingency plans that minimise damage, and forms of offensive cyber operations.

There is a particular problem associated with the nature of cyber warfare and the trends that appear to favour offensive over defensive operations as systems become more complex and integrated, hacking tools proliferate, and states allocate more resources to their offensive cyber capabilities.[68] Those responsible for cyber security themselves need to engage in offensive cyber intelligence operations in order to track the intentions, capabilities and priorities of any attackers. This drives a cyber-security dilemma, in which adversaries compete to penetrate each other's nuclear weapon systems in part to secure their own.

The overall impact is one of far greater instability and uncertainty of outcomes. When considering the consequences of nuclear weapons use, and the widespread recognition that once a nuclear exchange starts between nuclear armed states it is very unlikely to remain limited, is this really an acceptable future?

66. *National Security Strategy and Strategic Defence and Security Review 2015*, (23 November 2015), p. 36, http://bit.ly/1Nnq2ZF
67. Andrew Futter, 'Cyber Threats and Nuclear Weapons', *RUSI Occasional paper*, (July 2016), p.24, http://bit.ly/2qvhgBP
68 Joseph Menn, '90 percent of federal cyber budget used for offensive ops', *Fifth Domain Cyber*, http://bit.ly/2qx7dfT

"The WannaCry worm attack earlier this month affecting 300,000 computers worldwide, including vital NHS services, was just a taste of what is possible when cyber-weapons are stolen. To imagine that critical digital systems at the heart of nuclear weapon systems are somehow immune or can be confidently protected by dedicated teams of network managers is to be irresponsibly complacent. When states invest hundreds of billions of dollars in offensive nuclear weapon systems, the incentives are there amongst adversaries to develop capabilities that could neutralise that threat. Leading states are now investing billions of dollars in their offensive cyber capabilities, degrading confidence in the effect of those nuclear weapon systems, in the strategic balance and crisis management. This report assesses those vulnerabilities."

Lord Browne of Ladyton, former Secretary of State for Defence (2006-8), is Vice-Chairman of the Nuclear Threat Initiative in Washington DC and Convener of the European Leadership Network for Multilateral Nuclear Disarmament and Non-proliferation

British American Security Information Council (BASIC)
3 Whitehall Court
Westminster
London SQ1A 2EL

Charity Registration No. 1001081

T: +44 (0) 20 77663465
www.basicint.org