Institution: University of Leicester		
Unit of Assessment: 19		
Title of case study: Securing nuclear weapons systems against cyber threats: risks, awareness and responses.		
Period when the underpinning research was undertaken: October 2013 – August 2016		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s): Andrew Futter	**Role(s) (e.g. job title):** Professor of International Politics	**Period(s) employed by submitting HEI:** January 2012 – Present
Period when the claimed impact occurred: 2014 – 2020		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact

International concern about the cyber threat to nuclear weapons systems has risen sharply in recent years in both political and public spheres. Debate, policy and thinking about this threat have been directed by research conducted by leading nuclear strategy and arms control expert Professor Andrew Futter of the University of Leicester. Futter's research has: (i) influenced legislative thinking; and (ii) shaped the public policy debate by challenging established norms, and changing public attitudes toward cyber-nuclear threats, the Trident debate and the changing nature of the global nuclear threat.

2. Underpinning research

The research carried out by Professor Futter at the University of Leicester since 2013 examines the cyber threat posed to nuclear weapons systems. This research, initially funded by a three-year ESRC Future Research Leaders grant, was the first major academic work to analyse the new challenges and risks posed to the security and safety of nuclear weapons systems in a new cyber era, and to provide the foundation of an operational framework for how these new challenges could be understood and addressed by experts, governments, Non-Governmental Organisations (NGOs) and the public.

Futter's research **[R1, R2]** exposed the dangerously low levels of understanding about the nature and seriousness of the potential cyber threat to nuclear weapons systems via academics to policy makers, nuclear-armed governments and international NGOs and the lack of public awareness.

Thus, a major objective of his work was to produce the first conceptualisation of the cyber challenge, explain what was vulnerable, how, to whom and why, and make sure this was communicated to relevant stakeholders with an interest in the safe and secure management of nuclear weapons. This was achieved through a publication strategy that targeted specific outlets that would reach practitioners and policy makers as well as raising public awareness via mainstream media outlets to inform public opinion. This strategy ensured that awareness and understanding was substantially raised society-wide, thus driving real-world change.

Three significant findings from the research form the basis of the claimed impact:

(1) **Nuclear weapons systems are more vulnerable than governments have realised or acknowledged in the past**. Part of the research was motivated by concern that officials across the globe steadfastly said that nuclear weapons systems could not be hacked, because, for example, they were not connected to the Internet. Futter's research, notably his monograph **[R1]** and occasional paper **[R4]** showed that some key nuclear weapons systems are not in fact separated from unsecured networks and that, even if they were, systems could still be hacked, particularly while they were being built/maintained or through attacks on operators or the supply chain. The research stimulated a global debate on the implications of this for nuclear strategy, deterrence and arms control.

(2) Futter argued that the **UK Trident nuclear weapons system is not as invulnerable as conventional wisdom or UK government claim,** and that a recognition of this needed to be part of the public debate over whether the UK should retain or renew this system in the future. Futter was invited by the European Leadership Network (an independent, non-partisan, pan-European network of nearly 300 past, present and future European leaders working to provide practical real-world solutions to political and security challenges), to write a policy brief during the Trident renewal debate in 2016 to ensure the issue reached public and policy consciousness and that decisions would be informed by accurate assessment **[R3]**.

(3) Futter's research found that there are several dangerous new pathways to nuclear use and escalation driven by cyber risks, the new digitised nuclear context, and increased risk of nuclear explosion resulting from a new cyber-nuclear nexus. Futter's research identified and highlighted the **implications of the little-known US defence programme designed to hack into the missile and nuclear systems of its opponents** [**R5, R6**]. **[R5]** in particular, emphasises the risk of directing resources to a cyber-defence programme which not only has to anticipate and disrupt potential nuclear attack from other states whilst ensuring US technology remains sophisticated enough to hack enemy systems, but may pull resource away from developing and maintaining physical defence capability to effectively neutralise missile attacks once launched. In addition to the physical risk of pursuing such a policy, Futter outlines the political dangers, including normalising this as a political tactic and not providing sufficient protection against non-state aggressors.

3. References to the research

R1. Futter, A. *Hacking the Bomb*. Washington D.C., Georgetown University Press: 2018.
R2. Futter, A. "War Games Redux: Cyber Threats, U.S.-Russian Strategic Stability and the New Challenges for Nuclear Security and Arms Control." *European Security*. 24:2 (2016), pp163-180.
R3. Futter, A. "Is Trident Safe from Cyber Attack". European Leadership Network Policy Brief. 5 February 2016.
R4. Futter, A. "Cyber Threats and Nuclear Weapons". Royal United Services Institute Occasional Paper, (July 2016).
R5. Futter, A. "The danger of using cyber-attacks to counter nuclear threats". *Arms Control Today*. July/August 2016.
R6. Futter, A (ed.), *The United Kingdom and Nuclear Weapons*. Rowman and Littlefield: 2016.

4. Details of the impact

Research undertaken by Professor Futter at the University of Leicester has had international impact in two main areas: (i) influencing legislative thinking; and (ii) shaping the public policy debate by directly influencing lobbying groups and media coverage.

Influencing legislative thinking

Futter is a leading authority on nuclear cyber-threats and has provided evidence to the UK government several times between 2014 and 2018. In 2014, Futter provided written evidence outlining how cyber risks would alter deterrence thinking and escalation pathways, to the House of Commons Defence Committee, "Deterrence in the 21st Century" inquiry **[E1c]**. Written evidence from Futter in 2015, warning that UK nuclear weapons might be "less credible, useable or efficacious in the years to come" as a result of new cyber risks, was published by the House of Commons Defence Committee's inquiry "Flexible response? An SDSR checklist of potential threats and vulnerabilities" **[E1b].**

Futter was commissioned in 2016 to provide his expertise to underpin a section on "Cyber interference with a nuclear weapon", for the House of Commons Library POSTnote on Nuclear Security **[E1d]**, and his work was cited as recommended further reading in a House of Commons Library Briefing Paper on Trident **[E1e]**.

In 2018, he was invited to give oral evidence to the House of Lords Select Committee on International Relations inquiry into "U.K. Foreign Policy in a Shifting World Order", providing testimony on the cyber risks posed to the UK Trident nuclear weapons system **[E1a]**.

Briefings delivered by Futter to the UK Cabinet Office and the Top-Level Group of Parliamentarians for Nuclear Disarmament in 2018, at their request, has significantly shaped the thinking of key decision makers. He has worked closely with former UK Secretary of State for Defence, Lord Desmond Browne to direct parliamentary debate on the cyber threat to UK nuclear weapons. Lord Browne writes that: "*I have found Andrew Futter's work significantly influential in my evolving thinking about the dangers which the cyber threat to the command and control of nuclear weapons poses to strategic stability. I know from my conversations with other Parliamentarians that the same can be said for many of them*" **[E2]**.

Based on his expertise, Futter was invited twice in 2018 to brief the UK Cabinet Office on cyber-nuclear risks; both briefings have been described by a policy Advisor to the Cabinet Office as "*a really important contribution to our thinking*" **[E3].** Internationally, Futter was invited to brief the U.S. Strategic Command in 2018. As the agency responsible for integrating and coordinating the necessary command and control capability to provide support with the most accurate and timely information for the President, the Secretary of Defense, other national leadership and combatant commanders, including the oversight of the security of US nuclear weapons, this group represents influential stakeholders and details of Futter's briefing and presentation were shared via the US Strategic Command Academic Alliance newsletter in January 2019 **[E4]**.

Shaping the public policy debate

Futter's work has guided the formulation of positions of lobbying organisations and other stakeholders, as well as starting to shape approaches to the reporting of cyber-security in the media and engaging with information security professionals.

His research has been vital for the Washington D.C. based Nuclear Threat Initiative in their lobbying of the US government on cyber-nuclear risks [**E5a]**. Futter is a member of the Nuclear Threat Initiative's Cyber-Nuclear Weapons Study Group convened in 2017, in order to gather former senior military officials and top nuclear policy and cyber security experts to assess the risks posed to nuclear weapons by cyber threats and to develop policy to reduce those risks. As a 'leading voice' on the cyber threat to nuclear weapons systems based on his track record of high-quality research, Futter is a 'key member' member of this Group **[E5b]**. The Group published their influential first report 'Nuclear Weapons in the New Cyber Age' [**E7**] in 2018 and this has been cited by lobby groups and opinion-makers such as the Russian International Affairs Council, The United Nations Institute for Disarmament Research and Modern Diplomacy **[E10a]**.

The British American Security Information Council 2017 report 'Hacking UK Trident: A Growing Threat' **[E8]** gained national press coverage **[E10b]** upon its publication and features Futter's research, particularly **[R4]** which is described as "excellent" **[E8]**. The 2017 Nobel Peace Prize recipients, the International Campaign to Abolish Nuclear Weapons, invited Futter to help them shape their future research agenda and contribute to the development of their 2020 Briefing Paper 'Emerging technologies and nuclear weapons risks' **[E11]**.

Collaborating with professionals working in and reporting on cybersecurity, Futter is now embedding his research within a range of professional approaches. In 2019, Futter underpinned the design and delivery of training to a workshop for leading international journalists on reporting cyber-nuclear risks. The Executive Director and Founder of Atomic Report, the workshop organisers, stated that Futter's "*input was essential in helping this group of journalists understand how best to report and write about contemporary nuclear risks"* **[E6]**. Later in 2019, Futter was the invited keynote speaker at the CODE BLUE information security conference in Tokyo engaging with IT security specialists about the real-world impact of their work **[E9]**.

Futter is recognised as one of the leading experts on cyber-nuclear risks globally. His research is impacting and informing practitioners and policy makers and is repeatedly referenced in the national and international press **[E10c]**. In 2018 for example, Futter's research was mentioned throughout the *New Statesman's* Spotlight (a series of highly focused policy reports) Special Issue on Cyber Security **[E10c]**. Thus, Futter is directly informing public opinion on cyber-nuclear threats as well as informing legislative development and professional approaches across military and civilian sectors.

5. Sources to corroborate the impact

E1. Citations in UK Parliamentary Documents.

a. UK House of Lords, Select Committee on International Relations, 5th Report of Session 2017-19, "UK Foreign Policy in a Shifting World Order", HL Paper 250, (18 December 2018).

b. UK House of Commons Defence Committee, "Flexible response? An SDSR checklist of potential threats and vulnerabilities, First Report of Session 2015–16, HC 493, (21 November 2015).

c. UK House of Commons Defence Committee, "Deterrence in the Twenty-First Century", Eleventh Report of Session 2013-14, HC 1066, (27th March 2014).

d. UK Houses of Parliament Office of Science and Technology, POSTNOTE "Nuclear Security", Number 540, (October 2016).

e. UK House of Commons Briefing Paper Number 7353, "Replacing the UK's 'Trident' Nuclear Deterrent" (July 2016)

E2. Testimonial: Lord Desmond Browne of Ladyton, former UK Secretary of State for Defence.

E3. Testimonial: Policy Advisor, UK Cabinet Office.

E4. Deterrance and Assurance, US Strategic Command newsletter. https://www.stratcom.mil/Portals/8/Documents/DA3_Newsletter_Jan_19.pdf

E5. Nuclear Threat Initiative, Washington D.C.

a. Testimonial: Senior Vice President, Nuclear Threat Initiative, Washington D.C.

b. https://www.nti.org/analysis/atomic-pulse/cyber-threats-nuclear-weapons-should-we-worry-conversation-dr-andrew-futter/

E6. Testimonial: Executive Director of Atomic Reporters

E7. Nuclear Weapons in the New Cyber Age: Report of the Cyber-Nuclear Weapons Study Group 2018 https://media.nti.org/documents/Cyber_report_finalsmall.pdf

E8. Hacking UK Trident: A Growing Threat, 2017. https://basicint.org/wp-content/uploads/2018/06/HACKING_UK_TRIDENT.pdf

E9. Code Blue 2019: an international conference of the world's top class information security specialists https://codeblue.jp/2019/en/talks/ testimonial.

E10. Public debate.

a. Related to [E7]

https://russiancouncil.ru/en/analytics-and-comments/analytics/the-nuclear-dimension-of-cyber-threats/

https://unidir.org/files/publications/pdfs/nuclear-risk-reduction-a-framework-for-analysis-en-809.pdf

https://moderndiplomacy.eu/2019/07/19/the-nuclear-dimension-of-cyber-threats/

b. Related to [E8]

https://www.independent.co.uk/news/uk/home-news/uk-nuclear-submarines-cyber-attack-vulnerable-nuclear-war-security-experts-royal-navy-a7767496.html

https://www.dailymail.co.uk/sciencetech/article-4562476/Trident-submarines-hacked-start-nuclear-war.html

https://www.theguardian.com/uk-news/2017/jun/01/uks-trident-nuclear-submarines-vulnerable-to-catastrophic-hack-cyber-attack

c. General press coverage.

https://www.newstatesman.com/sites/default/files/ns_spotlight_cyber_security_supplement_may_2018.pdf

https://www.express.co.uk/news/world/949437/cyber-attacks-fake-news-threats-nuclear-security-expert-warns

https://www.thenational.scot/news/14901643.trident-alert-as-expert-says-nuclear-weapons-cannot-be-made-completely-safe-from-cyber-attack/

https://www.dailymail.co.uk/news/article-4849332/GUY-WALTERS-cyber-warfare-way-rid-Kim.html

E11. https://www.icanw.org/ican_hosts_meeting_on_emerging_technologies

https://www.icanw.org/briefing_emerging_technologies_and_nuclear_weapon_risks