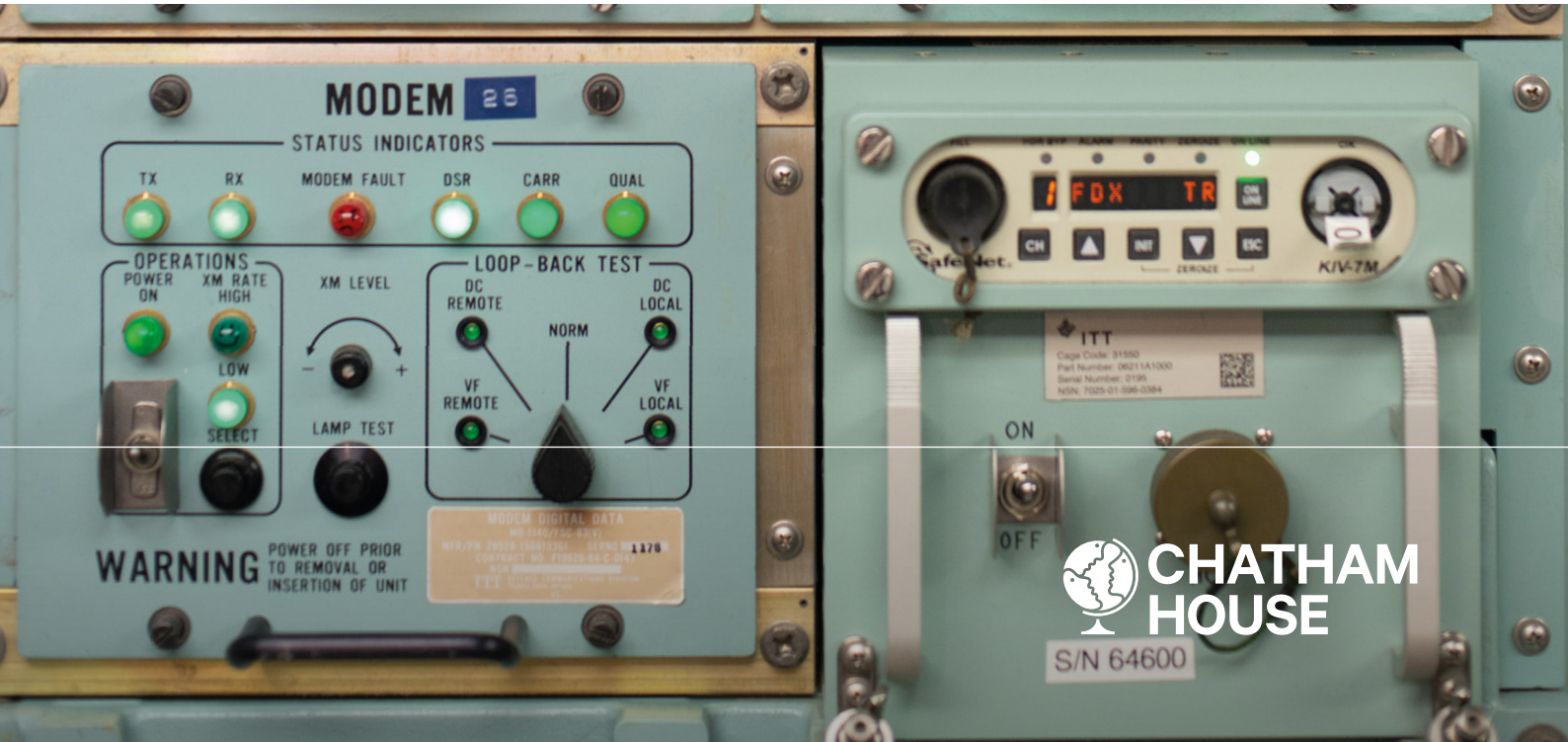
Research Paper

Yasmin Afina, Calum Inverarity and Beyza Unal
International Security Programme | July 2020

Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems



CHATHAM HOUSE

Contents

Summary	2
1. Introduction	3
2. Command, Control and Communication in NATO	7
3. Nuclear Command, Control and Communication	14
4. Entanglement of Conventional and Nuclear Command and Control	29
5. Legal Implications of Attacking Dual-use C3 Systems	31
6. Conclusion and Way Forward	33
Appendix 1: NATO Allies' Nuclear Planning and NC3 architecture	36
Appendix II: Nuclear Sharing	45
Appendix III: Control Deficiencies and Vulnerabilities	50
Acronyms and Abbreviations	52
About the Authors	54
Acknowledgments	55

Summary

- NATO's nuclear capability is provided by the US and the UK. The modernization of systems and arsenals held by both states is proceeding apace. This has involved – and continues to involve – the integration and use of increasingly sophisticated new technologies within their nuclear programmes, including in their respective command, control and communication (C3) systems.

- Cyber operations targeting NATO members' C3 systems and their assets, including nuclear assets, are also increasingly sophisticated in nature. While cybersecurity is a serious concern, and there is acknowledgment of the potential magnitude of cyberattacks, documentation available in the public domain indicates the need for NATO and its members to put in place further measures to ensure the cybersecurity of C3 systems, including those of nuclear systems (NC3). This is all the more pertinent given that some Allies' military capabilities still include legacy systems from the Soviet era.

- The protection of C3 systems requires the adoption of adequate, adaptable and robust cybersecurity measures, in order to ensure the integrity of these systems and to shield them from both internal and external disruption. The following five considerations are of relevance for the protection of NATO's own C3 systems, and those of its member states: software and network protection; data (integrity) protection; hardware protection; access/security controls; and cybersecurity awareness/security by design. These attest to the need for robust measures beyond the non-kinetic, digital realm to ensure the cybersecurity of NATO's C3 ecosystem.

- The increasing reliance on C3 assets that may be used for both conventional and nuclear operations raises the prospect of entanglement, and the associated risk of rapid escalation. The potential for unintended escalation is further exacerbated by the threat of cyberattacks and possible new threats emanating from other emerging technologies, including quantum computing. Unknown and unanticipated effects from cyber operations targeted at C3 assets may compromise the legality of these attacks when such assets may be of both military and civilian use simultaneously.

- Measures to prevent misinterpretation and rapid escalation are critical to the security of C3 systems. Such measures could include a clearer understanding of: how adversaries think about command and control; what would constitute a cyberattack in the context of C3 systems; and what would constitute adequate responses to such attacks within the frameworks of international law – particularly international humanitarian law.

- False confidence and false stress are equally problematic. In addition to ensuring the cybersecurity of their existing nuclear planning and NC3 architecture, NATO and Allies must reflect on how these dynamics will affect current understanding, arrangements and strategies surrounding the concept of nuclear sharing. Concerns over legacy infrastructure, in the context of an evolving threat landscape and the modernization of systems with digital means, raise questions with regard to the way forward for the hosting of US nuclear weapons in Europe, as well as for existing nuclear burden sharing agreements.

1. Introduction

With the growing sophistication of cyberthreats and digitalization of weapons systems, it is difficult to ensure cybersecurity from the design stage to deployment of a weapon system. Weapon systems increasingly rely on cutting-edge technologies in order to improve efficiency and accuracy. These technologies, however, may render weapon systems more vulnerable to cyberattacks. Some of the recurring technical aspects of weapons design that increase cyber vulnerability include:[1]

- Software dependencies
- Hardware dependencies
- Increased connectivity of networked systems
- Automation/autonomy

This is not necessarily a big problem. Cyberattacks against networked systems are not new, and they can be defended against and the worst impacts prevented. The problem is compounded, however, when countries put too much trust into complex systems that they consider failsafe and immune to cyberattacks – and subsequently choose to neglect the full range of potential threats and vulnerabilities. In terms of explosive and long-term impact, nuclear weapons are significantly more powerful than conventional weapons. Yet the system design of nuclear and conventional weapon systems is intertwined[2] through command, control and communication (C3) structures. Acknowledging that there are differences in functionality and varying levels of complexity between conventional and nuclear weapon systems, neither nuclear nor conventional C3 structures are, however, immune to cyberattacks.

For NATO, given a spectrum of weapon systems that has conventional means at one end and nuclear at the other, cyber technologies complicate warfighting and policy planning efforts. In conventional warfare, the fight is generally against a single adversary. When it comes to cyberattacks, decision-makers can find themselves combating multiple actors (both state and non-state) simultaneously and over a long period. In traditional policy planning, decision-making is structured around collective defence as enshrined in Article 5, whereby an armed attack against one

[1] A research paper published by Chatham House in 2018 provides a detailed examination of potential vulnerabilities, the nature of cyberthreats against nuclear weapons systems and potential actors. The paper also outlines the different types of cyber operations that might be conducted against nuclear weapons systems which, by extension, may also be conducted against NATO's NC3 systems and their assets – including sabotage through malware or viruses, interference, and hacking. See: Unal, B. and Lewis, P. (2018), *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf (accessed 3 Feb. 2020).

[2] See Acton, J. M. (2018), 'Escalation through entanglement', *International Security*, 43(1), pp. 56–99, doi:10.1162/ISEC_a_00320 (accessed 25 Sept. 2019). For an updated take on C3I entanglement from the same author, see: Acton, J. M. (2019), 'For Better or For Worse: The Future of C3I Entanglement', *Technology For Global Security*, Special Report, https://www.tech4gs.org/uploads/1/1/1/5/111521085/acton_sr.pdf (accessed 18 Feb. 2020).

NATO member is an attack against all members of the Alliance.[3] These parameters do not correspond directly to the cyber realm, which means that determining whether to invoke Article 5 measures may not be adequate and/or appropriate. The multiplicity of cyber incidents means that while NATO needs to take specific actions step-by-step, it needs to take these decisions on a daily basis. This puts tremendous strain on the traditional crisis management machinery.

It is important to realize that, in NATO, not all capabilities are generated, trained and exercised in the same manner. There are, variously, capabilities owned by NATO; capabilities that are provided by Allies; and other capabilities – such as offensive cyber operations – that are strictly under national control and conducted by states without NATO's involvement.

There have been several studies of the cybersecurity of nuclear weapon systems in recent years. Chatham House researchers have previously examined this issue, identifying cyber-vulnerable technologies in nuclear weapons systems in at least 13 areas.[4] Other researchers have also highlighted the growing threat and the need for managing risks.[5] However, due to classification issues, not much has been written for the public domain on NATO's C3 systems, and on how NATO incorporates cybersecurity into its capability development. Studies have also explored wider C3 issues such as the cyber vulnerabilities of NATO space-based strategic systems.[6]

Multiple issues arise from the literature in dealing with cyberattacks:

- **Attribution:** How can NATO and its Allies attribute malicious cyber activities? Is it useful to do so in all instances? If not, when is attribution important and valuable? How should NATO trust the reliability of the intelligence received from Allies and partner countries? What risks does NATO take when considering intelligence from external parties?

- **Response:** If NATO adopts a disproportionate response in a hasty manner, might this be considered as retaliation rather than response? If NATO responds consistently, would this result in deterrence against future attacks over time? What will reduce the risk and increase the gain (low risk/high gain) for NATO?

- **Deterrence:** What type of approach(es) could be successful against an adversary to deter them from attacking nuclear C3 (NC3) systems? Is successful deterrence achieved through deterrence by denial – i.e. by focusing on defensive measures, including resilience and redundancy? Or is it achieved through deterrence by punishment – i.e. by demonstrating that there are severe consequences for the aggressor? Is it through both deterrence by denial and deterrence through punishment? Or is it through neither?

[3] NATO (2019), 'Collective defence – Article 5', https://www.nato.int/cps/en/natohq/topics_110496.htm (accessed 25 Dec. 2019).
[4] Lewis, P. and Unal B. (2017), 'Cyber Threats and Nuclear Weapons Systems', in Borrie, J., Caughley, T. and Wan, W. (eds) (2017), *Understanding Nuclear Weapon Risks*, UNIDIR, pp. 61–71, https://www.unidir.org/files/publications/pdfs/understanding-nuclear-weapon-risks-en-676.pdf (accessed 26 Dec. 2019).
[5] Futter, A. (2018), *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, Washington, DC: Georgetown University Press. See also, Stoutland P. and Pitts-Kiefer, S. (2018), *Nuclear Weapons in the New Cyber Age*, NTI, https://media.nti.org/documents/Cyber_report_finalsmall.pdf (accessed 26 Dec. 2019).
[6] Unal, B. (2019), *Cybersecurity of NATO's Space-based Strategic Assets*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/publication/cybersecurity-nato-s-space-based-strategic-assets (accessed 30 Dec. 2019).

NATO's security and defence policy clearly outlines NATO as a nuclear Alliance, and states that for so long as nuclear weapons exist, NATO will continue to rely on them for deterrence purposes.[7] However, nuclear deterrence in the 21st century is in flux, due to a wide range of socio-political and technological challenges – among them cyber vulnerability.

NATO's nuclear capability is provided by the US and the UK.[8] Through the nuclear sharing principle, NATO's capabilities defend and protect all Allies. Moreover, all the non-nuclear weapon states within NATO (i.e. all Allies except the US, the UK and France) have committed, as signatories to the nuclear Non-Proliferation Treaty (NPT) not to resort to acquiring nuclear weapons themselves. It should be noted here that France, unlike the Alliance's other 29 member states, does not participate in the Nuclear Planning Group (NPG), the senior body responsible for determining NATO's nuclear policy and the role of its nuclear forces. (See Appendix I for further information on the NC3 architecture of the US, the UK and France.)

The nuclear burden sharing principle, which originated in the early 1960s, aimed to discourage proliferation while fostering unity and partnership across the Alliance.[9] Through this principle, Belgium, Germany, Italy, the Netherlands and Turkey currently host an estimated total of around 150 US forward-deployed nuclear weapons that are earmarked for the Alliance.[10] The US National Nuclear Security Administration (NNSA) is replacing the nuclear weapons deployed in Europe with modern systems through a life extension programme that consolidates four B61 models (B61-3, -4, -7 and -10) into a single design (B61-12). The B61-12 features new digital components, such as a guided tail-kit assembly, for increased accuracy. These digital upgrades make cybersecurity a greater challenge.[11]

This paper argues that NC3 is an area in which NATO cannot accept a high level of cyber risk. It is important to emphasize at the outset that this study comes with certain constraints. First, most of the open-source information comes from the Cold War period, and it must be assumed that NATO's nuclear planning and NC3 have evolved since then. Second, nuclear weapon states within NATO have been modernizing their NC3 structures; therefore, information available at present in the public domain may be contested. The confidentiality surrounding NATO's NC3 systems is in line with the importance of protecting these assets against potential threats. Therefore, this study comes with the predicament that it draws on open-source analysis and information, some of which was not officially verified. In addition, experts' analysis, including that of (former) officials, reflects their own subjective perceptions, such as confirmation bias and/or self-censorship, among others. The authors have attempted to partially mitigate this problem by including information and

[7] North Atlantic Treaty Organization (NATO) (2019), 'NATO's nuclear deterrence policy and forces', https://www.nato.int/cps/en/natohq/topics_50068.htm (accessed 16 Dec. 2019).
[8] Alberque, W. (2017), *The NPT and the origins of NATO's nuclear sharing arrangements*, Proliferation Papers, No. 57, Institut français des relations internationales, https://www.ifri.org/sites/default/files/atoms/files/alberque_npt_origins_nato_nuclear_2017.pdf (accessed 25 Dec. 2019).
[9] The White House (1964), 'The Future of the Nuclear Defence of the Atlantic Alliance', National Security Action Memorandum No. 318, 14 November 1964, https://www.discoverlbj.org/item/nsf-nsam318 (accessed 17 Dec. 2019).
[10] See Kristensen, H. M. and Korda, M. (2019), 'Tactical nuclear weapons, 2019', *Bulletin of the Atomic Scientists*, 75(5), pp. 252–261, doi: 10.1080/00963402.2019.1654273 (accessed 22 Jan. 2020).
[11] Reim, G. (2018), 'B61-12 nuclear bomb's guided tail kit approved for production', *Flight Global*, 10 December 2018, https://www.flightglobal.com/fixed-wing/b61-12-nuclear-bombs-guided-tail-kit-approved-for-production/130609.article (accessed 17 Dec. 2019).

understanding obtained through discussions with experts and officials in specific contexts (i.e. discussion in events and conferences held under the Chatham House Rule), to increase its accuracy and salience for today's NC3 systems.

This paper will first introduce NATO's C3 structure through the air, land and maritime domains. Second, the paper will introduce NC3, and examine key Ally countries' contribution to NATO's nuclear policy. The paper subsequently examines *known* incidents involving nuclear weapon systems as a means to frame the discussion on the level of risk that NATO and Allies are facing. In conclusion, it will offer a set of recommendations for NATO. The purpose of the paper is to identify, raise awareness of, and help reduce risks to NATO's nuclear weapon systems arising from cybersecurity vulnerabilities. It aims to respond to the need for more public information on cyber risks in NATO's nuclear mission, and to provide policy-driven research to shape and inform nuclear policy at member-state level by demonstrating that the responsibility to protect NATO's systems lies not just with the nuclear weapon states, but with all Allies.

2. Command, Control and Communication in NATO

A C3 system[12] may be broadly defined as the information system that enables the command, control and communications within a given military structure.[13] This chapter will examine command, control and communication, and examine the C3 concept within the framework of NATO, particularly in relation to the Alliance's core domains of operation: air, maritime and land. An understanding of NATO's C3 systems in these domains is conducive to further reflection on the relevance of cybersecurity to their effective functioning.

While the definition and scope of C3 varies from one structure to another, NATO defines the first two elements as follows:

- **Command:** 'The authority vested in an individual of the armed forces for the direction, coordination, and control of military forces.'[14] Planning may not be excluded from this component, given its importance to providing direction, coordination and control, in addition to early warning as well as threat detection and identification systems.

- **Control:** 'The authority exercised by a commander over part of the activities of subordinate organizations, or other organizations not normally under his command, that encompasses the responsibility for implementing orders or directives.'[15]

The US Naval Academy's definition of communications in the context of C3 systems may be used as a reference for the purpose of this paper:

- **Communications:** 'The ability and function of providing the necessary liaison to exercise effective command between tactical or strategic units of command.'[16]

It is also important to note that while in many instances official documents may be exclusively referring to command and control (C2), the latter requires communications to ensure its effectiveness in operations.[17] Communications is critical, and arguably forms one of three 'building

[12] The understanding of C3 within this paper must not be confused with Consultation, Command and Control, as an area covered by NATO's Consultation, Command and Control Board (C3B). 'Consultation' refers to an established system of consulting, communicating, discussing and decision-making focusing on the political processes of consensus decision-making; whereas 'Communication' here must be understood in an operational sense with a military function. See: NATO (2017), 'Consultation, Command and Control Board (C3B)', https://www.nato.int/cps/en/natohq/topics_69279.htm (accessed 12 Sept. 2019).
[13] United States Naval Academy (undated), 'Chapter 20: Command, Control and Communication', *Fundamentals of Navy Weapons Systems*, https://fas.org/man/dod-101/navy/docs/fun/part20.htm (accessed 12 Sept. 2019).
[14] NATO Standardization Office (2018), *AAP-06 NATO Glossary of Terms and Definitions (English and French)*, https://standard.di.mod.bg/pls/mstd/MSTD.blob_upload_download_routines.download_blob?p_id=281&p_table_name=d_ref_documents&p_file_name_column_name=file_name&p_mime_type_column_name=mime_type&p_blob_column_name=contents&p_app_id=600 (accessed 1 Aug. 2019).
[15] Ibid.
[16] United States Naval Academy (undated), 'Chapter 20: Command, Control and Communication'.
[17] C2 and communications are therefore inextricably linked, hence for the purpose of this paper C2 will not be dissociated from the communications dimension.

blocks' of any deterrent strategy; hence it cannot be separated from command and control, as any attack on communications assets would have serious implications on the exercise of C2, and even attacks that are not directly aimed at those communications assets would eventually have the spillover effect of disrupting communications.[18]

The C2 system in place within NATO is designed to support both strategic commands of NATO's Command Structure: Allied Command Operations (ACO) and Allied Command Transformation (ACT).[19] ACO, under the command of the Supreme Allied Commander Europe (SACEUR), is responsible for the planning and execution of all NATO military operations, as directed by the North Atlantic Council. ACT, under the command of Supreme Allied Commander Transformation (SACT), is mandated to spearhead NATO's military transformation; its main areas of responsibility include education, training and exercises, and promoting interoperability throughout the Alliance. Allies provide resources and capabilities to the NATO Command Structure. In military operations – for deploying forces, for instance – NATO's deployable C2 systems are connected through deployable interfaces to those of national systems. In this regard, NATO relies on the Federated Mission Network (FMN) capability to bring national and NATO capabilities together, and to better train, communicate and operate.[20]

A NATO Research Task Group (SAS-085) identified and set out the principles of a successful command and control, capable of effecting, coping with, and/or exploiting changes in circumstances.[21] NATO refers to this capability as 'C2 agility', which may have different approaches depending on the parameters of the mission – including information availability, the level of collaboration, and the decentralization of decisions.[22] The study undertaken by the NATO Research Task Group identifies five approaches based on these three parameters, ranging from one without shared collective objectives, or kinds of interaction between C2 nodes (conflicted C2), to a robustly networked collection of C2 nodes with the broadest possible distribution of decision rights (edge C2).[23] Thus, to ensure effective agility so that Allies may 'switch' approaches at all times, depending on the needs of operations,[24] there is a need for thorough security across all hardware, networks and software used by the Alliance to allow for such agile command and control. For instance, an operation that requires the decentralization of decisions may be rendered ineffective if the parts of the network that are used to communicate and coordinate decisions are tampered with by adversaries: the transmission of information and decisions may be delayed; critical information may be intercepted; and, ultimately, operation success will be hampered. Centralized decisions will

[18] Bracken, P. (2019), 'Communication Disruption Attacks in a Nuclear Context', *DEFENSE.info*, 25 Oct. 2019, https://defense.info/re-shaping-defense-security/2019/10/communication-disruption-attacks-in-a-nuclear-context/ (accessed 24 Jan. 2020).
[19] NATO (2018), 'The NATO Command Structure', https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/1802-Factsheet-NATO-Command-Structure_en.pdf (accessed 1 Aug. 2019).
[20] NATO (2019), 'Federated Mission Networking', https://www.act.nato.int/activities/fmn (accessed 25 Dec. 2019).
[21] NATO Research and Technology Organization (2014), *STO Technical Report: C2 Agility, Task Group SAS-085 Final Report*, http://www.dodccrp.org/sas-085/sas-085_report_final.pdf (accessed 24 Sept. 2019).
[22] Ibid., p. 21.
[23] Development, Concepts and Doctrine Centre (2017), *Joint Concept Note 2/17: Future of Command and Control*, Ministry of Defence, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643245/concepts_uk_future_c2_jcn_2_17.pdf (accessed 24 Sept. 2019).
[24] NATO Research and Technology Organization (2014), *STO Technical Report: C2 Agility, Task Group SAS-085 Final Report*, p. 87.

also require strong resilience in supporting assets, as an attack against those part of the central system may subsequently affect the wider ecosystem of C2 assets. In some situations, decentralization of decisions may benefit the Alliance, as this may force the adversary to execute simultaneous attacks upon the decentralized network.

NATO relies on tactical data links (TDL) as part of its command, control, communication, computers, intelligence, surveillance and reconnaissance (C4ISR) systems. TDL provides information transmission in near-real time and simultaneously across NATO platforms, such as space, ground, air and surface platforms. It allows users to transmit and receive encrypted data, and can differentiate between 'friendly' data and data received from adversarial systems. It is an important component of the Joint Intelligence Surveillance and Reconnaissance (JISR) capability, critical for early warning, operations planning, situational awareness and target information.[25] TDL is used in a number of applications, including air, land, surface, subsurface and space surveillance, electronic warfare sensors, weapon coordination, air control, navigation and network management.[26] The loss of TDL due to physical or cyber intrusion may subsequently have high mission impact and jeopardize its success.

The following elements supporting NATO's operations in three of its 'physical' domains of operation – air, land and maritime – provide an overview of elements constituting NATO's C3 system.

Air domain

For peacetime tasks and as part of NATO integrated air and missile defence (NIAMD), air C2 and ballistic missile defence fall under the responsibility of the Commander Allied Air Command. In crisis response operations, SACEUR will appoint a Joint Force Air Component Commander (COM JFAC) to conduct air C2 specifically for a designated operation.[27]

Air C2 systems enable the management of all types of air operations over NATO Allies territory and beyond, ranging from air traffic control and airspace management to surveillance and force management, including refuelling.[28] These systems integrate, *inter alia*, surveillance, air mission control and force management functions. The implementation of air C2 systems also entails the activation of 'a number of deployable control and reporting centres […] with integrated deployable sensors'.[29] The extent to which this applies in space (which it should be noted is beyond the scope of

[25] Stoica A., Militaru, D., Moldoveanu, D. and Popa, A. (2016), 'Tactical Data Link—From Link 1 to Link 22', *"Mircea cel Batran" Naval Academy Scientific Bulletin*, XIX(2), https://www.anmb.ro/buletinstiintific/buletine/2016_Issue2/MES/317-322.pdf (accessed 25 Dec. 2019).
[26] Ibid., pp. 318–319.
[27] NIAMD uses the NATO Integrated Air and Missile Defence System (NATINAMDS), which consists of 'a network of interconnected national and NATO systems comprised of sensors, command and control facilities and weapons systems'. See NATO (2019), 'NATO Integrated Air and Missile Defence', 15 April 2019, https://www.nato.int/cps/en/natohq/topics_8206.htm (accessed 10 Jul. 2020); and NATO (2016), *Allied Joint Doctrine for Air and Space Operations*, NATO Standardization Office, pp. 2-1 and 2-3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/624137/doctrine_nato_air_space_ops_ajp_3_3.pdf (accessed 16 Sept. 2019).
[28] Ibid.
[29] Ibid., pp. 2–3.

this paper) may potentially evolve, given that NATO only recently recognized space as a discrete domain of operations.[30]

In the air domain, threat analysis generated through air-based defence systems provides situational awareness in airspace. This information feeds into the Combat Reporting Centre, which is then reported up to the senior level. Depending on the issue area, senior cadre decides on the necessary response, such as tasking an Ally aircraft to undertake an action. This process forms NIAMD. NIAMD can pull together air, land and maritime threats, to provide timely and robust information to the Alliance in peacetime as well as in crisis and conflict. Currently, NIAMD's mission involves observing Alliance airspace for threats and defending the Alliance against ballistic missile threats. Securing NIAMD from cyberattacks at a time of conflict would be mission-critical to preserving NATO's situational awareness.[31]

Effective, robust and reliable communication systems are critical to allowing 'effective liaison' at all times – i.e. the communication system needs to survive in crisis situations – which has been defined as a 'key factor in the success of joint operations'.[32] The 2016 Allied Joint Doctrine for Air and Space Operations attests to the need for effective liaison between forces for coordinated operations, with the air operational liaison reconnaissance team, with the on-site personal representative, and between the various joint boards and working groups that take part in decision-making processes. This also implies the need to protect the 'hardware' assets underpinning C3 systems such as radars, sensors and communications assets, including those based in space, without which effective liaison, coordination and implementation of C2 would not be possible.[33]

NATO capabilities have been undergoing significant transformation. This includes integrating different types of theatre ballistic missile defence systems (BMDS) provided by key NATO Allies, including Italy, Germany France, the UK and the US, into a single network, while providing layered protection against ballistic missile attacks.[34] For instance, as part of the Active Layered Theatre Ballistic Missile Defence (ALTBMD) programme, NATO is replacing its existing C2 systems in Europe, setting 'new standards of interoperability for air operations'.[35] Through interoperability, NATO is connecting Ally forces and increasing their readiness and effectiveness for NATO missions and operations. Interoperability, however, brings with it cybersecurity challenges.

Interoperability of forces to conduct joint operations is only possible when Allies rely on 'friendly' capabilities. For instance, the disagreement over Turkey's purchase of Russian S-400 air missile defence system (discussed in fuller detail in Appendix II) is causing great concern within the Alliance. Some of the concerns raised in this regard include the lack of interoperability between the

[30] NATO (2019), 'Foreign Ministers take decisions to adapt NATO, recognize space as an operational domain', 20 November 2019, https://www.nato.int/cps/en/natohq/news_171028.htm#:~:text=NATO%20Foreign%20Ministers%20met%20in,of%20NATO%20leaders%20in%20London.&text=They%20agreed%20to%20recognize%20space,%2C%20land%2C%20sea%20and%20cyber (accessed 25 Dec. 2019).
[31] NATO (2019), 'NATO Integrated Air and Missile Defence', https://www.nato.int/cps/en/natohq/topics_8206.htm (accessed 18Dec. 2019).
[32] Ibid.
[33] See Unal (2019), *Cybersecurity of NATO's Space-based Strategic Assets*.
[34] NATO (2005), 'Launch of NATO's Active Layered Theatre Ballistic Missile Defence (ALTBMD)', https://www.nato.int/cps/en/natolive/news_21656.htm (accessed 25 Dec. 2019).
[35] Ibid.

S-400 system and the US's F-35 programme of which Turkey had been part. Another concern relates to the possibility of providing the vendor country (in this case Russia) with the ability to collect sensitive information about Ally forces if NATO's TDL system is integrated with the system being purchased. TDL in the air domain shares near real-time information with air, land and maritime forces, meaning that, at a time of conflict, an adversary (or adversaries) in possession of such sensitive information could have tremendous advantage over NATO Allies, with the potential to considerably jeopardize mission success.

Considering that weapon systems *may* have cybersecurity vulnerabilities from the design stage, it would only be the manufacturing company and the vendor (state) that would be fully aware of the system's design features and potential vulnerabilities. NATO's and the US's concern to protect Alliance systems is critical; yet there has not been much discussion in the public domain of the cybersecurity aspect of the S-400 purchase.

The purchase of Russian or Chinese defence equipment by NATO Allies has long been an issue of concern for the Alliance. In 2013, for instance, Turkey indicated its intention to purchase a Chinese missile defence system, although it later reversed this decision when it became apparent that China would not transfer the technological details of the system, including the full specification and design. And there are three countries within NATO – Bulgaria, Greece and Slovakia – that purchased Russian S-300 missile defence systems back in the 1990s. One of the logical ways to resolve the S-400 predicament, therefore, is the establishment of stronger procurement baselines and standardization agreements (STANAGs) for NATO that integrate cybersecurity measures and the examination of potential cyber vulnerabilities. Considering that nuclear forces and conventional forces are intertwined in the C2 structure, it is vital to understand the full range of possible risks posed by the S-400 – including for all integrated C3, nuclear planning and nuclear systems. This also means that the Alliance always needs close oversight of the state of health of hardware, firmware and the software in order to ensure that NATO forces are securely connected in times of crisis.

Land domain

NATO Allied Land Command (LANDCOM) is responsible for coordinating and synchronizing NATO and partner land forces, and deploys, on order, headquarter elements to provide planning, coordination and C2 capabilities to Allied forces.[36]

The 2016 NATO Command and Control of Allied Land Forces document is referenced in the Allied Joint Doctrine for Land Operations to provide the doctrine applicable to the C2 of NATO land forces, including decision-making and targeting processes, organizational structure, duties and responsibilities.[37] It has been described as supporting the Allied Joint Doctrine for Land Operations published in March 2016.[38] The latter provides overall guidance on the principles needed to plan

[36] NATO Allied Command (undated), 'Mission', https://lc.nato.int/about-us/mission (accessed 16 Sept. 2019).
[37] NATO (2016), *Allied Joint Doctrine for Land Operations, NATO Standard, AJP-3.2, Edition A, Version 1*; NATO (2016), 'ATP-3.2.2, Command and Control of Allied Land Forces'.
[38] NATO (2016), *Allied Joint Doctrine for Land Operations, NATO Standard, AJP-3.2, Edition A, Version 1*.

and conduct land operations within the framework of NATO, and is complemented by both the NATO C2 of Allied Land Forces (ATP-3.2.12) and Land Tactics (ATP-3.2.1) documents.[39]

The NATO Communication and Information Agency (NCI Agency) has been leading the acquisition and support processes for NATO's new Land C2 Information System (LC2IS), a software designed to support the planning, execution and the assessment of land-heavy operations. The software's functions include: 'to enable and improve the effective C2 of NATO Land Forces; support NATO commanders in their-decision making process; and improve information exchange'. LC2IS has also been stated to enable improved interoperability with national systems, and, as part of several testing rounds, underwent an interoperability test with the national systems of the Netherlands and the US.[40]

In addition to the need for close oversight of all assets, as previously stated, interoperability with national systems also implies the need for a degree of technical harmonization between Alliance and national systems. Their respective encryption standards and settings must allow straightforward and effective interoperability when the need arises, while also ensuring that they maintain the highest encryption and authentication standards possible to secure the C3 systems.

Maritime domain

The Allied Maritime Command (MARCOM) constitutes the central command of all NATO maritime forces, and is responsible for all maritime matters within NATO's remit.[41] In particular, it is responsible for the planning and command of maritime operations, and of major maritime and joint exercises. In addition, Naval Striking and Support Forces (STRIKFORNATO) is mandated to deliver, on order, a deployable and scalable headquarters to plan and execute joint maritime operations and provide the C2 of maritime ballistic missile defence.[42]

The maritime domain is not a single-flag task force. It is always a joint task, and requires robust communication channels across allied forces. In peacetime, maritime capabilities are on standby on a continuous basis. NATO Maritime Interdiction Operational Training Centre (NMIOTC), in Crete (Greece), is a Centre of Excellence that supports maritime operations through training in Ally and partner countries. It examines cybersecurity in order to manage risks pertaining to the maritime sector.

The maritime domain relies on both ground and space capabilities, such as satellite communications and radio frequencies. Moreover, systems that ships rely on go through digitalization and automation processes,[43] both of which present challenges to cybersecurity. Maritime unmanned systems, for instance require autonomous and remotely operated equipment,

[39] Ibid, p. XI.
[40] NATO (2017), 'NATO Land Command and Control Information Service – Version 6.0 passes a major Milestone', https://www.ncia.nato.int/about-us/newsroom/nato-land-command-and-control-information-service-e28093-version-60-passes-a-major-milestone.html (accessed 5 Nov. 2019).
[41] Allied Maritime Command (undated), 'Mission', https://mc.nato.int/about-marcom/mission-.aspx (accessed 16 Sept. 2019).
[42] Naval Striking and Support Forces (undated), 'Mission Statement', https://sfn.nato.int/missionstatement.aspx (accessed 16 Sept. 2019).
[43] Tiele, D. R. (2018), *Game Changer — Cyber Security in the Naval Domain*, ISPSW Strategy Series No: 530.

including Global Positioning System (GPS) receivers. With advanced networking, despite all efforts of segmentation, maritime unmanned systems are reported to be 'frequently connected to the internet'.[44] Moreover, ships rely on position, navigation and timing (PNT) characteristics, with specific GPS application, that are subject to cyber intrusions.

Compared with the land and air domain capabilities (e.g. aircraft, ground-based missile platforms, etc.), the submarine environment may have an advantage in that its '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'.[45] This does not, however, mean that submarines are immune to cyberattacks. Contrary to common belief, submarines can be vulnerable to data corruption and malware injection, among others, especially when they are undergoing maintenance.

In order to coordinate activities among Allied forces in the maritime domain, NATO relies on the Link 22 network. Link 22 is a NATO-wide, secure, beyond line of sight (BLOS)[46] TDL. Prior to Link 22, NATO used Link 11 (also known as TADIL A), to exchange near real-time information across the Alliance. The range of problems reported with Link 11 includes: delays in processing and receiving information (due to roll-call transmission characteristics); crypto-technology not meeting modern processing requirements (encryption problems); security vulnerabilities in the system bringing the possibility of spoofing; and the use of single fixed-frequency network (either high frequency or ultra-high frequency) leading to potential jamming.[47] By switching to Link 22, NATO provided time-based encryption,[48] resulting in improved cybersecurity of data. However, secure architecture and inherent design can only protect military systems to a certain point. Technological advances, specifically those in cyber technology, will continue to challenge new systems, eventually exposing previously unknown weaknesses in their design.

In addition, MARCOM and Supreme Headquarters Allied Powers Europe (SHAPE) have been developing a NATO Joint Maritime Deployable C2 Capability, for which the C2 Centre of Excellence is providing expertise and recommendations.[49] This capability would enable the use of other physical platforms, such as landing platform docks, ships taken up from trade, and landing platform helicopters, other than a command ship as a mobile, afloat command platform to conduct operations, including C3, at sea. This is particularly important for the decentralized conduct of operations and creating resilience in maritime C2 systems.

[44] Ibid., p. 3.
[45] Abaimov, S. and Ingram, P. (2017), *Hacking UK Trident: A Growing Threat*, BASIC, https://basicint.org/wp-content/uploads/2018/06/HACKING_UK_TRIDENT.pdf (accessed 19 Dec. 2019).
[46] Beyond line of sight (BLOS) allows to communicate that are apart from each other and when there is no clear line of sight.
[47] Northrop Grumman (2014), *Understanding Voice and Data Link Networking: Northrop Grumman's Guide to Secure Tactical Data Links*, San Diego: Northrop Grumman, pp. 4–36, https://www.northropgrumman.com/Capabilities/DataLinkProcessingAndManagement/Documents/Understanding_Voice+Data_Link_Networking.pdf (accessed 25 Dec. 2019).
[48] Time-based encryption requires the receiver to have a time instant key or a code to decrypt and recover the message. For more information, see Paterson, K. G. and Quaglia, E. A. (2010), *Time-Specific Encryption*, Information Security Group, Royal Holloway, University of London, http://www.isg.rhul.ac.uk/~kp/tse.pdf (accessed 19 Dec. 2019).
[49] NATO Command and Control Centre of Excellence (undated), 'NATO Maritime Deployable C2 Capability', http://web.archive.org/web/20180902194743/https:/c2coe.org/knowledge-development/nato-maritime-deployable-c2-capability/ (accessed 15 Jun. 2020).

3. Nuclear Command, Control and Communication

NC3 systems refers to the information systems supporting the exercise of command and control, as well as the communications between units of command in military operations involving the planning and use of nuclear weapons.

The US is the only NATO member to have earmarked nuclear weapons (B61 gravity bombs) for the purpose of nuclear sharing in the context of NATO, and has stationed nuclear weapons in Belgium, Germany, Italy, the Netherlands and Turkey as part of nuclear burden sharing (see Appendix II). It is therefore inevitable that the NC3 system in place within NATO is inextricably linked to the US's own NC3 system, which will be further outlined in detail below. The UK and France have independent nuclear weapon systems, addressed in Appendix I of this paper.

The protection of C3 systems requires the adoption of adequate, adaptable and robust cybersecurity measures to ensure their integrity and shield them from internal and external disruption. Cybersecurity measures are critical to ensuring the survivability, integrity and resilience of C3 systems. NATO has indeed designated cyberspace as a domain of operation since 2016, which attests to its importance in military operations.[50]

It should be noted that there is disagreement among some experts regarding the actual *extent* of cyberthreats against C3 assets, in particular those for nuclear operations. NC3 assets are, however, in themselves complex, and are part of a wider – itself more complex – 'ecosystem' of networks, software and hardware making up the entire NC3 system. Offensive cyber capabilities are without doubt highly sophisticated at present, and such capabilities are in the hands of a small number of actors. In other words, cyberthreats need to be tailored to the targeted assets along with the NC3 ecosystem of which they are part, which may be difficult given the secrecy surrounding the technical information and specifications of these systems. This, then, could result in scepticism regarding the actual *feasibility* of conducting any cyber operations at all against NC3 assets: unless adversaries issuing such threats display credibility and trigger actual fear, targeted states will not fully grasp the level of risk such cyberthreats may pose to the NC3 systems. The preparation, conduct and operationalization of cyberattacks against systems as complex as NC3 would require not only a tremendous amount of financial, technical and human resources, but also a great deal of time – which may be further extended if any of the targeted system's configurations are modified, requiring the malware to be 'updated' accordingly. The development of such offensive cyber means would require a high level of expertise and knowledge to:

- Map out the NC3 system;
- Understand the interaction and dependency between networked assets;

[50] NATO (2016), 'Warsaw Summit Communiqué', 9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed 28 May 2019).

- Identify potential vulnerabilities, entry points and additional layers of security;
- Disable potential redundancies; and
- Develop an accurate, effective malicious programme that would require testing before eventually being implanted to infect the NC3 ecosystem.

NATO cybersecurity practices across domains

In order to protect its C3 systems from cyber operations, NATO has put in place key measures, including Federate Mission Networking (FMN). Defined as a 'capability aiming to support command and control and decision-making in future operations through improved information-sharing',[51] FMN's architecture is framed so as to achieve interoperability between Allies and partner countries with capabilities ranging from messaging services to security services.[52] FMN is built on lessons learned from the development, implementation and evolution of the Afghanistan Mission Network (AMN),[53] a NATO-sustained initiative to create a common network from a collection of national and NATO networks.[54] It has provided NATO with a coalition-wide network that has enabled greater situational awareness and facilitated better decision-making. FMN aims to go beyond mission-based networks and provide a ready mechanism that can support any training, exercise or operation NATO might undertake in the future.[55] There are several FMN elements that are significant for achieving cybersecurity within Ally and partner capabilities: FMN rests on a governance model with rules, procedures, policies and standards, and it gives direction to NATO Allies and partners. Its baseline requirements also involve cyber and information security measures. Within the FMN management group, there are several working groups, including on capability planning, and on interoperability, assurance and validation. By allocating their capabilities to FMN, NATO Allies and partner countries confirm that their communication and information systems comply with NATO's security and interoperability principles and standards.[56]

As agreed at its 2010 Lisbon Summit, NATO has been investing in a ballistic missile defence capability for collective defence purposes. As part of the burden sharing principle, members have agreed to expand the Active Layered Theatre Ballistic Missile Defence (ALTBMD) Capability.[57] As a result, Turkey hosts a forward-based early warning radar in the context of NATO's ballistic missile

[51] NATO (2015), 'Federated Mission Networking', https://www.act.nato.int/activities/fmn (accessed 14 Feb. 2020).
[52] Brannsten, M. R., Johnsen, F. T., Bloebaum, T. H. and Lund, K. (2015), 'Toward federated mission networking in the tactical domain', *IEEE*, 53(10), doi: 10.1109/MCOM.2015.7295463 (accessed 1 Aug. 2019).
[53] United States Chairman of the Joint Chiefs of Staff Instruction (2016), *Mission Partner Environment Executive Steering Commmittee; Coalition Interoperability Assurance and Validation Working Group*, Directive Current as of 27 March 2019, CJCSI 5128.02, 10 November 2016, p. A-1, https://www.jcs.mil/LinkClick.aspx?fileticket=RSW4RZfZlWc%3D&tabid=19767&portalid=36&mid=46626 (accessed 25 Dec. 2019).
[54] Serena, C. C. et al. (2014), *Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network*, RAND Corporation, https://www.rand.org/pubs/research_reports/RR302.html (accessed 1 Aug. 2019).
[55] NATO (2015), *The Secretary-General's Annual Report 2014*, NATO, https://www.nato.int/cps/en/natohq/opinions_116854.htm (accessed 1 Aug. 2019).
[56] NATO (2017), *Allied Joint Doctrine for Communication and Information Systems*, NATO Standard, AJP-6, Edition A, Version 1.
[57] NATO (2012), 'Chicago Summit Declaration', https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en (accessed 24 Sept. 2019).

defence capability,[58] and Romania hosts the Aegis Ashore ballistic missile defence system (BMDS).[59]

Even though deployed systems may be secured from cyberattacks, the servers and facilities of a host country may be vulnerable. A 2018 report by the US Department of Defense's Inspector General found that there were specific vulnerabilities and weaknesses that could be exploited by security-cleared contractors, government officials or outside parties.[60] These weaknesses included: not implementing multifactor authentication to access technical information at specific locations; not encrypting BMDS technical information during transmission (although the report redacts where this technical information was transmitted between); and not introducing intrusion detection techniques on classified networks. The report found that: 'The disclosure of technical details could allow U.S. adversaries to circumvent BMDS capabilities, leaving the United States vulnerable to deadly missile attacks.'[61] Such disclosure would have an impact beyond the US, and would affect NATO Allies at large, as these capabilities also form part of the Alliance's overall missile defence capabilities.

Systems are only one component of what C3 constitutes. C3 capability as a whole is developed through establishing doctrine, operation, training, materiel, leadership, personnel, facilities and interoperability. C3 training is provided in NATO schools, such as in Oberammergau, Germany.

Assurance is also part of the process to ensure that capabilities developed are fit for cybersecurity baselines. Testing and retesting, as well as redundancy measures, are conducted throughout the development and design stages of C3 capabilities.

NATO has layers of security in place to prevent malicious access to C3 systems. There are barriers of entry, such as restricted access to critical systems. In the case of cyberspace, every element has a physical point of connection (e.g. critical national infrastructure, weapon systems). The security of these physical points rests with each member nation. There are national regulations to ensure cybersecurity measures are in place, and NATO can also issue additional requirements to its members. For instance, there are telecommunications requirements to support national disaster emergency response. However, the implementation of these requirements rests with each nation. Responsible state behaviour should accompany any baselines and standards in this area.

That NATO and its Allies recognize the importance of cybersecurity is reflected in various unclassified documents and statements in all domains of operation.[62] The following five themes are identified as relevant to NATO and Allies' C3 systems to ensure their cyber resilience:

[58] Ibid.
[59] NATO (2019), 'Aegis Ashore ballistic missile defence system in Romania completes scheduled update', 9 August 2019, https://www.nato.int/cps/en/natohq/news_168377.htm (accessed 19 Dec. 2019).
[60] The publicly available report is redacted. See Inspector General, U.S. Department of Defense (2018), *(U) Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information*, https://media.defense.gov/2018/Dec/14/2002072642/-1/-1/1/DODIG-2019-034.PDF (accessed 28 May 2019).
[61] Ibid.
[62] Although NATO has also recognized the cyber domain as a domain of operation in and of itself, it is important to emphasize that cybersecurity must be considered across all domains and not exclusively in the cyber domain (thus including air, land and the maritime domain).

- Software and network protection
- Data (integrity) protection
- Hardware protection
- Access/security controls
- Cybersecurity awareness/security by design

It is important to emphasize that these themes are not mutually exclusive, and that a critical node relevant to one may be equally relevant to others; hence, there may be coupling in systems. In other words, a cyber operation could affect C3 systems in more than one way. In 2011, for instance, malware reportedly infected the cockpits of the US's Predator and Reaper drones,[63] logging every keystroke made by pilots as they remotely flew missions over Afghanistan and other areas of operation.[64] While, in this example, the protection of the cockpits' network and software was jeopardized, so too was the integrity of the data (i.e. the pilots' keystrokes). Unauthorized access and the obtaining of logged keystrokes could provide adversaries with data that would reveal usage patterns that could subsequently be used in their own operations to counter or avoid the drones, and/or eventually sell or otherwise distribute these data to third parties – including non-state armed groups. Furthermore, the interception of these data could also reveal how the piloting system (e.g. the software used to pilot the drones) works. This information may be used by an adversary to develop malware and other means to potentially disrupt and/or disable the piloting software – and ultimately bring about mission failure.

Furthermore, a cyber incident may affect more than one domain at the same time. For instance, in early 2009 the French navy's computer systems and internal network were reported to have been infected by a malware (Conficker virus) as a result of failure to install Microsoft updates.[65] Starting from the navy's internal network (Intramar) on 12 January, the virus reportedly spread and affected logistics and communication exchanges. Claims that the virus also affected aircraft on the ground, which were unable to download flight plans as the virus also affected databases, were denied by the French defence ministry.[66] In general, this example demonstrates that cyber incidents could potentially create a domino effect, affecting more than one domain simultaneously.

The five recurring cybersecurity themes that are relevant to ensuring the resilience of NATO's C3 systems are examined in greater depth below. It is important to highlight that these principles have

[63] Predator and Reaper drones currently in service are used for intelligence, surveillance, target acquisition and reconnaissance (ISTAR) and attack missions. Both aircraft are armed and remotely controlled by an operational crew via satellite communication. See Royal Air Force (2019), 'MQ-9A Reaper', https://www.raf.mod.uk/aircraft/mq-9a-reaper/ (accessed 1 Aug. 2019) and Air Force Technology, 'Predator RQ-1/MQ-1/MQ/9 Reaper UAV', https://www.airforce-technology.com/projects/predator-uav/ (accessed 1 Aug. 2019).
[64] Schachtman, N. (2011), 'Exclusive: Computer Virus Hits U.S. Drone Fleet', *WIRED*, 7 October 2011, https://www.wired.com/2011/10/virus-hits-drone-fleet/ (accessed 28 May 2019).
[65] Willsher, K. (2009), 'French fighter planes grounded by computer virus', *The Telegraph*, https://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html (accessed 22 Dec. 2019).
[66] Merchet, J. (2009), 'Les armées attaquées par un virus informatique (actualisé)', *Libération*, 5 February 2009, http://secretdefense.blogs.liberation.fr/2009/02/05/les-armes-attaq/ (accessed 28 May 2019).

been identified by the authors through the study of official NATO documents on the subject, and that they do not represent acknowledged NATO policy.

Theme 1: software and network protection

Protection of software and networks covers the intangible dimension of C3 systems, and includes networks connecting computers and information systems to one another; networks connecting command and control systems to weapons systems; data processing software; and software as operations enablers (e.g. navigation software).[67]

Interference with communications networks could heavily disrupt control over weapons systems, and ultimately over operations and safety. Safeguarding networks is equally important in peacetime, as breaches could potentially result in misinterpretation, miscalculations and rapid inadvertent escalation. For instance, early in the morning of 23 October 2010, the US reportedly lost communication with 50 of its Minuteman III intercontinental ballistic missiles:[68] computer screens at the Francis E. Warren Air Force Base underground launch control centres displayed the message Launch Facility Down (LFDN). While the cause of this incident was attributed to hardware issues[69] (reports suggest that a circuit card had been dislodged by routine vibration and heat),[70] this example stresses the importance of preserving the integrity of communications networks for monitoring purposes at all times. In a situation where political tensions are high, such incidents could potentially result in inadequate responses that may rapidly escalate the situation to an armed conflict – even nuclear – unless states have clear guidelines and procedures that allow them to detect and identify the nature of such incidents, and thus prevent the risk of unnecessary escalation due to misinterpretation/misunderstanding.

More recently, among the findings of the annual report for 2018 of the US Director, Operational Test and Evaluation was that there were survivability and cybersecurity shortfalls in the Patriot Post Deployment Build (PDB)-8 IOT&E, part of the Patriot missile defence system[71] of the US Army.[72] These shortfalls could provide an opportunity for adversaries to disrupt operations, or even tests, involving the Patriot system, thus weakening air and missile defence systems.

[67] How to ensure the protection of software and networks is another question that touches beyond the scope of this paper. For example, it has been argued that 'complexity is the enemy of security': see Grosse, E. (2019), *Security at Extreme Scales*, Technology for Global Security Special Report, https://www.tech4gs.org/uploads/1/1/1/5/111521085/security_at_extreme_scales_2019_grosse_4.pdf (accessed 31 Jan. 2020).
[68] Schlosser, E. (2013), 'Neglecting our nukes', *POLITICO*, 16 September 2013, https://www.politico.com/story/2013/09/neglecting-our-nukes-096854 (accessed 10 Jun. 2019).
[69] Shachtman, N. (2010), 'Communication ICBM SNAFU', *WIRED*, 26 October 2010, https://www.wired.com/2010/10/communications-dropped-to-50-nuke-missiles-in-icbm with 50 nuke missiles dropped in -snafu/ (accessed 20 Jun. 2019).
[70] Schlosser (2013), 'Neglecting our nukes'.
[71] The Patriot is a surface-to-air defence system designed 'to counter tactical ballistic missiles, cruise missiles and advanced aircraft'. See Army Technology, 'Patriot Missile Long-Range Air-Defence System', https://www.army-technology.com/projects/patriot/ (accessed 1 Aug. 2019).
[72] Director, Operational Test and Evaluation (2018), *FY 2018 Annual Report*, https://www.dote.osd.mil/Publications/Annual-Reports/2018-Annual-Report/ (accessed 10 Jun. 2019).

Some NATO documents indicate the need for software and network protection.[73] For instance, the Allied Joint Doctrine for Air and Space Operations identifies joint intelligence, surveillance and reconnaissance (ISR) as an integrated intelligence and operations set of capabilities 'which synchronizes and integrates the planning and operations of all collection capabilities with processing, exploitation, and dissemination of the resulting information in direct support of planning, preparation, and execution of operations'.[74] Air and space-based ISR assets in particular play a critical role in building early understanding of potential crisis points and thus enhance the quality of political and high-level military decision-making, as well as in both conventional and nuclear weaponry command and control. ISR assets include airborne imagery platforms, satellites and ground sensors. Compromised ISR missions could affect NATO in many ways, including faulty assessment and response to threats; inability to transmit ISR information over potential adversaries' territory; loss of situational awareness; loss of battlefield awareness, thereby jeopardizing the desired operational objective; and crippling of defensive systems. These vulnerabilities underscore the critical nature of software and network protection.[75]

Such incidents may not only result in the disruption, or potentially even the failure, of missions. They could also jeopardize the credibility of the state's nuclear forces and, ultimately, undermine their ability to deter. Allies need to take such vulnerabilities into account, exercise caution and conduct internal audits to identify and address cyber vulnerabilities – both existing in weapons systems in service and in weapons systems under development across the entirety of the contractors' and sub-contractors' supply chain.

Theme 2: data (integrity) protection

Data protection has two dimensions: the protection of data from theft/unauthorized access; and the protection of the data's integrity. Both are of equal importance and relevance to NATO's C3 systems from a cybersecurity perspective, as they could equally affect the success of operations. For instance, NATO's Allied Joint Doctrine for Land Operations states that land operations will seek to profit from cyber activity that can damage, defend, exploit and attack computers, as well as any data held on them.[76] The document recognizes the importance of data and the value of affecting the adversary's data – thus also recognizing the importance of protecting NATO's own data. In this context, NCI Agency's Network Services and IT Infrastructure Service Line facilitates the 'enabling of secure and resilient data, voice and video communication services worldwide', so as to 'connect

[73] Some of the documents that cover software and network protection include: NATO (2018), *Joint Air Power Strategy*, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180626_20180626-joint-air-power-strategy.pdf (accessed 28 May 2019); NATO Standardization Office (2016), *NATO Standards AJP 3.3, Allied Joint Doctrine for Air and Space Operations*, Edition B Version 1, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/624137/doctrine_nato_air_space_ops_ajp_3_3.pdf (accessed 28 May 2019); NATO Standardization Office (2016), *NATO Standards AJP-3.2, Allied Joint Doctrine for Land Operations*, Edition A Version 1, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/624149/doctrine_nato_land_ops_ajp_3_2.pdf (accessed 1 Aug. 2019); and NATO (2010), *Active Engagement, Modern Defence: Strategic Concept For the Defence and Security of the Members of the North Atlantic Treaty Organization*, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf (accessed 20 Jun. 2019).
[74] NATO (2016), *Allied Joint Doctrine for Air and Space Operations*, NATO Standardization Office, pp. 1–15.
[75] Unal (2019), *Cybersecurity of NATO's Space-based Strategic Assets*.
[76] NATO Standardization Office (2016), *NATO Standards AJP-3.2, Allied Joint Doctrine for Land Operations*, p. 1–23.

the dots in space, cyberspace, air, land and maritime'.[77] Data security also plays an important role for instance when conducting image analysis for targeting purposes.

Protection of data from theft/unauthorized access

Commonly referred to as espionage, unauthorized access to data/information could present an opportunity for adversaries to understand the technical specifications of NC3 systems or learn stealth characteristics of nuclear-capable aircraft, which in turn could provide an opportunity for them to exploit this knowledge to interfere with these systems. While espionage in itself is not a new phenomenon, malicious actors are now able to access and steal a greater amount of data using increasingly sophisticated means, and they can potentially exploit these data through modelling and simulation techniques in order to gain advantage over NATO.

In December 2018 the US District Court, Southern District of New York (*USA v Zhu Hua, Zhang Shilong*) sealed an indictment against two members of a hacking group operating in China known as Advanced Persistent Threat 10 (APT10 Group).[78] The APT10 Group was stated to have harnessed over 40 computers in order to steal confidential data from those systems belonging to the US Department of the Navy, including the personally identifiable information of more than 100,000 Navy personnel.[79] In addition, the group 'obtained unauthorized access to at least approximately 90 computers belonging to commercial and defence technologies companies and US Government agencies and stole hundreds of gigabytes of sensitive data and information from their computer systems'.[80] Targets included seven companies involved in aviation, space and/or satellite technology, and three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments (one company involved in maritime technology; the NASA Goddard Space Center; the NASA Jet Propulsion Laboratory). The group also 'successfully obtained unauthorized access to computers belonging to at least 25 other technology-related companies involved in, among other things, information technology services, radar technology, and computer processor technology'.[81]

This example demonstrates that unauthorized access to data and data theft could have multiple implications for command, control and communications at various stages and in all domains of combat:

- Unauthorized access to personally identifiable information of personnel could provide opportunities for social engineering[82] and subsequent gathering of confidential, critical information directly from the individual targets, or from the contamination of computer systems

[77] NATO Communications and Information Agency (undated), 'NATO's Consultation and Command Networks', https://www.ncia.nato.int/Our-Work/Pages/Network-Services-and-IT-Infrastructure.aspx (accessed 10 May 2019).
[78] United States District Court Southern District of New York (2018), *United States of America v. Zhu Hua, Zhang Shilong,* https://www.justice.gov/opa/press-release/file/1121706/download (accessed 10 Jun. 2019).
[79] Ibid.
[80] Ibid.
[81] Ibid.
[82] Social engineering here must be understood as an act to influence one for the victim to act in a certain manner through technological means, such as phishing or baiting. This can lead to the obtention of information, or even the contamination of computer systems unbeknownst to the victim. For examples of definition, see Kaspersky (2019), 'Social Engineering – Definition', https://www.kaspersky.co.uk/resource-center/definitions/what-is-social-engineering (accessed 21 Jun. 2019); Norton by Symantec (2019), 'What is social engineering? Tips to help avoid becoming a victim', https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html (accessed 21 Jun. 2019).

and networks as a result of the victim's actions. In other words, members of the APT10 Group could use stolen identifiable information to reach Navy personnel, manipulate the target or use the target as a disguise, masquerade as an authorized entity to gain access to the Navy's C3 systems by using the targeted personnel's credentials, or by exploiting hardware, software and network vulnerabilities, critical to the nuclear systems.

- Unauthorized access to sensitive information related to warfare/defence technologies and electronic systems developed by private contractors – such as sensors, radars or information processing systems – could provide an opportunity to reverse-engineer these systems, thereby causing wider disruption.

- Access to such technical information could also provide an opportunity for an adversary to study and reverse-engineer the data, identify technical specificities and eventual vulnerabilities and shortfalls, and develop capabilities much more sophisticated than the original ones. These concerns are not new; however, the way adversaries could obtain these technical data is (e.g. through access to the targeted information). These data could also be stolen and sold – as was the case with sensitive documents related to the US MQ-9 Reaper drone and M1 Abrams tank advertised for sale on a dark web forum in 2018.[83]

Protection of integrity of data

This aspect of data protection refers to protection from any external, unwanted interference that could negatively affect decision-making and operations. This is particularly important in the context of the increasing use of artificial intelligence (AI) and machine learning, which depend heavily on the quantity and quality of input data. All aspects of C3 could potentially benefit from automation to collect and process a larger pool of data to feed into sophisticated training and simulation tools, data analyses, situational awareness, decision-making, control and monitoring processes as well as feedback mechanisms. Sensors and powerful computer processors are critical components, as is the quantity and quality of data fed into the machines at the development and training stages as well as in their actual use. The pool of data collected and used may be susceptible to data poisoning attacks, which would in turn corrupt the learning model[84] and, subsequently, the results used to underpin C3. The US's 2018 Nuclear Posture Review[85] recognizes data integrity as part of a resilient NC3 network. Although AI and machine learning do not currently form part of the nuclear launch decision-making process, they have been considered and slowly integrated into the other parts of the military decision-making processes.[86]

[83] Burgess, M. (2018), 'A dumb security flaw let a hacker download US drone secrets', *WIRED*, 11 July 2018), https://www.wired.co.uk/article/router-hacking-drone-reaper-military-secrets (accessed 28 May 2019).
[84] Steinhardt, J., Pang Wei, K. and Liang, P. (2017), 'Certified Defenses for Data Poisoning Attacks', 31st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA, http://papers.nips.cc/paper/6943-certified-defenses-for-data-poisoning-attacks (accessed 1 Aug. 2019).
[85] Office of the Secretary of Defense (2018), *Nuclear Posture Review*, p. 56, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF (accessed 10 Oct. 2019).
[86] For a discussion on AI and nuclear risks, see Boulanin, V. (2019), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume 1: Euro-Atlantic Perspectives*, Solna: Stockholm International Peace Research Institute, https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf (accessed 8 Jun. 2020).

Theme 3: hardware

The third relevant theme in the protection of NATO's C3 systems is the protection of hardware/assets. The protection of the tangible components of these systems is equally important as software protection, and critical in preserving the C3 systems currently in place. Hardware may range from sensors for surveillance and tracking to cables supporting communication networks and computer systems. It is clear that the protection of hardware is vital for making NATO's doctrines operational, including the Allied Joint Doctrine for Air and Space Operations and the 2009 Allied Land Tactics document.[87] The importance of hardware is further recognized in NATO members' national documents, such as the UK's Joint Doctrine Note on Cyber and Electromagnetic Activities,[88] or France's 2017 Senate report on nuclear deterrence, which recognizes the potential kinetic consequences of cyberattacks.[89] As NATO's Allied Joint Doctrine for Land Operations notes, cyberspace has interdependence with the electromagnetic spectrum and space domain.[90] The protection from cyberattacks of hardware, software, networks or data cannot be held strictly separate from the protection from electronic and electromagnetic threats.

Hardware plays a critical role in enabling communications – the disruption or destruction of which could enable adversaries to penetrate these communication lines and conduct cyber operations, or even destroy these lines. In October 2015 Russian submarines were reportedly operating 'aggressively' near vital undersea cables carrying almost all global internet communications, raising concerns among US military and intelligence officials that Russia might be planning to attack these lines in times of tension or conflict.[91] While undersea cables are difficult to physically access, adversaries with the right capabilities to reach them could pose a serious threat to the survivability of networks relying on the cables in question.

Malfunctioning sensors, whether as a result of malicious interference or purely unintentional, may also have unforeseen links with command, control and communications, and such system connections may ultimately lead to catastrophic consequences. In June 2016 the UK Royal Navy's HMS Vengeance test-fired an unarmed Trident II D5 ballistic missile off the coast of Florida; however, the missile went off course by reportedly several thousand miles.[92] The problem seems to not come from the missile itself or the launch system, but involved telemetry data – information gathered from various points and fed to the missile.[93] In principle, telemetry works through sensors

[87] NATO Standardization Office (2009), *Allied Land Tactics ATP-3.2.1*, https://www.scribd.com/doc/250355763/ATP-3-2-1-Land-Tactics (accessed 1 Aug. 2019).
[88] UK Ministry of Defence (2018), *Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities*, Joint Doctrine Note 1/18, Development, Concepts and Doctrine Centre, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf (accessed 10 Jun. 2019).
[89] Pintat, X., Lorgeoux, J., Trillard, A. and Allizard, P. (2017), *La nécessaire modernisation de la dissuasion nucléaire*, Rapport d'information n°560 (2016-2017), Sénat, http://www.senat.fr/rap/r16-560/r16-560.html (accessed 28 May 2019).
[90] NATO Standardization Office (2016), *NATO Standards AJP-3.2, Allied Joint Doctrine for Land Operations*, pp. 1 – 23.
[91] Sanger, D. E. and Schmitt, E. (2015), 'Russian Ships Near Data Cables Are Too Close for U.S. Comfort', *New York Times*, 25 October 2015, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html (accessed 10 Jun. 2019).
[92] MacAskill, E. (2017), 'How did the Trident test fail and what did Theresa May know?', *Guardian*, 23 January 2017, https://www.theguardian.com/uk-news/2017/jan/23/how-did-the-trident-test-fail-and-what-did-theresa-may-know (accessed 10 Jun. 2019).
[93] MacAskill, E., 'MoD cannot fall back on usual excuses to explain Trident misfire', *Guardian*, 22 January 2017, https://www.theguardian.com/uk-news/2017/jan/22/mod-cannot-fall-back-on-usual-excuses-to-explain-trident-misfire (accessed 10 Jun. 2019).

at the remote source which measures physical or electrical data; and telemetry data may be relayed using radio, infrared, ultrasonic, GSM, satellite or capable, depending on the application.[94] Although this incident did not result from malicious interference with the sensors, it serves to demonstrate how tampering with sensors could have serious consequences. Adversaries could either use electronic warfare capabilities to disrupt the data collected by the sensors, or they could launch cyberattacks on the means used to relay the telemetry data – for example satellites. In a situation of armed conflict, successful disruption of an armed missile's trajectory would not only result in the loss of the mission from a strategic standpoint, it could also potentially lead to civilian harm, especially if the armed missile lands in a populated area – thus resulting in severe humanitarian consequences and violations of international humanitarian law (IHL). Protection of hardware is of particular importance in light of the sophistication of electronic warfare capabilities, such as the US Air Force's Counter-Electronics High Power Microwave Advanced Missile Project (CHAMP),[95] which could exploit high-power microwave bursts to disable computers and electronics within the targeted area.[96] China is also reportedly developing similar high-power microwave technologies.[97]

Theme 4: access/security controls

Access and security controls are not explicitly mentioned in NATO's strategy and doctrine documents *per se*, however it is clear that classification of information and limited physical access to certain premises constitute a critical part in protecting C3 systems. Providing layers of defence establishes oversight of the nuclear C3. Moreover, it enables limited physical access to sensitive C3 premises only by authorized individuals, including private contractors. Limiting physical access, as a result, reduces cyber risks from insider threats and prevents accidental breach.

The US Department of Defense has recently released two relevant reports. In March 2018 its Inspector General released a report, *Logical and Physical Access Controls at Missile Defense Agency Contractor Location*s,[98] based on a performance audit conducted in March–December 2017. The publicly available report sets out in detail some of the findings, but does not disclose the name and location of the seven contractor facilities assessed.

This audit demonstrates that while the Missile Defense Agency (MDA)'s contractors may be dealing with highly sensitive components of nuclear C3 systems – such as classified technical information with access to classified networks – there remain many vulnerabilities that could present

[94] Stackify (2017), 'What Is Telemetry? How Telemetry Works, Benefits of Telemetry, Challenges, Tutorial, and More', https://stackify.com/telemetry-tutorial/ (accessed 10 Jun. 2019).
[95] Boeing (2012), 'Boeing Non-kinetic Missile Records 1st Operational Test Flight', https://boeing.mediaroom.com/2012-10-22-Boeing-Non-kinetic-Missile-Records-1st-Operational-Test-Flight (accessed 31 May 2019).
[96] Lewis, B. (2012), 'Raytheon EMP weapon tested by Boeing, USAF Research Lab', Military Embedded Systems, http://mil-embedded.com/news/raytheon-emp-missile-tested-by-boeing-usaf-research-lab/ (accessed 10 Jun. 2019).
[97] Kania, E. B. (2017), 'The PLA's Potential Breakthrough in High-Power Microwave Weapons', *The Diplomat*, 11 March 2017, https://thediplomat.com/2017/03/the-plas-potential-breakthrough-in-high-power-microwave-weapons/ (accessed 10 Jun. 2019); Fisher, R. D. Jr (2013), 'China's Advanced Weapons', China's Progress with Directed Energy Weapons', Testimony before the U.S.-China Economic and Security Review Commission hearing, 23 February 2017, https://www.uscc.gov/sites/default/files/Fisher_Combined.pdf (accessed 10 Jun. 2019).
[98] Inspector General, U.S. Department of Defense (2018), *Logical and Physical Access Controls at Missile Defense Agency Contractor Locations*, https://media.defense.gov/2018/Apr/05/2001899799/-1/-1/1/DODIG-2018-094.PDF (accessed 10 Jun. 2019).

opportunities for adversaries to interfere, disrupt, or even disable and destroy critical components of C3 systems. This is of particular concern given past incidents and previous reports. For instance, a malware (agent.btz) infiltrated the US Central Command Computer systems through a USB drive in 2008.[99]

This may notably pose a threat to C3 systems, the survivability of which may depend on the security controls and processes implemented by MDA contractors. The report notes specifically that these contractors are in possession of classified and unclassified technical information related to BMDS; however, 'system and network administrators at three contractors that managed BMDS technical information on classified networks did not identify and mitigate vulnerabilities on classified networks and systems'.[100] Should an adversary be able to infiltrate these contractors' networks, they may be able to obtain access to classified BMDS technical information, thus jeopardizing the credibility of Allies' BMDS.

Fuller details from the Inspector General's report are included in Appendix III. To summarize here, the 'control deficiencies' identified by the audit conducted on seven contractors in the US, and which may present serious implications for the security of BMDS facilities, included:[101]

- Multifactor authentication was not consistently used
- System passwords were not always strong
- Lack of periodical risk assessments by contractors
- Problems with systematically mitigating network and system vulnerabilities
- Lack of oversight of third-party service providers' activities in network protection
- Contractors allowed users to process and store unclassified controlled technical information on personal electronic devices
- Removable media were not properly protected
- Problems with automatic locking of systems after inactivity or after unsuccessful login attempts
- Lack of consistency in how system access and user privileges were granted
- Issues in keeping and reviewing system activity reports

In December 2018 the Inspector General of the Department of Defense released a further report, *Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information*,[102] that echoed the concerns expressed by the report published earlier that year. Its

[99] Shachtman, N. (2008), 'Under Worm Assault, Military Bans Disks, USB Drives', *WIRED*, 19 November 2008, https://www.wired.com/2008/11/army-bans-usb-d/ (accessed 28 May 2019).
[100] Inspector General, U.S. Department of Defense (2018), *Logical and Physical Access Controls at Missile Defense Agency Contractor Locations*, p. 4.
[101] Ibid., pp. 4–21.
[102] Inspector General, U.S. Department of Defense (2018), *(U) Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information*.

findings ultimately concluded that officials did not consistently implement security controls and processes to protect BMDS technical information, which could allow US adversaries to circumvent ballistic missile capabilities. The findings included: a vulnerability detected in 1990 and failure to mitigate the vulnerability ever since; officials did not encrypt removable media or did not enforce the use of encryption; and the Army, Navy and MDA did not protect networks and systems that process, store and transmit technical information from unauthorized access and use. Suffice to say that identification of cyber vulnerabilities is of value only if audit recommendations are implemented accordingly.

While both reports are worrying, and demonstrate the difficulties the US may have in ensuring constant oversight on the implementation of adequate and robust security measures by contractors, it is also encouraging to see that the US government is conducting audits to identify those vulnerabilities and issuing recommendations to address them. In 2019, for example, the US Defense Innovation Board published a study with recommendations to address 'the most critical statutory, regulatory, and cultural hurdles US Department of fence faces in modernizing its approach to software', including those developed by contractors.[103] From as early as 2013, moreover, the Defense Science Board Task Force on Resilient Military Systems drafted a report, *Resilient Military Systems and the Advanced Cyber Threat*, as a result of which the Task Force was asked to 'review and make recommendations to improve the resilience of DoD systems to cyberattacks, and to develop a set of metrics that the Department could use to track progress and shape investment priorities'.[104] Yet, considering that the US is generally proactive in protecting its weapons systems, the findings of the audit should stimulate questions as regards the other nuclear weapons states. Publicizing these positive measures may not only play a role in reinforcing Allies' own willingness to enhance their cybersecurity measures and ensure their C3 systems' survivability; it may also play a deterrent role *vis-à-vis* adversaries. Put otherwise, these documents attest to the US's level of awareness and capabilities to addressing the identified cyber vulnerabilities. Such measures could constitute best practice for NATO and NATO Allies to consider adopting and implementing.

Theme 5: cybersecurity awareness/by design

This final theme is to develop capabilities that are secure by design. Cybersecurity awareness and cybersecurity by design must be incorporated into the entire life cycle of weapons systems acquisitions and other capabilities, as well as in operations and missions.

From a cybersecurity awareness standpoint, NATO Allies must further reinforce cybersecurity training for all staff at all levels – to not only raise awareness of the existence of cyberthreats and vulnerabilities, but also to enhance their ability to identify, adopt the appropriate reaction and

[103] McQuade, J. M., Murray, R. M., Louie, G., Medin, M., Pahlka, J. and Stephens, T. (2019), *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, Defense Innovation Board, https://media.defense.gov/2019/Apr/30/2002124828/-1/-1/0/SOFTWAREISNEVERDONE_REFACTORINGTHEACQUISITIONCODEFORCOMPETITIVEADVANTAGE_FINAL.SWAP.REPORT.PDF (accessed 24 Jan. 2020).
[104] Gourley, B. (2013), 'DSB Report on Resilient Military Systems and the Cyber Threat', GovLoop, 1 March 2013, https://www.govloop.com/community/blog/dsb-report-on-resilient-military-systems-and-the-cyber-threat/ (accessed 3 Feb. 2020).

address adequately these risks. All staff across the entire chain of command need to be able to do this in a comprehensive manner to protect C3 systems. This ultimately underscores the importance of the human factor, which must not be neglected or overlooked in cybersecurity discussions: while software and hardware are the main areas of concern from a technical standpoint, human processes and human involvement in the weapons systems enterprise (i.e. operators, coders, engineers, system designers, among others) are equally critical for their security. This is also closely related to the previous theme, where access and security controls are heavily dependent on human processes, regulation and oversight. Challenges to cybersecurity will be fundamentally human in nature, and may very well represent one of the most worrying threat vectors to gain access and control to systems.

In addition, there is a need for NATO Allies to realize, acknowledge and ensure that their newly developed systems are secure by design. A report released by the US Government Accountability Office (GAO) in October 2018, *DOD Just Beginning to Grapple with Scale of Vulnerabilities*,[105] underscores this point. The report identified that multiple factors contribute to the current state of the Department of Defense's weapon systems cybersecurity, including: the increasingly computerized and networked nature of its weapons; its past failure to prioritize weapon systems cybersecurity; and its nascent understanding of how best to develop more cyber secure weapon systems.[106] Specifically, the Department of Defense's weapon systems are more software- and IT-dependent and more networked than ever before. The report further noted that this has transformed weapon capabilities and constitutes a 'fundamental enabler' of the US's modern military capabilities. The report concluded that the Department of Defense is still in the early stages of trying to understand how to apply cybersecurity to weapon systems. One notable example cited in the report is the department's choice to focus on the cybersecurity of its networks but not the weapon systems themselves, which points to the need for all states to rethink the way they approach and attempt to address cybersecurity vulnerabilities and threats, as well as the importance of adopting a comprehensive and holistic approach. In other words, the Department of Defense must not exclusively focus on the cybersecurity of its networks. It must also ensure that newly deployed weapons systems and those currently at the development, testing and evaluation stages are cyber secure by design (built-in), as well as adopt the adequate measures to ensure that those weapons systems that are already deployed, including legacy ones, are cyber secure (e.g. through regular stress-testing and scans, and technical and human resources dedicated to immediately develop and install patches remedying the effects and consequences of cyberattacks). This approach will foster a culture of cybersecurity and ensure in the long term that deployed weapons systems will be resilient against the growing number and sophistication of cyberattacks.

Several Department of Defense officials are of the opinion that it may take 'some missteps' for the department to learn what works and what does not work with respect to weapon systems cybersecurity.[107] This somewhat indicates a shift from the deterministic approach to traditional systems, expected to perform predictable tasks in bounded environments,[108] towards a more

[105] United States Government Accountability Office (2018), *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, https://www.gao.gov/assets/700/694913.pdf (accessed 10 Jun. 2019).
[106] Ibid.
[107] Ibid., p. 11.
[108] Macias, F. (2008), 'The Test and Evaluation of Unmanned and Autonomous Systems', *ITEA Journal*, 29(4): pp. 388–395, https://pdfs.semanticscholar.org/4743/d713805045e9a22dd9def7e9a8ec9f5c525c.pdf (accessed 23 Jun. 2019).

probabilistic approach, accepting the fact that weapons systems may have cyber vulnerabilities and may actually face cyberattacks – or at least, to reiterate that wording, 'some missteps'.[109]

This observation is echoed in the US Director – Operational Test and Evaluation's (DOT&E) 2018 annual report, which sets out the need for further consideration for cybersecurity awareness and by design by the Department of Defense.[110] Vulnerabilities identified during earlier testing periods were still present at cybersecurity testing in 2018, such as the vulnerabilities identified in the F-35 training systems, the Autonomic Logistics Information Systems (ALIS) version 3.0, and the ALIS-to-shipboard network interface on board a nuclear powered aircraft carrier.[111] Cybersecurity testing on the currently fielded version of the Joint Operation Planning and Execution System (JOPES, v4.3.0.2) – the system that is used 'to translate policy decisions into operations plans to meet U.S. requirements to employ military forces, support force deployment, and conduct contingency and crisis action planning' – produced an inadequate test result due to the team's failure to conduct the test in accordance with the approved test plan.[112] No advanced attacks could be conducted. This means that the Department of Defense is currently using a version of a C2 system to operationalize policy decisions, including force deployment, without being fully aware of the extent of survivability of the system and without all the important actors knowing the full range of potential existing vulnerabilities.[113] Another example relates to the Infantry Carrier Vehicle – Dragoon (ICV-D) developed by the US Army in March 2015.[114] ICV-D obtained lethality upgrades allowing crews to detect, identify and defeat targets at greater ranges and against a wider array of enemy targets. However, exploitable cybersecurity vulnerabilities were found, and the report notes that adversaries demonstrate 'the ability to degrade select capabilities of the ICV-D when operating in a contested cyber environment'.[115] In most cases, the exploited vulnerabilities predate the integration of the lethality upgrade. ICV-D received lethal upgrades before exploitable cybersecurity vulnerabilities were identified and addressed. While on the one hand the upgrade may have changed the system such that prior vulnerabilities are no longer valid; on the other hand, the upgrade could result in even more cyber vulnerabilities.

Moreover, in 2018 the GAO found while the MDA is developing a system to track and destroy enemy missiles, the military personnel and decision-makers would benefit from better communication about the system's capabilities and limitations[116] – including, given its critical nature, in the realm of cybersecurity.

[109] United States Government Accountability Office (2018), *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, p. 11.
[110] Director, Operational Test and Evaluation (2018), *FY 2018 Annual Report*.
[111] Ibid., p. 23.
[112] Ibid.
[113] Ibid., pp. 37–38.
[114] Ibid., pp. 103–104.
[115] Ibid.
[116] U.S. Government Accountability Office (2018), 'Missile Defense: The Warfighter and Decision Makers Would Benefit from Better Communication about the System's Capabilities and Limitations', https://www.gao.gov/products/GAO-18-324 (accessed 10 Jun. 2019).

While these findings may be of high concern for NATO and its Allies, leading to questions regarding the survivability of NATO's NC3 systems, it is also encouraging to see that the US has official bodies (the GAO, IG and DOT&E) conducting audits to identify those vulnerabilities and issuing recommendations to address them. What is critical, however, is whether these findings and recommendations will be taken into account and be implemented.

4. Entanglement of Conventional and Nuclear Command and Control

The increasing reliance on dual-use C3 assets, those used both for conventional and nuclear operations, raises the issue of entanglement and the risk of rapid escalation. These dual-use assets can range from communications satellites to early warning systems, radars and transmitters. According to recent research, notably by James M. Acton, parties to a conflict 'could have strong incentives to attack the adversary's dual-use C3I [command, control, communication and intelligence] capabilities to undermine its nonnuclear operations'.[117] An attack on a dual-use C3 asset would particularly hold strong incentives for adversaries possessing nuclear weapons and not ruling out their potential use. For instance, a cyberattack on early warning satellites will provide a tremendous advantage to the adversary by either delaying the detection of a missile launch (conventional or nuclear) or even preventing it from being identified in the first place.

James M. Acton addresses two mechanisms that lead to escalation.[118] First is a 'misinterpreted warning', probably at a time of crisis, where a state's dual-use C3 assets are targeted by conventional weapons or cyber interferences and the target state might misinterpret these attacks as 'preparations for an incoming use of nuclear weapons' by their adversary.[119] The targeted state might miscalculate and respond in a highly escalatory way that leads to full-scale conventional or nuclear war. Second, if a state's C3 capability was attacked by conventional means, it might lose its advantage to destroy an adversary's nuclear weapon systems. In order to prevent such a situation happening, the state might use pre-emptive countermeasures that would themselves lead to escalation,[120] thus adding nuclear 'use it or lose it' pressures to conventional crises.

It is important to note that the escalation mechanisms identified by Acton rest on hypothetical situations in which states that have been forced, for the purposes of the argument, into adopting an inherently escalatory posture; in reality, this may not be the inevitable outcome. The role of conventional forces and cyber interferences is highlighted primarily and under specific conditions as a route to escalation, rather than also as a source of potential de-escalation. Although risks of escalation through entanglement might be greater in some cases, it is hard to judge a state's possible actions only by counting its conventional or nuclear capabilities or by assigning an escalatory role to them. Escalation is a choice, and the logic of escalation mechanisms removes the factor of human agency for conflict avoidance. Ultimately, survival of a state may not, in all instances, be linked to the survival of its nuclear forces.

Sometimes, from a cybersecurity perspective, an attack on dual-use C3 systems may lead to increased uncertainty as regards who conducted such an attack, what is the intention behind it, and how quickly the system would recover. These last two points are further called into question in a

[117] Acton, J. M. (2018), 'Escalation through entanglement'.
[118] Ibid.
[119] Ibid., p.58.
[120] Ibid., p. 59.

context of reliance on increasingly autonomous technologies, which are now already assisting the conduct of cyber defensive operations – which implies the potential for their future use in underpinning offensive operations as well.

In other cases, cyberattacks may not in themselves be enough to make deterrence less stable. Deterrence is all about perception, and ensuring that states can continue to project confidence. This may be false confidence, however, where their nuclear C3 assets are concerned. Once a state starts to question the credibility of its NC3 assets, suspecting that these assets are already penetrated, the assets may lose the associated value of deterrence. During a crisis, how a state assesses whether an incident is a glitch or a surprise attack also crucially depends on the trust that the state puts in deterrence, as well as on state's capacity to conduct and be certain of the findings of cyber forensic investigation. Thus, for some states it is hard to let go of – or to even question – deterrence assumptions.

5. Legal Implications of Attacking Dual-use C3 Systems

Given the complexity and sophistication of C3 systems, it is difficult, if not impossible, to entirely predict and anticipate outcomes of a cyberattack and/or the probability of a given outcome. For example, an attack on a dual-use C3 system may have unintended consequences, such as the rapid increase of temperature of the hardware due to the modification of settings and parameters, consequently causing physical damage to the targeted assets when perhaps the initial motivation behind the attack was limited to merely modifying settings and parameters. Potential unintended consequences add layers of uncertainty and complexity to problems of misinterpretation and could potentially add escalatory pressure. These unintended consequences can subsequently have serious legal implications, notably in the realm of law of armed conflict/international humanitarian law (IHL).

In an armed conflict, an armed attack must respect the principles of distinction, proportionality and precautions.[121] These principles may be (unintentionally) violated due to the dual-use nature (military and civilian) of assets used for both nuclear and conventional C3. In the context of an armed conflict, if the affected assets were used both for military and civilian applications, determining the extent to which the attack on these assets would constitute a 'definite military advantage' at the time of the operation would be key in determining the legality of the attack vis-à-vis the principle of distinction.[122] For instance, global navigation satellite systems (GNSS) play a crucial role in accurate timing and synchronization, as well as in weapon guidance (navigation),[123] all of which constitute critical elements for both nuclear and non-nuclear operations. However, an operation directed at GNSS assets could not only prove to be highly escalatory for the reasons outlined above, but may also potentially constitute a violation of the legal principle of distinction, given that the same assets are used not solely in the defence sector, but throughout national critical infrastructure sectors for civilian purposes.[124] While dual-use C3 assets may be cost-effective and

[121] The principles of distinction, proportionality and precautions in attack are of customary nature, and are respectively codified for international armed conflicts in Articles 48, 51(5)(b), and 58 of the 1977 Additional Protocol I to the 1949 Geneva Conventions. These principles are also applicable in non-international armed conflicts.
[122] The legality of an armed attack on a dual-use object (which may have both military and civilian functions) depends on whether, at the time of the attack, it would have constituted a 'definite military advantage'. For the ICRC's definition of military objectives, see: International Committee of the Red Cross (undated), 'Rule 8. Definition of Military Objectives', https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule8 (accessed 17 Oct. 2019).
[123] Unal (2019), *Cybersecurity of NATO's Space-based Strategic Assets*, p. 10.
[124] A cyber operation on a dual-use C3 asset may potentially constitute a violation of the customary principle of distinction between civilian objects and military objectives in IHL, as codified in Articles 48 and 52(2) of the 1977 Additional Protocol I to the 1949 Geneva Conventions. Parties to a conflict must distinguish at all times between military objectives and civilian objects while directing an armed attack. For a discussion on whether the principle of distinction applies in cyber operations, see Lubell, N. (2013), 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?', *International Law Studies*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2719034 (accessed 25 Dec. 2019). The International Criminal Tribunal for the former Yugoslavia examined the issue of dual-use objects that may be both a military objective and a civilian object and the legality of armed attacks on such dual-use objects. For a discussion, see: Cotter, M. (2018), 'Military Necessity, Proportionality and Dual-Use Objects at the ICTY: A Close Reading of the *Prlić et al.* Proceedings on the Destruction of the Old Bridge of Mostar', *Journal of Conflict and Security Law*, 23(2), pp. 283–305, https://doi.org/10.1093/jcsl/kry015 (accessed 27 Sept. 2019). The First Tallinn Manual argues that 'an object used for both civilian and military purposes – including computers, computer networks, and cyber infrastructure – is a military objective.' The Manual is not legally binding and offers a potential interpretation of the law on cyber operations, which may (or may not) be applied in the context of a cyber operation on a GNSS asset. See International Group of Experts at the Invitation of

practical from an operational perspective, with the growing sophistication and increasing number of offensive cyber operations they may be problematic from an IHL perspective.

This is of importance given the potential for unintended consequences of cyber operations and what this may mean for the civilian sphere. Indiscriminate cyber operations may cause damage without distinction to military objectives and civilian objectives.[125] In the context of a cyber operation on a dual-use C3 asset in an armed conflict, it is almost impossible to ensure that the direct and indirect consequences of the attack remain within the existing legal frameworks for the conduct of hostilities and do not spill over to cause harm on civilian objects. However, it is important to note in this context that damages caused to these civilian objects may to a certain extent be lawful as long as they are proportionate.[126]

Another key aspect is the customary precautionary principle against the effects of an attack, for which parties to a conflict 'must take all feasible precautions to protect the civilian population and civilian objects under their control against the effects of attacks'.[127] There is value in examining the extent to which states have a legal obligation in ensuring and taking 'all feasible precautions' to protect these dual-use assets that the civilian sphere and the military may depend on for C3 purposes (e.g. weather forecast satellites) against the effects of attacks.

In addition, the assessment of an attack's legality may prove to be challenging in the context of cyber operations against NC3 systems, as there may be conflicting views on whether or not there is an armed conflict – thus how the norms on the conduct of hostilities in IHL apply (and whether the law of armed conflict is applicable, at all) – unless the attack is obviously part of a wider conflict. It is also debatable whether a cyber operation is considered to cross the threshold of armed conflict, and thus for the laws of armed conflict to be applicable.[128] This uncertainty may particularly dominate when the attacks are of relatively low impact, and thus may not even be considered as an 'attack' in its legal sense. Such operations can be even more problematic if the disruption comes from a non-state armed group.[129]

The NATO Cooperative Cyber Defence Centre of Excellence (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, p. 134.

[125] International Committee of the Red Cross (2019), *International Humanitarian Law and Cyber Operations during Armed Conflict*, https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf (accessed 25 Dec, 2019)

[126] This is in accordance with the customary rule of proportionality, based on which the launch of an attack that 'may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof' should not 'excessive in relation to the concrete and direct military advantage'. See International Committee of the Red Cross (undated), 'Rule 14. Proportionality in Attack', https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule14 (Accessed 10 June, 2020).

[127] International Committee of the Red Cross, 'Rule 22. Principle of Precautions against the Effects of Attacks', https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule22 (accessed 26 Sept. 2019).

[128] Krawczyk, L. (2019), 'How does cyber warfare fit in the framework of International Humanitarian Law?', Leiden Law Blog, 9 August 2019, https://leidenlawblog.nl/articles/cyber-warfare-the-definition-challenge (accessed 20 Dec. 2019).

[129] The rules applicable to an armed conflict between states are different from those applicable to an armed conflict between a state and a non-state armed group. The threshold to trigger the application of IHL is higher if the adversary of the state party to the armed conflict is a non-state entity, and the latter must meet a certain number of criteria in order to be considered party to an armed conflict with a state under IHL.

6. Conclusion and Way Forward

This paper addresses, for the public domain, cyber resilience in NATO's NC3 systems in the air, land and maritime domains. In this regard, the paper has considered five themes that are valuable for cybersecurity considerations: software and network protection; data protection; hardware protection; access/security controls; and cybersecurity awareness/security by design.

The cybersecurity of weapon systems comes down to the confidence in system and information integrity. In order to ensure system integrity, resilience approaches should also be complex. It is important to realize that public perception regarding the cybersecurity of nuclear weapon systems is relatively unfavourable, compared with the confidence that NATO and NATO Allies have in their C3 systems. This paper covers a spectrum of *known* cybersecurity incidents. It is important to acknowledge that, due to NATO's established barriers to prevent entry to critical systems, not all *known* cases may pose meaningful threats to the Alliance's C3 and/or NC3 systems.

At the technical level, even if known cases do pose threats to NC3 systems, some level of vulnerability may in fact increase system resilience in the long run. Managing risk through the experience of past cyber incidents and the process of mitigating these threats and actively withstanding some disturbances with acceptable recovery time may be considered *un mal nécessaire*[130] in protecting NC3 systems. At the decision-making level, however, there is almost no margin for error. This means that policymakers and military cadre alike must assess intelligence data and all other relevant information with a critical eye, because missteps in decision-making may result in conflict escalation.

In the public sphere, it is impossible to know how many of the cyberattacks that have been reported have posed real, tangible risk to NC3 systems. It may be the case that one side is over-exaggerating the problem (civil society in public discourse) whereas the other at times is understating it (official discourse). False confidence and false stress are equally problematic. Whereas false confidence may lead to unintended consequences (e.g. accidental nuclear use), false stress may lead to excessive fear, and this may affect policies and decision-making as well potentially resulting in overspending. Bridging the gap between the two discourses requires both sides to work together: NATO Allies must be able to share relevant information in the public domain without breaching security, and experts must work to debunk false certainties with regard to the cybersecurity (or insecurity) of NC3 systems.

As technological progress proceeds apace, networks that are physically isolated at the design stage are rarely isolated throughout their life cycle. Patching, maintenance and the introduction of new digital components to legacy systems, or even the proximity of smart devices, will continue to challenge the cybersecurity of weapon systems. Closed networks may have connections with open networks; however, there will still be protocols, such as limited access and clearance requirements, and screening processes, that can prevent cyber infiltration. In simple terms, if someone plugs an

[130] The closest translation in English would be 'a necessary evil'.

infected USB into a system, this does not necessarily mean that the system will be compromised: a system can be protected against infection by existing barriers.

The ecosystem is in itself important in upholding cybersecurity. In this regard, trying to change human behaviour through regulation (not allowing smart watches into military compounds, for instance) may be necessary, but regulation alone is insufficient as a defence, and it may overlook and detract from addressing fundamentally systemic issues. States should prioritize making networks and systems human-friendly, while taking active measures to remediate potentially harmful human behaviour by fostering a culture of cybersecurity.[131]

Cyberthreats may pose questions as regards the integrity of data, thus leaving decision-makers in doubt as to whether the information they hold is truly reliable. The application of emerging technologies may be useful in providing evidence-based information in such instances. Although, at times, new technology (AI with machine learning techniques, for instance) may challenge NC3, technology-enhanced decision-making (e.g. through modelling and simulation techniques and big data analysis) may be able to provide valuable information when decisions need to be taken within a very short time frame. Autonomous and automated technologies will also play an increasingly important role in detecting, assessing, characterizing and mitigating vulnerabilities and novel attack vectors in critical systems, as the work of the US Department of Defense's Defense Advanced Research Projects Agency (DARPA) and its contractors suggests.[132]

An assessment of how adversaries think about command and control might also help NATO and Allies to understand cyber offence and cyber defence strategies. NATO should also address the cyber risk that comes with procurement of military equipment from countries that are not friendly to NATO (e.g. Russia or China). At its 2018 Brussels Summit, NATO stated its commitment to 'working to address existing dependencies on Russian-sourced legacy military equipment through national efforts and multinational cooperation'.[133] At present, several NATO countries – among them Montenegro, Romania, Bulgaria and Poland – possess legacy equipment from the Soviet era.[134] A study of the cybersecurity of Russian legacy systems in NATO member countries and methods, as part of efforts to reduce this dependency, would provide important analysis and insights for the Alliance.

[131] HM Government (2016), 'National Cybersecurity Strategy 2016-2011', https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (accessed 20 Dec. 2019).
[132] As a response to the increasing number of broad-spectrum cyberthreats, one of DARPA's research programmes seeks to 'develop automated tools to detect and characterize novel attack vectors, collect the right contextual data, and disseminate protective measures both within and across enterprises'. In addition, DARPA has awarded a contract to Galois to 'build a tool that uses a hybrid human-machine approach to detecting cyber security vulnerabilities that go undetected using traditional methods'. See, respectively, Patel, T. (undated) 'Cyber-Hunting at Scale (CHASE)', Defense Advanced Research Projects Agency, https://www.darpa.mil/program/cyber-hunting-at-scale (accessed 3 Feb. 2020); and Galois (2019), 'Galois Awarded $8.6 Million DARPA Contract to Build Cyber Reasoning Tool that Discovers Security Vulnerabilities', 20 August 2019, https://galois.com/news/chess-cyber-reasoning-tool-to-discover-security-vulnerabilities/ (accessed 3 Feb. 2020).
[133] NATO (2018), 'Brussels Summit Declaration', 11 July 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm (accessed 6 Jan. 2020).
[134] See International Institute for Strategic Studies (IISS) (2019), 'Chapter Four: Europe', in IISS (2019), *The Military Balance*, 119(1), pp. 66–165, doi: 10.1080/04597222.2018.1561029 (accessed 6 Jan. 2020).

There will always be some risks for NATO when it comes to defending its strategic assets, including nuclear systems.[135] The question is therefore: What are the areas in which its assets are so critical that NATO cannot tolerate any risk at all, and where could it progressively accept a greater level of risk as the importance of certain assets declines? Considering that NATO cannot defend all of its assets, prioritization of efforts on the basis of significance and risk should continue to be the guiding principle.

[135] This leads to the fundamental question of nuclear weapons risks. For a discussion on analytically framing nuclear risks considerations, see Wan, W. (2019), *Nuclear Risk Reduction: A Framework for Analysis,* Geneva: United Nations Institute for Disarmament Research, https://www.unidir.org/sites/default/files/2019-11/nuclear-risk-reduction-a-framework-for-analysis-en-.pdf (accessed 17 Mar. 2020).

Appendix I: NATO Allies' Nuclear Planning and NC3 Architecture

That NATO members' NC3 architecture is secure and reliable is of particular importance for deterrence purposes. Even when the Alliance's NC3 systems are under attack, all member states should be able to demonstrate their detection, forensics and response capabilities, which necessitates that NC3 architecture continues to function as planned. Drawing on information available in the public domain, this section sets out that architecture for the three nuclear weapon states within NATO.[136]

The US

Authority to order the use of the US's nuclear weapons lies solely with the US president,[137] as commander-in-chief of the armed forces. While this has been subject to deliberation,[138] the role of actors other than the president in authorizing the use of nuclear weapons is consultative, and serves to assist the planning of operations. Critically, however, this does not extend to the ability to veto decisions.[139] The NC3 architecture in the US has certain distinct functions, including force management, nuclear planning, situation monitoring, decision-making, and distributing force direction orders.[140] The exercise of these functions requires dedicated, redundant and survivable connectivity for the president to communicate effectively with all nuclear-capable forces through a network of communications and warning systems. These allow the president to make and communicate critical decisions without constraint.[141]

The US NC3 system is known to comprise of as many as 160 different systems, including but not limited to communication networks, control centres, land stations, radio receivers, satellites and aircraft.[142] As a result, there are many cases in which a number of different elements contribute to the delivery of US NC3 missions. Much of the apparatus presently included in this inventory is legacy infrastructure developed accumulatively throughout the course of the Cold War, which is now undergoing comprehensive modernization through a process that includes incorporating new

[136] France retains strict autonomy over its nuclear weapons, and does not participate in the NATO Nuclear Planning Group.
[137] Woolf, A. F. (2018), *Defense Primer: Command and Control of Nuclear Forces*, Congressional Research Service, https://fas.org/sgp/crs/natsec/IF10521.pdf (accessed 10 Oct. 2019).
[138] Lewis, J. G. and Tertrais, B. (2019), *The Finger on the Button: The Authority to Use Nuclear Weapons in Nuclear-Armed States*, CNS Occasional Paper #45, James Martin Center for Nonproliferation Studies, Middlebury Institute of International Studies at Monterey, https://www.nonproliferation.org/wp-content/uploads/2019/02/Finger-on-the-Nuclear-Button.pdf (accessed 10 Oct. 2019).
[139] Wellerstein, A. (2019), *NC3 Decision Making: Individual Versus Group Process*, Tech4GS Special Reports, https://www.tech4gs.org/uploads/1/1/1/5/111521085/tech4gs_wellerstein_commander_nc3_5.pdf (accessed 10 Oct. 2019).
[140] Clark, R. M., Lt. Gen., USAF (2019), *Air Force Instruction 13-550: Air Force Nuclear Command, Control, and Communications (NCD3)*, United States of America Department of the Air Force, https://fas.org/irp/doddir/usaf/afi13-550.pdf (accessed 1 Aug. 2019).
[141] Office of the Deputy Assistant Secretary of Defense for Nuclear Matters (2016), *Nuclear Matters Handbook*, Department of Defense and the Department of Energy National Nuclear Security Administration, https://www.acq.osd.mil/ncbdp/nm/NMHB/docs/NMHB_2016-optimized.pdf (accessed 1 Aug. 2019).
[142] Larsen, J. (2019), 'Nuclear Command, Control, and Communications: US Country Profile', NAPSNet Special Reports, https://nautilus.org/napsnet/napsnet-special-reports/nuclear-command-control-and-communications-us-country-profile/ (accessed 10 Oct. 2019).

technology means to tackle modern threats.[143] US NC3 is composed of 'early warning satellites and radars, communications satellites, aircraft, and ground stations, fixed and mobile command posts, control centers for nuclear systems'[144] – all of which contain digital components. The malicious manipulation of hardware or software in a nuclear platform could cause malfunctioning of these elements, and may compromise the mission completely.

The president, the Secretary of Defense and other senior cadre make decisions on nuclear weapons deployment based on the collection of information via the US Nuclear Command and Control System (NCCS).[145] Moreover, the NCCS provides the means by which the president can then make the decision to authorize the use of nuclear weapons, based on information gathered to provide warning of attacks on the US and its NATO Allies.[146] There are a number of stages involved in this process that each entails the use of NC3 infrastructure, starting with intelligence gathering[147] and proceeding through early warning systems, communications, authorizations and eventual launch.

For the purpose of providing missile early warning, the Defense Support Program (DSP) remains in use as part of the Satellite Early Warning System. The early warning system is composed of fixed, terrestrial phased array warning radars, as well as its successor, the Space Based Infrared System (SBIRS), and the US Nuclear Detonation Detection System.[148] The DSP is a constellation of satellites that operate in geosynchronous orbit and detect launches using heat-detecting infrared sensors.[149] SBIRS works similarly to DSP, and was aimed to replace this ageing system, with additional capabilities such as the ability to simultaneously scan large areas and fixate on a particular area for various scales of missile activities.[150] However, a replacement to SBIRS, which began practical operations in 2011, has already been chosen in the form of the Next Generation Overhead Persistent Infrared System. This will consist of five satellites that are to build up SBIRS and 'integrate missile defence sensors',[151] providing increased warning time and survivability.[152] Together, these provide the basis of the US tactical warning system, along with the Ballistic Missile Early Warning System (BMEWS), which is comprised of terrestrial systems based in Alaska, Greenland and the UK. Considering that it relies on both terrestrial (i.e. radar) and space capabilities (e.g. satellites), there is a certain level of redundancy in the US early warning systems. Yet, this still may not provide survivability. Although these tactical warning systems are scattered around the world, they are only in three locations; and since these are fixed sites, they would be vulnerable to nuclear attack in time of conflict.

[143] Ibid.
[144] Office of the Secretary of Defense (2018), *Nuclear Posture Review*.
[145] Office of the Deputy Assistant Secretary of Defense for Nuclear Matters (2016), *Nuclear Matters Handbook*.
[146] Woolf (2018), Defense Primer: Command and Control of Nuclear Forces.
[147] Long, A. and Green, B. R. (2015), 'Stalking the Secure Second Strike: Intelligence Counterforce and Nuclear Strategy', *Journal of Strategic Studies* 38(1-2), https://www.tandfonline.com/doi/pdf/10.1080/01402390.2014.958150 (accessed 11 Jun. 2020).
[148] Office of the Secretary of Defense (2018), *Nuclear Posture Review*, p. 56.
[149] Williams, I. (2018), 'Defense Support Program (DSP)', Missile Threat, Center for Strategic and International Studies, https://missilethreat.csis.org/defsys/dsp/ (accessed 10 Oct. 2019).
[150] Missile Defense Project (2018), 'Space-based Infrared System (SBIRS)', Missile Threat, Center for Strategic and International Studies, https://missilethreat.csis.org/defsys/sbirs/ (accessed 10 Oct. 2019).
[151] Ibid.
[152] Strout, N. (2019), 'How a new missile warning system benefits industry', C4ISRnet, https://www.c4isrnet.com/battlefield-tech/space/2019/07/25/how-a-new-missile-warning-system-benefits-industry/ (accessed 10 Oct. 2019).

Communications as part of NC3 are carried out across the full breadth of the electromagnetic spectrum. This is due to the fact that the US operates multimodal nuclear weapon systems, which each benefit from the use of different bands of the spectrum for different systems, including higher-frequency waves for communication via satellites, while very low frequency (VLF) radio waves are used for broadcast communications with submersible vehicles such as submarines. For the purpose of communicating with air delivery crews and ICBM crews, the president and nuclear force commanders have both the Defense Satellite Communications System (DSCS) and the Advanced High Frequency Satellite System (AEHF).[153] These operate within the super high frequency (SHF) and extremely high frequency (EHF) bands, respectively, and offer greater resilience against electromagnetic blackout caused in the event of nuclear detonation. These frequencies also benefit from having higher data transmission rates (in comparison with the ultra and very high frequency bands that are commonly used by commercial and military radios), and are more difficult for adversaries to jam.[154] At the other end of the spectrum, large terrestrial antennas are required in order for nuclear command to communicate with submerged submarines. Submarines cannot receive EHF bands, as these waves cannot penetrate deep under water. Until 2004 extremely low frequency (ELF) waves were used to transmit messages to US submarines operating at great depths; however, a number of difficulties, including the rate at which data could be sent by using such means, reportedly led the US to shut down this method of communication.[155] Instead, today the VLF band is preferred for use in communication with submerged submarines; however, this frequency does not allow for communication at as great depths as ELF.

In addition to these fixed and geosynchronous communications apparatus, the US also operates a mobile airborne communications relay capability in the form of the E-6B. This is equipped with the airborne launch control system (ALCS), which allows commanders on board to communicate with all three elements of the US nuclear triad, including a five-mile extendable antenna to allow communication with submerged submarines.[156]

The UK

The UK solely operates a continuous-at-sea nuclear capability, the Trident Vanguard-class submarine, with at least one on patrol at all times. It is stipulated that the notice to fire takes 'several days'.[157] In other words, the nuclear missiles are currently not on standby (launch on warning) and would require an interval of time prior to launching. In theory, this would prevent any accidental launch scenarios. The 2013 Trident Alternatives Review, however, set out the requirement for deterrence as: 'A minimum nuclear deterrent capability that, during a crisis, is able

[153] Deptula, D. A. and LaPlante, W. A. with Haddick, R. (2019), *Modernizing U.S. Nuclear Command, Control, and Communications*, The Mitchell Institute for Aerospace Studies, http://docs.wixstatic.com/ugd/a2dd91_ed45cfd71de2457eba3bcce4d0657196.pdf (accessed 10 Oct. 2019)
[154] Ibid.
[155] Stromberg, J. (2015), 'Why the US Navy once wanted to turn Wisconsin into the world's largest antenna', Vox, 10 April 2015, https://www.vox.com/2015/4/10/8381983/project-sanguine (accessed 10 Oct. 2019); Sherriff, L. (2004), 'US Navy cuts ELF radio transmissions', The Register, 30 September 2004, https://www.theregister.co.uk/2004/09/30/elf_us_navy/ (accessed 17 Feb. 2020).
[156] Deptula and LaPlante with Haddick (2019), *Modernizing U.S. Nuclear Command, Control, and Communications*.
[157] Defence Nuclear Organisation, Ministry of Defence (2018), 'The UK's nuclear deterrent: what you need to know', Policy paper, https://www.gov.uk/government/publications/uk-nuclear-deterrence-factsheet/uk-nuclear-deterrence-what-you-need-to-know (accessed 23 Aug. 2019).

to deliver at short notice a nuclear strike against a range of targets at an appropriate scale and with very high confidence.'[158] Although the review report emphasized that this requirement is not a statement of UK policy,[159] if implemented, it may leave open the possibility of reducing the time frame to launch a missile to less than 'several days'. It is viewed by some as one of Trident's significant strengths that the ability exists to both shorten and extend this response time without such actions escalating a crisis.[160] Furthermore, the 2006 White Paper on the UK's nuclear deterrent outlined that while a 'Trident submarine is on deterrent patrol at any one time … that submarine is *normally* at several days 'notice to fire" [emphasis added].[161] This formulation alludes to the possibility of reducing this several days' notice to fire in exceptional, abnormal circumstances.

The UK currently maintains only sea-based nuclear forces.[162] The prime minister possesses exclusive authority to ultimately authorize the launch of nuclear missiles, whose orders would likely be conveyed from the Nuclear Operations Targeting Centre within the Pindar complex under Whitehall.[163] An accident and reporting document from the UK Government's Marine Accident Investigation Branch noted: 'Within the Northwood HQ, command and control of submarines was exercised by two Operating Authorities: Commander Task Force (CTF) 345, who exercised command of the Vanguard class strategic deterrent submarines; and CTF 311, who exercised command of all other UK submarines and NATO submarines operating in the Eastern Atlantic and UK waters.'[164]

During the Labour administration under Tony Blair, it was revealed that the prime minister also holds the authority to decide the contingency course of action to take in a situation where a decapitation attack has occurred (i.e. the British government has ceased to function). This is set out in four identical, handwritten 'letters of the last resort', addressed to the commanding officers of each Vanguard-class submarine.[165] Deliberate ambiguity surrounds the details of this process; however, a 10 Downing Street spokesperson did reaffirm the existence of the letters in April 2020 during Prime Minister Boris Johnson's hospitalization with COVID-19.[166] External communication

[158] HM Government, Cabinet Office (2013), *Trident Alternatives Review*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/212745/20130716_Trident_Alternatives_Study.pdf (accessed 23 Aug. 2019).
[159] Ibid. p. 3.
[160] Gower, J. (2019), *United Kingdom: Nuclear Weapon Command, Control, and Communications*, NAPSNet Special Reports, https://nautilus.org/napsnet/napsnet-special-reports/united-kingdom-nuclear-weapon-command-control-and-communications/ (accessed 10 Oct. 2019).
[161] The Secretary of State for Defence and The Secretary of State for Foreign and Commonwealth Affairs (2006), *The Future of the United Kingdom's Nuclear Deterrent*, CM 6994, p. 13 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/27378/DefenceWhitePaper2006_Cm6994.pdf (accessed 17 Feb. 2020).
[162] Walker, J. D. (2019), *A History of the United Kingdom's WE 177 Nuclear Weapons Programme*, BASIC, https://www.basicint.org/wp-content/uploads/2019/03/A-History-of-the-United-Kingdoms-WE-177-Nuclear-Weapons-Programme-ONLINE.pdf (accessed 23 Aug. 2019).
[163] Hennessy, P. and Jinks, J. (2015), 'Cameron's doomsday machine', *Sunday Times*, 11 October 2015, https://www.thetimes.co.uk/article/camerons-doomsday-machine-6wj0b66m3pg (accessed 10 Oct. 2019).
[164] Marine Accident Investigation Branch (2016), *Report on the investigation of the collision between the stern trawler Karen (B317) and a dived Royal Navy submarine in the Irish Sea on 15 April 2015*, Accident Report No. 20/2016, https://assets.publishing.service.gov.uk/media/57fe2e2ee5274a496200000a/MAIBInvReport20_2016.pdf (accessed 17 Feb. 2020).
[165] It is important to realize that sources on this information are historical and that this policy might have changed.
[166] Reynolds, E., McGee, L., Cullen, S. and Cotovio, V. (2020), 'Boris is 'stable' in ICU amid questions about who's running the UK', CNN, 8 April 2020, https://edition.cnn.com/2020/04/07/uk/boris-johnson-coronavirus-uk-gbr-intl/index.html (accessed 28 May 2020). The matter of the Johnson 'letters of last resort' has been raised in both the House of Commons

to and from the submarine reportedly uses a US–UK common military-grade encryption system, and transmits data through very low frequency and low frequency radio – although data may also be received from satellites when on or near the surface at higher frequency.[167] Another redundancy measure available to the prime minister in times of crisis is the ability to nominate formal nuclear deputies.[168] This measure, implemented after 9/11, allows these nominated ministers to make nuclear release decisions 'in case the top political authority becomes decapitated'.[169] In doing so, this adds another layer of resilience to the UK's nuclear decision-making capability.

While the prime minister possesses exclusive authority over the launch of nuclear missiles, it is worth noting that in 1962 the UK's nuclear capability was assigned to NATO through the Nassau Agreement, whereby 'the UK Prime Minister offered to commit the UK's nuclear armed V-bomber force, operational since the late 1950s, to a 'NATO pool', together with corresponding American, and possibly French, nuclear assets', which has in turn influenced British nuclear policy and strategy.[170] Although this has had some implications for the command and control of the UK's nuclear weapons,[171] the UK retains the authority to use its nuclear forces without the requirement to consult NATO Allies when 'supreme national interests are at stake'.[172] Moreover, the UK's peacetime nuclear policy means that nuclear warheads are not preassigned to any targets (such as cities); hence the command and control relationship between the UK and NATO in the current structure is relatively loose.[173] The UK is not reliant on the US Global Positioning System (GPS) for navigational purposes[174] to launch nuclear missiles, given that Trident D5 missiles are believed to operate with precision guidance by astro-inertial navigation system instead.[175]

As previously noted, one method by which communications with the submerged submarines take place is through the use of VLF transmissions.[176] The primary means by which these communications are reportedly transmitted is through the VLF transmitter at the Skelton Transmitting Station, however the NATO Interoperable Submarine Broadcast System (NISBS) also

and House of Lords in recent years by Angus Robertson (Scottish National Party) and Lord Lee of Trafford (Liberal Democrats) respectively, but there has been no reaffirmation by members of sitting governments.

[167] Gower, J. (2019), *United Kingdom: Nuclear Weapon Command, Control, and Communications*.

[168] Ibid.

[169] Hutchinson, R. (2004), *Weapons of Mass Destruction: The No-Nonsense Guide to Nuclear, Chemical and Biological Weapons Today*, London: Weidenfeld and Nicolson.

[170] Smith, M. A. (2011), 'British nuclear weapons and NATO in the Cold War and beyond', *International Affairs*, 87(6), p. 1391, https://doi.org/10.1111/j.1468-2346.2011.01042.x (accessed 10 Oct. 2019).

[171] Davis, I. (2015), *The British Bomb and NATO: Six decades of contributing to NATO's strategic nuclear deterrent*, Stockholm International Peace Research Institute, https://www.sipri.org/sites/default/files/files/misc/NATO-Trident-Report-15_11.pdf (accessed 10 Oct. 2019).

[172] UK Ministry of Defence (2005), *Response to Freedom of Information Request About the UK Nuclear Deterrent*, https://ams3.digitaloceanspaces.com/ukdj/2017/12/UK-Nuclear-Deterrent-FOI-Response.pdf (accessed 10 Oct. 2019).

[173] Smith, M. A. (2011), 'British nuclear weapons and NATO in the Cold War and beyond', p. 1399.

[174] Defence Nuclear Organisation, Ministry of Defence (2018), 'The UK's nuclear deterrent: what you need to know'.

[175] Keller, J. (2018), 'Draper Lab to upgrade inertial guidance units on Trident submarine-launched nuclear missile systems', *Military & Aerospace Electronic*s, 2 March 2018, https://www.militaryaerospace.com/computers/article/16726450/draper-lab-to-upgrade-inertial-guidance-units-on-trident-submarinelaunched-nuclear-missile-systems (accessed 17 Feb. 2020); Missile Defense Project, 'Trident D-5 at a Glance' (2016), Missile Threat, Center for Strategic and International Studies, https://missilethreat.csis.org/missile/trident/ (accessed 17 Feb. 2020).

[176] VLF transmitters are used for communications with submarines. See Meredith, N. P., Horne, R. B., Clilverd, M. A., Ross, J. P. J. (2019), 'An investigation of VLF transmitter wave power in the inner radiation belt and slot region', *Journal of Geophysical Research: Space Physics*, 124(7), pp. 5246–5259, http://nora.nerc.ac.uk/id/eprint/522480/ (accessed 17 Feb. 2020).

provides alternative routes by which to transmit messages.[177] Should an attack take place on the Skelton Transmitting Station, or should it for whatever reason be rendered inoperable, measures exist by which to maintain the lines of communication between the prime minister and the submarines.

Despite assurances made by the then UK defence secretary Sir Michael Fallon that the Vanguard fleet of submarines 'operate in isolation when they are out on patrol',[178] and are thus less likely to be affected by cyber operations, it is possible for systems on board the submarines to be compromised or hacked at alternative stages. While on patrol, the Vanguard submarines' systems are largely isolated from the internet and civilian networks, and this does reduce the opportunities available to aggressors. Attack vectors do still exist, but these are more likely to be exploited during construction or maintenance phases, when new software and/or hardware are installed while the submarine is ashore.[179] As such, it would be unwise to consider the submarines as being completely insulated against cyberattacks, given the various stages at which systems could be compromised, spoofed or hacked – whether at an early stage in the supply chain, or during routine maintenance and upgrades.

France

In March 1966, in a letter to US President Lyndon Johnson, President Charles de Gaulle declared his intention to withdraw France from the NATO integrated military command structure.[180] This decision was reversed in 2009,[181] but to date France does not participate in the NATO Nuclear Planning Group.[182] France's nuclear doctrine applies a principle of strict autonomy and sufficiency. In the view of many experts, by intending to maintain an independent nuclear force, France deliberately complicates the deterrence calculations of the adversary; thus, the Alliance supports the French nuclear policy.[183] A future study of adversaries' views on this matter could shed valuable light on the effectiveness of this policy. The French nuclear stockpile is stated to be kept always at the lowest level possible 'compatible with the strategic context'.[184] At present, France sustains capabilities to operate and launch nuclear strikes in two domains: in the air and at sea. The nuclear

[177] Ainslie, J. (2005), *The Future of the British Bomb*, London: WMD Awareness Programme, p. 85; Plesch, D. and Ainslie, J. (2016) *Trident: Strategic Dependence & Sovereignty*, SOAS University of London, https://www.soas.ac.uk/cisd/news/file114165.pdf (accessed 10 Oct. 2019).
[178] Johnston, I. (2017), 'Defence Secretary unable to deny Trident nuclear submarines run on same outdated software hackers exploited to cripple NHS systems', *Independent*, 14 May 2017, https://www.independent.co.uk/news/uk/home-news/nuclear-submarines-windows-xp-ransomware-wannacry-wanna-defender-michael-fallon-defence-secretary-a7734966.html (accessed 10 Oct. 2019).
[179] Abaimov, S. and Ingram, P. (2017), *Hacking UK Trident: A Growing Threat*.
[180] See France in NATO (2017), 'Archive – Letter from President Charles de Gaulle to President Lyndon Johnson on France's withdrawal from the NATO command structure (March 7 1966)', https://otan.delegfrance.org/Archive-Letter-from-President-Charles-de-Gaulle-to-President-Lyndon-Johnson-on (accessed 20 December 2019).
[181] NATO (undated), 'France and NATO', https://www.nato.int/cps/en/natohq/declassified_160672.htm?selectedLocale=en (accessed 20 December, 2019).
[182] Ibid.
[183] Tertrais, B. (2019), *French nuclear deterrence, policy, forces and future*, Fondation pour la Recherche Stratégique, Recherches & Documents N. 01/2019, p. 45, https://www.frstrategie.org/web/documents/publications/recherches-et-documents/2019/201901.pdf (accessed 20 Dec. 2019).
[184] France (2010), *Nuclear disarmament: France's practical commitment*, Working paper submitted by France, 2010 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, NPT/CONF.2010/WP.33, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/315/33/PDF/N1031533.pdf?OpenElement (accessed 7 Aug. 2019).

weapons possessed by France at present are exclusively of a strategic nature, [185] although in the past France developed short-range ballistic missiles capable of delivering a nuclear payload, such as Pluton and Hadès.[186] The Gendarmerie de la sécurité des armements nucléaires, part of the Gendarmerie Nationale (a branch of the armed forces under the authority of the ministry of the interior), is responsible for the oversight, monitoring and control of nuclear stockpiles to ensure their readiness at all times.[187]

The president is the sole holder of the authority to order the launch of nuclear weapons. In addition to the president, the prime minister and the ministry of defence take part in the decision-making process.[188] Moreover, chief of defence staff (CEMA), chief of the presidential military staff (CEMP), and Nuclear Forces Division of the Defence Staff (EMA/FN) play a role in the execution of the order. The president may give the order from the Jupiter Command Post located within the premises of the Élysée Palace, or from a mobile command post when the president is travelling.[189] The order goes to CEMA, who has to verify the order, lay out a plan, and execute it. The transmission between the president and CEMA goes via an operational facility, the Centre opérationnel des forces nucléaires.[190] The message is transmitted via the RAMSES strategic and survival meshed network.[191] RAMSES has been undergoing a series of expansions (RAMSES IV is the latest version), and it is 'hardened and protected against electromagnetic waves'[192] – presumably to be hardened against an electromagnetic pulse (EMP) attack. Should the RAMSES network be unavailable or destroyed, the SYDEREC system (système de dernier recours) will be used as a last resort measure to ensure the transmission of nuclear orders made by the president.[193] The SYDEREC system[194] uses 'antennas supported by inflatable balloons, carried by mobile vehicles'.[195] Creating multiple pathways and capabilities in the decision-making process indicates considerations of redundancy throughout the communications systems, which reduces the risk of failure in case of a system shutdown.

[185] Boulaud, M., Pintat, X., Chevènement, J., Demessine, M., Durrieu, J., Gautier, J., Gournac, A., Larcher, G. and Piras, B. (2012), 'L'avenir des forces nucléaires françaises', Rapport d'information N° 668, Sénat, Session Extraordinaire de 2011-2012, https://www.senat.fr/notice-rapport/2011/r11-668-notice.html (accessed 7 Aug. 2019).
[186] See Federation of American Scientists (2000), 'Pluton', https://fas.org/nuke/guide/france/theater/pluton.htm (accessed 7 Aug. 2019); and Missile Defense Project (2018), 'Hadès', Missile Threat, Center for Strategic and International Studies, https://missilethreat.csis.org/missile/hades/ (accessed 7 Aug. 2019).
[187] Gendarmerie nationale, 'La gendarmerie de la sécurité des armements nucléaires', https://www.gendarmerie.interieur.gouv.fr/Notre-institution/Nos-composantes/Gendarmeries-specialisees/Gendarmerie-de-la-securite-des-armements-nucleaires-Gsan (accessed 7 Aug. 2019).
[188] Tertrais, B. (2019), *French nuclear deterrence, policy, forces and future*, p. 20.
[189] Vie Publique (2017), 'Comment le président de la République peut-il déclencher le "feu nucléaire" ?', https://www.vie-publique.fr/questions/comment-president-republique-peut-il-declencher-feu-nucleaire.html (accessed 7 Aug. 2019).
[190] Guisnel, J. and Tertrais, B. (2016), *Le Président et la Bombe: Jupiter à l'Elysée*, Paris: Odile Jacob.
[191] Tertrais, B. (2019), *French nuclear deterrence, policy, forces and future*.
[192] Pelopidas, B. (2019), *France Nuclear Command, Control and Communications*, NAPSNet Special Reports, https://nautilus.org/napsnet/napsnet-special-reports/france-nuclear-command-control-and-communications/ (accessed 17 Dec. 2019); and Guisnel and Tertrais (2016), *Le Président et la Bombe*, pp. 247–299.
[193] Ibid., p. 71.
[194] The SYDEREC system replaced ASTARTE, an aerial transmission system with very low frequency transmitters in C-160 Transall aircrafts with built-in resilience against electromagnetic pulses. See Association Nationale des Forces Aériennes Stratégiques (2014), *La Revue Forces Aériennes Stratégiques 50 Ans*, Agence Kas Editions, http://anfas.fr/contact/revue-50ansfas.pdf (accessed 7 Aug. 2019).
[195] See Lewis and Tertrais (2019), *The Finger on the Button*, p. 17; and Guisnel, J. and Guerric, P. (2017), 'Si Emmanuel Macron devait appuyer sur le bouton …', *Le Point*, 16 September 2017, https://www.lepoint.fr/societe/si-emmanuel-macron-devait-appuyer-sur-le-bouton-16-09-2017-2157505_23.php (accessed 7 Aug. 2019).

Currently, through the HERMES programme, France is modernizing various nuclear transmission components, which rely on a network of infrastructures.[196] Under this programme, the TRANSOUM (transmission des sous-marins) programme is dedicated to the modernization of transmissions at sea, while TRANSAERO is responsible for the modernization of means of communications in the airborne component – both related to nuclear deterrence and operations.[197]

On airspace control, France currently uses a mobile long-range air defence 3D radar system (Ground Master 406), which may possibly detect cruise missiles.[198] Two of these systems were delivered in French Guiana and Nice in 2014 and 2017 respectively, and one was reported to be operational as of 2019 in Lyon;[199] and it has been suggested that these radars could be linked to NATO's Air Command and Control System or to the mobile component of the French Système de commandement et de conduite des opérations aérospatiales (command and control system of operations in aerospace).[200] As a mobile system, Ground Master 406 would have greater protection (compared with fixed radar systems) against physical attacks at time of conflict. However, these systems may still be vulnerable to cyberattacks. Hence, radar systems many not be truly survivable in conflict, and satellite communications should always accompany them as a redundancy measure.

The 2018 Military Planning Act[201] reiterates France's strategic priorities for 2019–25, based on the 2013 White Paper, and sets the financial framework to put in place and operationalize the measures envisaged under the legislation. The act notably provides for an increase in the allocated budget for the armed forces, including to update existing operational capabilities, supporting national and

[196] Boulaud, Pintat, Chevènement, et al. (2012), 'L'avenir des forces nucléaires françaises', p. 15.
[197] Sénat (2018), 'Projet de loi de finances pour 2018 : Défense : Équipement des forces', https://www.senat.fr/rap/a17-110-8/a17-110-811.html (accessed 7 Aug. 2019).
[198] Armée de l'Air (2017), 'Inauguration d'un nouveau radar de défense aérienne, le GM 406', 26 October 2017, https://www.defense.gouv.fr/air/actus-air/inauguration-d-un-nouveau-radar-de-defense-aerienne-le-gm-406 (accessed 12 Aug. 2019); and Armée de l'Air (2014), 'Un nouveau radar pour la Guyane', 3 December 1014, https://www.defense.gouv.fr/air/actus-air/un-nouveau-radar-pour-la-guyane (accessed 11 Jul. 2020). France used to invest in space-based early warning systems that could identify ballistic missile launches during their boost phase: its SPIRALE (Système Préparatoire Infra-Rouge pour l'Alerte) demonstrator military programme was dedicated to enable the development of an early warning system based on two microsatellites, both equipped with an infrared camera, as well as a ground segment for satellite control and for image processing. See: eoPortal Directory, 'SPIRALE (The French Spaceborne Early Warning Demonstrator) Mission', https://directory.eoportal.org/web/eoportal/satellite-missions/s/spirale (accessed 7 Aug. 2019). SPIRALE partly aimed to respond to the need initially stipulated by the French 2008 White Paper for an early detection and warning capability by 2020. See: Ministry of Defence (2008), *Défense et la Sécurité nationale, Le Livre Blanc*, Government of France, p. 183, https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341.pdf (accessed 12 Aug. 2019). The programme enabled the collection of infrared images to foster understanding in physics necessary for the development of future early warning systems. See Gautier, J., Pintat, X. and Reiner, D. (2011), 'La défense antimissile balistique : bouclier militaire ou défi stratégique ?', Rapport d'information n°733, Sénat, Session Extraordinaire de 2010-2011, https://www.senat.fr/rap/r10-733/r10-733.html (accessed 12 Aug. 2019). It has however been recognized, due to technical and financial considerations, that a space-based early warning system will not be operational by 2020 (as initially stated in the 2008 White Paper); and this system may require partnerships with other European countries – notably with Germany and Italy, for which steps have already been taken.[198] In addition, the French ministry of the armed forces is currently undertaking research on low-frequency ballistic missile early warning radar systems with the démonstrateur de radar très longue portée (DRTLP), codeveloped by ONERA and Thales, for which a technology demonstrator has been shipped and for which tests have already begun in southwest France. See Tran, P. (2018), 'France tests radar to detect and track ballistic missiles, satellites', *Defense News*, 23 March 2018, https://www.defensenews.com/intel-geoint/sensors/2018/03/23/france-tests-radar-to-detect-and-track-ballistic-missiles-satellites/ (accessed 12 Aug. 2019).
[199] Galland, P. (2019), 'Dans les coulisses des galeries souterraines de l'armée de l'air au mont Verdun', *Le Progrès*, 5 January 2019, https://www.leprogres.fr/rhone-69-edition-villefranche-et-beaujolais/2019/01/05/on-vous-raconte-ce-qu-on-a-vu-dans-les-galeries-souterraines-du-mont-verdun-ou-se-trouve-l-armee-de-l-air (accessed 11 Jul. 2020).
[200] Armée de l'Air (2017), 'Inauguration d'un nouveau radar de défense aérienne, le GM 406'.
[201] Journal Officiel de la République Française (2018), 'Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense', https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037192797&categorieLien=id (accessed 7 Aug. 2019).

European strategic autonomy as well as for research and development. Article 5 covers the increase in the armed forces human resources planned for the period to 2025, notably to underpin the prioritization of information and cyberdefence issues, as well as to address the vulnerabilities of command and control systems.[202]

The issue of the cybersecurity of command, control and communications systems has been officially recognized as a potential threat to nuclear deterrence both from a technical and a doctrinal perspective, as set out for instance in a 2017 Senate report.[203] Cyber operations could disable or enable C3 systems that would ultimately either prevent the use of nuclear forces or to cause unintentional/accidental use.

[202] République Française, Ministère des Armées (2018), *Projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense*, https://www.defense.gouv.fr/content/download/523151/8769287/file/LPM%202019-2025%20-%20Projet%20de%20loi.pdf (accessed 7 Aug. 2019).
[203] Pintat, Lorgeoux, Trillard and Allizard (2017), *La nécessaire modernisation de la dissuasion nucléaire*.

Appendix II: Nuclear Sharing

The concept of nuclear sharing was developed during the Cold War as a means by which to both improve the Alliance's readiness to respond to attack from the USSR and provide a more comprehensive deterrent. By the 1950s, the US had deemed that the only feasible way in which to counter the conventional threat posed by the USSR in Europe was to station nuclear weapons throughout Western Europe.[204] This led to the first nuclear weapons being stationed in Europe in September 1954; however, it is recorded that non-nuclear components, including bomb casings or assembles, were transported to the UK as early as 1950.[205] Subsequently, the US has stationed nuclear weapons throughout Europe. The exact numbers are not known, but experts have estimated current stockpiles as detailed in the table below.[206]

Airbase	Location	Operated by	2019 estimated stockpiles
Aviano	Italy	NATO (US)	25–35 US non-strategic B-61 gravity bombs
Ghedi Torre	Italy	Italy	20 US non-strategic B-61 gravity bombs
Büchel	Germany	Joint: US & Germany	10–20 US non-strategic B-61 gravity bombs
Volkel	Netherlands	Netherlands	10–20 US non-strategic B-61 gravity bombs
Kleine Brogel	Belgium	Belgium	10–20 US non-strategic B-61 gravity bombs
Incirlik	Turkey	Turkey	50 US non-strategic B-61 gravity bombs

As the table above identifies, the US currently has solely B-61 gravity bombs at the listed airbases. These bombs are stored in an underground weapon security and survivability system (WS3),[207] with electronic monitoring and control units that include sensors, electronic-data transmission units, motion detectors, video cameras, etc. At the depths of the Cold War, these numbers were greater and additional airbases also served as host to US nuclear weapons.[208] While the US has provided

[204] Alberque, W (2017), *The NPT and the origins of NATO's nuclear sharing arrangements*.
[205] Norris, R. S, Arkin, W. M. and Burr, W. (1999), 'Where they were', *Bulletin of the Atomic Scientists*, 55(6), pp. 26–35, https://www.archives.gov/files/declassification/pidb/meetings/where-they-were.pdf (accessed 6 Oct. 2019).
[206] Data gathered from Nuclear Threat Initiative (2019), 'Nuclear Disarmament Italy', https://www.nti.org/analysis/articles/italy-nuclear-disarmament/ (accessed 10 Oct. 2019); Nuclear Threat Initiative (2019), 'Nuclear Disarmament Germany', https://www.nti.org/analysis/articles/germany-nuclear-disarmament/ (accessed 10 Oct. 2019); Nuclear Threat Initiative (2019), 'Nuclear Disarmament Netherlands', https://www.nti.org/analysis/articles/netherlands-nuclear-disarmament/ (accessed 10 Oct. 2019); Nuclear Threat Initiative (2019), 'Nuclear Disarmament Belgium', https://www.nti.org/analysis/articles/belgium-nuclear-disarmament/ (accessed 10 Oct. 2019); and Nuclear Threat Initiative (2019), 'Nuclear Disarmament Turkey', https://www.nti.org/analysis/articles/turkey-nuclear-disarmament/ (accessed 10 Oct. 2019). Hans Kristensen also highlights similar numbers; although he makes a precise estimate, stating that in Belgium, Germany, Italy and Netherlands there are 20 B61 bombers. See Kristensen, H. M. (2019), 'U.S. Nuclear Weapons in Europe', Briefing to the Center for Arms Control and Non-Proliferation, Federation of American Scientists, 1 November 2019, https://fas.org/wp-content/uploads/2019/11/Brief2019_EuroNukes_CACNP_.pdf (accessed 25 Dec. 2019).
[207] The US calls this system a Weapon Storage and Security System.
[208] Kristensen, H. M. (2005), *U.S. Nuclear Weapons in Europe: A Review of Post-Cold War Policy, Force Levels, and War Planning*, Natural Resources Defense Council, https://www.nrdc.org/sites/default/files/euro.pdf (accessed 10 Oct. 2019).

the munitions, the host states have been responsible for the vehicles to deliver the payloads, which includes their maintenance. This again contributes to the sharing of the burden among NATO member states; this element of the agreement has presented challenges, which will be considered later.

From the early 1960s, codified nuclear sharing agreements between NATO members began to develop in order to govern the use of these weapons, beginning with the establishment of consultation procedures, which have their roots in the revision of the NATO doctrine under then US Secretary of Defense Robert McNamara.[209] Given the highly confidential and sensitive nature of this process, publicly available information on how this consultation takes place, and by what means, is rather limited. However, one of few resources in the public domain notes that the entire request and release sequence would take 24 hours when accounting for transmission of request.[210] While the technology used for the purpose of conveying commands has developed significantly throughout subsequent decades, reducing the time required in order to relay messages, open source material provides interesting insights into the procedures involved in the approval of a nuclear mission from a host state. Of particular note is that, notwithstanding the purpose of the consultation process to allow for the possibility of a host or potentially affected state to veto the use of nuclear weapons, this consultation process has historically been established to take place 'time and circumstances permitting'.[211] This proviso serves to undermine the basis of the consultation process, rendering it non-mandatory and opening the possibility that it could be bypassed in conditions in which time frames are often compressed. However, and regardless of the consultation process, nuclear host countries have been part of the NPG, and in practical terms control of the military bases that weapons would deploy out of are under their control, so they can veto at the planning stage on a scenario basis and can in practice prevent a decision if they really wanted to. On balance, therefore, the use of nuclear weapons by host countries without US consent is in all probability the most concerning scenario, rather than vice versa.

Nuclear sharing was primarily developed as a means by which to share the burden of maintaining the NATO nuclear deterrent among Alliance members.[212] As part of these agreements, US nuclear weapons have been hosted within the various member countries, remaining in the custody of the US until required for missions, at which point custody and responsibility would be transferred to the host nation for delivery.[213] This also serves as the means by which NATO member states that do not possess nuclear weapons are able to host them without contravening the nuclear Non-Proliferation Treaty (NPT), as they remain, according to NATO, in the 'absolute control and

[209] Charles, D. (1985), 'Who controls NATO's nuclear weapons?', *Bulletin of the Atomic Scientists*, 41(4), pp. 45–48, doi: 10.1080/00963402.1985.11455949 (accessed 10 Oct. 2019).
[210] Kelleher, C. M. (1987), 'NATO Nuclear Operations', in Carter, A. B., Steinbruner, J. D. and Zrakat, C. A. (eds) (1987), *Managing Nuclear Operations*, Washington, DC: Brookings Institution, p. 457; Ball, D. 'Controlling Theatre Nuclear War', *British Journal of Political Science*, 19(3), p. 320, https://www.jstor.org/stable/193844 (accessed 25 Dec. 2019).
[211] Charles (1985), 'Who controls NATO's nuclear weapons?'.
[212] Chalmers, M. (2009), 'NATO's Nuclear Weapons: An Introduction to the Debate', in Chalmers, M. and Lunn, S. (2009), *NATO's Tactical Nuclear Dilemma*, Royal United Services Institute, pp. 1–5, https://rusi.org/sites/default/files/201003_op_natos_tactical_nuclear_dilemma.pdf (accessed 10 Oct. 2019).
[213] King, J., Lindborg, C. and Maxon, P. (2008) *NATO nuclear sharing: Opportunity for change?* BASIC Getting to Zero Papers Number 9, pp. 1–2, https://basicint.org/wp-content/uploads/2018/06/gtz09_0.pdf (accessed 10 Oct. 2019).

custody'[214] of the nuclear weapon states of the Alliance during peacetime, with transfer of control and custody undertaken solely at time of war.[215]

Partially in response to increasing political pressure from host states, not least arising from a series of near misses at the various European host sites,[216] 'dual key' arrangements were reportedly established to add an additional layer of security and to share the burden further. The dual key system requires the authorization of both the US and the host country in order for the weapons to be used.[217] This mechanism involves the incorporation of electronic locks, also known as Permissive Action Links (PALs),[218] which US personnel would have to deactivate prior to usage, after which point pilots from NATO host countries would have full control over the weapons until delivery.[219]

There are, however, numerous inherent challenges posed by the maintenance of these nuclear sharing agreements that, together, constitute security concerns deserving of consideration. As part of the nuclear sharing agreements between the US and host countries, 'custody, repair and improvements to the weapons and the storage bunkers are the responsibility of the U.S. Air Force', whereas 'perimeter security (fences, monitors, and motion detectors) and access to the storage sites is the responsibility of the host nation'.[220] This complicates matters, as the maintenance of both is essential to the secure storage and security of the weapons; however, as the arrangement seems to exist, the US and the host state are reliant on each other to uphold their respective commitment. Such circumstances can be detrimental to ensuring the safety and security of holding weapons in host states, as detailed in the US Department of Defense's Blue Ribbon Report released in 2008.[221] Notably, standards in both personnel and physical security measures were found to vary across the different host bases; and the 'host nation support to maintain security infrastructure at nuclear-capable units' was stated to remain an issue, with most in need of resources to meet the US Department of Defense security requirements.[222] The US has limited scope to ensure that efforts are made to ameliorate such security threats beyond investing in modernizing these facilities and

[214] NATO (2017), *NATO and the Non-Proliferation Treaty*, NATO, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170323_170323-npt-factsheet.pdf (accessed 10 Oct. 2019).
[215] See King, Lindborg and Maxon (2008), *NATO nuclear sharing: Opportunity for change?* However, this argument has been subject to continued contest on the grounds that the mere hosting of nuclear weapons in fact serves to contravene the NPT. See also:Spagnuolo, L. (2011), *NATO's nuclear Posture and Burden Sharing Arrangements: an Italian perspective*, BASIC, https://basicint.org/wp-content/uploads/2018/06/report_from_roundtable_doc_0.pdf (accessed 10 Oct. 2019).
[216] See Schlosser, E. (2013), *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety*, New York: Penguin Books.
[217] Williams, I. and Andreasen, S. P. (2015), 'The Future of NATO's Nukes', Hoover Institution, 25 March 2015, https://www.hoover.org/research/future-natos-nukes (accessed 6 Oct. 2019); Linne, R. L (1994), *The History of NATO TNF Policy: The Role of Studies, Analysis and Exercises Conference Proceedings*, Livermore: Sandia National Laboratories, https://inis.iaea.org/collection/NCLCollectionStore/_Public/26/072/26072023.pdf (accessed 10 Oct. 2019).
[218] Kristensen (2005), *U.S. Nuclear Weapons in Europe: A Review of Post-Cold War Policy, Force Levels, and War Planning*.
[219] Sechser, T. S. (2016), 'Sharing the bomb: how foreign nuclear deployments shape nonproliferation and deterrence', *The Nonproliferation Review*, 23(3–4), pp. 443–458, doi: 10.1080/10736700.2016.1259062 (accessed 10 Oct. 2019).
[220] Remkes, R. C. N. (2011), 'The Security of NATO Nuclear Weapons: Issues and Implications', in Andreasen, S. and Williams, I. (eds) (2011), *Reducing Nuclear Risks in Europe: A Framework for Action*, Nuclear Threat Initiative, pp. 66–75, https://media.nti.org/pdfs/NTI_Framework_Chpt3.pdf (accessed 10 Oct. 2019).
[221] Peyer, P. A. (2008), *Air Force Blue Ribbon Review of Nuclear Weapons Policies and Procedures*, Headquarters U.S. Air Force, https://fas.org/nuke/guide/usa/doctrine/usaf/BRR-2008.pdf (accessed 10 Oct. 2019).
[222] Ibid., pp. 50–52.

encouraging the host state to take the necessary security measures, thus exerting pressure on the sharing agreements.[223]

Concerns over the physical security of nuclear weapons hosted in Europe have been exacerbated in recent years by a combination of increasing regional instability in Europe and its near-neighbourhood, combined with the actions of non-state armed groups and paramilitary groups.[224] It has been reported that the commander of the Incirlik Air Base was involved in the attempted coup in Turkey in 2016, and that the Turkish authorities cut off the power supply to the base in order to reduce the risk of conspirators using the facility.[225] Officials and experts raised both safety and security concerns over Incirlik Air Base after this incident, as the US nuclear weapons had to rely on back-up power for a period of five days after the coup attempt was discovered. It had already been acknowledged in the early 2000s that there was a growing likelihood of a terrorist attack against a European NATO base hosting nuclear weapons;[226] and this concern has latterly been fuelled by recent actions by Islamic State of Iraq and Syria (ISIS). Following the terrorist attacks in Paris and Brussels in late 2015 and early 2016, it emerged that ISIS operatives had been observing nuclear facilities in Belgium, leading to increased concerns that the group was aiming to target nuclear facilities and potentially acquire nuclear materials.[227] This intelligence served to heighten existing concerns (including in the US government) over the security of nuclear sites in Belgium, which once more underscores the inherent vulnerabilities that exist as a result of NATO's nuclear sharing agreements and the delegation of responsibility for ensuring that facilities are secure. The possibility of cyber intrusion into the nuclear enterprise also remains as a possibility, especially considering that Iranian civil nuclear centrifuges were affected by a malware (Stuxnet) in 2010,[228] and that the US has reportedly infiltrated the North Korean ballistic missile system and caused failures during the testing stage.[229]

When NATO's nuclear sharing agreements were first established, the threat landscape was dramatically different compared with that of the present day. Adversaries and the nature of threats have changed, as have theatres of warfare, as technological advancements have contributed towards new military approaches. These changes have led to reconsideration of the necessity of hosting US

[223] Other studies have also indicated that American bases within the US also face similar challenges. See Lewis, P., Aghlani, S., Pelopidas, B. and Williams, H. (2014), *Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy*, Chatham House Report, London: Royal Institute of International Affairs, https://www.chathamhouse.org/publications/papers/view/199200 (accessed 10 Oct. 2019).
[224] Remkes (2011), 'The Security of NATO Nuclear Weapons: Issues and Implications'.
[225] Borger, J. (2016), 'Turkey coup attempt raises fears over safety of US nuclear stockpile', *Guardian*, 17 July 2016, https://www.theguardian.com/us-news/2016/jul/17/turkey-coup-attempt-raises-fears-over-safety-of-us-nuclear-stockpile (accessed 25 Dec. 2019).
[226] Ibid.
[227] Rubin, A. J. and Schreuer, M. (2016), 'Belgium Fears Nuclear Plants Are Vulnerable', *New York Times*, 25 March 2016, https://www.nytimes.com/2016/03/26/world/europe/belgium-fears-nuclear-plants-are-vulnerable.html (accessed 10 Oct. 2019).
[228] Broad, W., Markoff, J. and Sanger, D. (2011), 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', *New York Times*, 15 January 2011, https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (accessed 20 Jun. 2020).
[229] Gartzke, E. and Lindsay, J. (2017), 'The U.S. wants to stop North Korean missiles before they launch. That may not be a great idea', *Washington Post*, 15 March 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/03/15/the-u-s-wants-to-stop-north- korean-missiles-before-they-launch-that-may-not-be-a-great-idea/ (accessed 1 Dec. 2019); Gartzke, E. and Lindsay, J. R. (2017), 'Thermonuclear cyberwar', *Journal of Cybersecurity*, 3(1): pp. 37–48, https://doi.org/10.1093/cybsec/tyw017 (accessed 11 Jul. 2020).

nuclear weapons in Europe,[230] as well as of the existing nuclear sharing agreements.[231] In particular, such reconsideration has been motivated by concerns over legacy infrastructure, not least in a context in which treaties are being abandoned, and nuclear infrastructure is being modernized with digital means, increasing the attack vector for cyberattacks.[232] Presently, it is believed that Incirlik Air Base in Turkey, which is estimated to host around 50 US B-61 bombs, does not have permanent nuclear-capable aircraft (F-16s) and is thus unable to carry out joint nuclear missions at short notice, as envisaged under NATO nuclear sharing agreements.[233] This has been complicated further by the recent removal of Turkey from the F-35 joint strike fighter programme as a result of its interest in purchasing the Russian S-400 air defence system.[234] The F-35 had been intended to replace the previous nuclear-capable aircraft in Turkey; however, the US raised concerns over the capability of the Russian-developed air defence system to collect stealth information on the F-35. In particular, concerns have centred on the potential connectivity between the S-400 and the F-35's Autonomic Logistics Information System (ALIS), which is core to operating it with a global fleet understanding.[235] As such, this overlapping of C4ISR systems could provide unprecedented access to a host of sensitive information. At present, it appears that remaining nuclear-capable F-16s that are currently stationed at other airbases (Balıkesir and Akıncı) throughout Turkey would need to be used in order for Turkey to remain actively involved in the delivery of the weapons stationed at Incirlik.[236] This complicates the timeline of deciding, planning and preparing for a tactical nuclear operation from Turkey,[237] reducing the credibility of nuclear deterrence provided by the host country.

Taken together, these developments will likely provoke questions over the sustainability of the nuclear sharing agreement between the US and Turkey. It will also raise questions as to what type of cybersecurity arrangements exist between the host country and the US in order to protect the airbases in Europe against threat. Moreover, considering that most of the nuclear weapons have been in the European territory for several decades, their modernization has been in discussion within the US. Although modernization is fundamentally important for nuclear safety, it carries cybersecurity risks (e.g. new digital components integrated to legacy systems, patching, etc.) that should not be underestimated.

[230] Varialle, C. (2015), *Tactical Nuclear Weapons, NATO and Deterrence: Are NATO's TNW actually a threat to the credibility of its own deterrence?*, BASIC, https://www.basicint.org/wp-content/uploads/2018/06/tnw-nato-deterrence-cvarriale-nov2015.pdf (accessed 10 Oct. 2019).
[231] King, Lindborg and Maxon (2008), *NATO nuclear sharing: Opportunity for change?*.
[232] Erlanger, S. (2019), 'Are We Headed for Another Expensive Nuclear Arms Race? Could Be.', *New York Times*, 8 August 2019, https://www.nytimes.com/2019/08/08/world/europe/arms-race-russia-china.html (accessed 10 Oct. 2019).
[233] Street, T. (2018), *NATO Nuclear Sharing*, Org Explains #5, Oxford Research Group, https://www.oxfordresearchgroup.org.uk/Handlers/Download.ashx?IDMF=0eb97254-e224-4afe-af4e-220ad435e881 (accessed 10 Oct. 2019).
[234] Mehta, A. (2019), 'Turkey officially kicked out of F-35 program, costing US half a billion dollars', *Defense News*, https://www.defensenews.com/air/2019/07/17/turkey-officially-kicked-out-of-f-35-program/ (accessed 10 Oct. 2019).
[235] Kasapoğlu, C. (2019), 'Turkey and Nuclear Command, Control and Communications', NAPSNet Special Reports, https://nautilus.org/napsnet/napsnet-special-reports/turkey-and-nuclear-command-control-and-communications/ (accessed 10 Oct. 2019).
[236] Ibid.
[237] Ibid.

Appendix III: Control Deficiencies and Vulnerabilities

In March 2018 the US Department of Defense Inspector General released a report on logical and physical access controls at Missile Defense Agency contractor locations,[238] based on a performance audit conducted in March–December 2017. The publicly available report sets out some of the audit's findings, but does not disclose the name and location of the seven contractor facilities assessed. The report identifies a set of control deficiencies and vulnerabilities that may have security implications with the potential to affect the security and credibility of the US's ballistic missile defence systems on which NATO may rely upon both for defence and deterrence purposes.[239] Below is the summary of control deficiencies identified in the published report and their subsequent potential security implications based on the report's analysis:

Control deficiencies/vulnerabilities	Potential security implications
Multifactor authentication was not consistently used	• Provides more opportunity for unauthorized access to internal networks (and the data/information they contain) – whether remotely or not. • Eases the task of unauthorized third parties wishing to access internal networks: the lack of multifactor authentication means that they could potentially obtain access by only obtaining a personal identification information (e.g. password, which may be obtained by phishing or password spraying methods) without protection from additional layers of security (e.g. a physical token or card).
System passwords were not always strong	• Eases the obtaining of passwords (e.g. through phishing methods), unauthorized access to data and the information system/network infrastructure, and data theft (and potential disclosure). • A low standard of password complexity requirement may further exacerbate problems from the lack of consistency in multifactor authentication.
Contractors did not periodically conduct system risk assessments	• Lack of awareness of potential existing vulnerabilities. • Lack of awareness of the systems and network architecture's survivability and resilience.
Network and system vulnerabilities were not consistently mitigated	• Vulnerabilities may increasingly affect networks and potentially hardware (including new ones) the longer they remain. • Absence of cybersecurity culture: fosters a passive, underestimating attitude towards cyber vulnerabilities.
No oversight of third-party service provider's network protection activities	• Existing vulnerabilities in third-party service provider's network due to a lack of protection may be used as an entry point for malicious cyber operations.

[238] Inspector General, U.S. Department of Defense (2018), *Logical and Physical Access Controls at Missile Defense Agency Contractor Locations*.
[239] Ibid., pp. 4–21.

	• These vulnerabilities could also result in unintentional cyber disruptions due to negligence/failure of these third parties to adopt proper measures to protect the network and hardware.
Contractor allowed users to process and store unclassified controlled technical information on personal electronic devices	• Potential data theft, disclosure and dissemination outside of internal/authorized networks/devices. • Lack of oversight over data once stored on personal electronic devices. • Personal electronic devices may not be subject to the same security standards as the contractor's systems.
Removable media were not properly protected	• Unauthorized access to computer systems and internal networks. • Theft of data (including technical information/specifications of systems under the Missile Defense Agency). • Intentional or unintentional dissemination of (concealed) malware in systems containing BMDS technical information, which could potentially result in the disabling and/or destruction of software and/or hardware (e.g. complete wipe-out of data, modification or destruction of a computer system's or network's architecture).
Systems did not automatically lock after inactivity or unsuccessful login attempts	• Absence of automatic lock after inactivity may give unauthorized access to non-authorized third parties. • Potential absence or inaccuracy of logs/monitoring of failed login attempts.
System access and user privileges were not consistently granted	• Access to and theft of classified information, including technical information. • Lack of clarity on the classification of information.
System activity reports were not properly maintained and reviewed	• Inability to detect/monitor failed login attempts and possible data exfiltration attempts. • Lack of traceability: may hinder investigations and solving of malfunctions/suspected malicious activities,

Acronyms and Abbreviations

ACO	Allied Command Operations
ACT	Allied Command Transformation
ALCS	airborne launch control system
ALIS	Autonomic Logistics Information System
ALTBMD	Active Layered Theatre Ballistic Missile Defence
AMN	Afghanistan Mission Network
APT	Advanced Persistent Threat
BMDS	ballistic missile defence system(s)
BMEWS	Ballistic Missile Early Warning System
C2	command and control
C3	command, control and communication
C3I	command, control, communication and intelligence
C4ISR	command, control, communication, computers, intelligence, surveillance and reconnaissance
CEMA	Chef d'état-major des armées (chief of defence staff)
CEMP	Chef de l'état-major particulier du président de la République (chief of the presidential military staff)
COM JFAC	Joint Force Air Component Commander
DoD	United States Department of Defense
DOT&E	Director, Operational Test and Evaluation
DSP	Defense Support Program
FMN	Federated Mission Network
GAO	Government Accountability Office
GNSS	global navigation satellite systems

GPS	Global Positioning System
ICBM	intercontinental ballistic missile
IHL	international humanitarian law
ISIS	Islamic State of Iraq and Syria
ISR	intelligence, surveillance and reconnaissance
JISR	Joint Intelligence, Surveillance and Reconnaissance
LANDCOM	Allied Land Command
MARCOM	Allied Maritime Command
MDA	Missile Defense Agency
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NC3	nuclear command, control and communication
NCI Agency	NATO Communications and Information Agency
NIAMD	NATO integrated air and missile defence
NNSA	National Nuclear Security Administration
NPT	Treaty on the Non-Proliferation of Nuclear Weapons
PNT	position, navigation and timing
RAMSES	réseau amont maillé stratégique et de survie (strategic and survival network)
SACEUR	Supreme Allied Commander Europe
SACT	Supreme Allied Commander Transformation
SHAPE	Supreme Headquarters Allied Powers Europe
STRIKFORNATO	Naval Striking and Support Forces
SYDEREC	système de dernier recours (system of last resort)
TDL	tactical data links

About the Authors

Yasmin Afina is a research assistant with the International Security Programme at Chatham House, working on projects related to nuclear weapons systems, emerging technologies including cyber and artificial intelligence, and international law. She formerly worked for the United Nations Institute for Disarmament Research and the United Nations Office for Disarmament Affairs. Yasmin holds an LLM from the Geneva Academy of International Humanitarian Law and Human Rights, and an LLB from the University of Essex, as well as a bachelor's and postgraduate degree in international law from the Université Toulouse I Capitole. She is also a PhD candidate in law at the University of Essex, researching the role of reliability in assessing the legality of artificial intelligence use for military targeting.

Calum Inverarity is a research analyst and coordinator with the International Security Programme at Chatham House. His work focuses primarily on conflict prevention and resolution, including the role of governance in facilitating these processes. He formerly worked with the Bruegel economic think-tank, and with the Democratic Progress Institute and UN House, Scotland. Calum holds an MSc in conflict resolution and governance from the University of Amsterdam, and a BA in international development and international relations from the University of Leeds; as part of his studies, he also spent time at the University of California, San Diego and the University of Ghana.

Dr Beyza Unal is a senior research fellow with the International Security Programme at Chatham House. She specializes in nuclear and cyber policies, conducting research on cybersecurity and critical national infrastructure security and cybersecurity of nuclear weapons systems. Dr Unal also conducts research on urban preparedness and city resilience against CBRN threats. She formerly worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, taught international relations, transcribed interviews on Turkish political history, and served as an international election observer during the 2010 parliamentary elections in Iraq. Dr Unal is interested in NATO's defence and security policy as well as security in the Middle East, and has been given various fellowships for her achievements; most notably, she is a William J. Fulbright alumna. She has also received funding from the US Department of Energy to participate in workshops in Brookhaven National Laboratory, the James Martin Centre for Nonproliferation Studies, and Sandia National Laboratory.

Acknowledgments

The authors would like to thank Ploughshares Fund and the Stanley Center for Peace and Security for their funding and support of this research project. In particular, we appreciate the contributions of Ben Loehrke to this research, and his trust in our work.

Many other people have contributed to this project. We express gratitude to all the participants who attended our research workshop on the topic in 2019. Particular thanks go to Patricia Lewis, Philip Reiner, Andrew Futter and Jamie Shea, among many others. We received valuable feedback from anonymous peer reviewers, whose opinions we have incorporated as far as possible. Finally, many thanks go to the Chatham House publications team for their work with us on this paper.

Independent thinking since 1920

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical including photocopying, recording or any information storage or retrieval system, without the prior written permission of the copyright holder. Please direct all enquiries to the publishers.

Chatham House does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author(s).

Copyright © The Royal Institute of International Affairs, 2020

Cover image: Control panels in an underground Launch Control Center outside Great Falls, Montana, on 1 July 2018.

Photo credit: Copyright © The Washington Post/Getty Images

ISBN 978 1 78413 414 3

This publication is printed on FSC-certified paper.

FSC

Typeset by Soapbox, www.soapbox.co.uk

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223