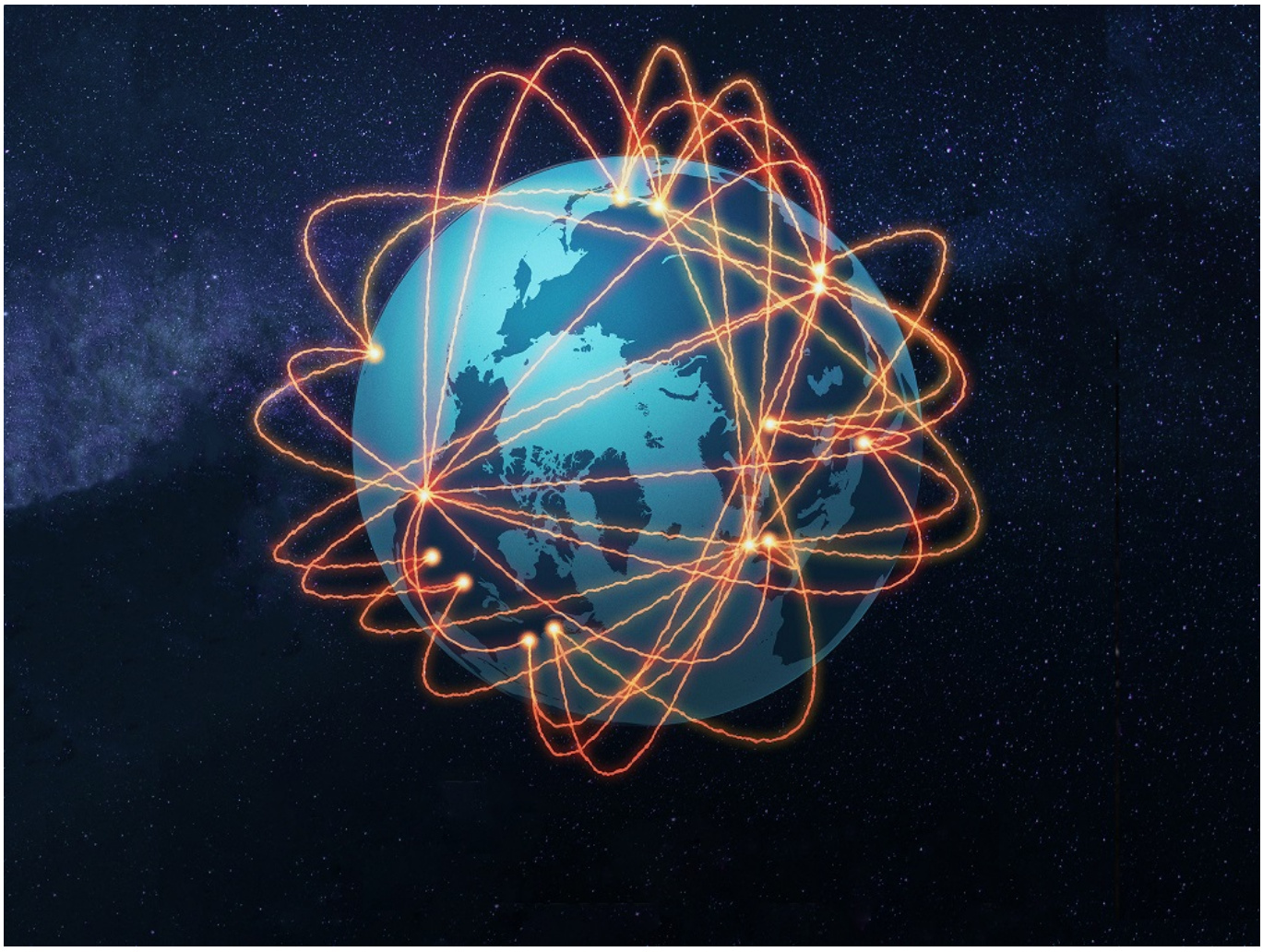
SYNTHESIS REPORT–NC3 SYSTEMS AND STRATEGIC STABILITY: A GLOBAL OVERVIEW



Recommended Citation

Peter Hayes, Binoy Kampmark, Philip Reiner, Deborah Gordon, "SYNTHESIS REPORT–NC3 SYSTEMS AND STRATEGIC STABILITY: A GLOBAL OVERVIEW", NAPSNet Special Reports, May 05, 2019, https://nautilus.org/napsnet/napsnet-special-reports/synthesis-report-nc3-syste-s-and-strategic-stability-a-global-overview/

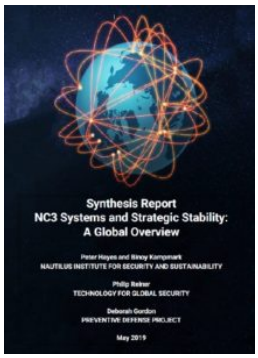
PETER HAYES, BINOY KAMPMARK, PHILIP REINER, DEBORAH GORDON

MAY 5 2019

I. INTRODUCTION

This essay is the Synthesis Report of a workshop of fifty NC3 experts held at the Hoover Institution at Stanford University on January 22 to 23, 2019. Nine states have nuclear weapons and fourteen states have nuclear command, control, and communications (NC3) systems. How multiple nuclear-armed states interact in nuclear-prone conflicts is poorly understood. National NC3 capabilities are technically dissimilar and operate in different governance and cultural systems. Of note, there are no common standards of NC3 performance. Additionally, the impact of NC3 systems on the risk of nuclear war in regional flashpoints is a new factor in the decisions of the global nuclear weapons states. How NC3 operates in this new complexity, including how new technologies such as social media, quantum computing, cyberwarfare, autonomous vehicles, and artificial intelligence affect "legacy" NC3 systems and organizations, are urgent questions for researchers and practitioners alike. The Synthesis Report also suggests possible NC3 communication, cooperation, and collaboration measures between NC3 operators and practitioners, and the involvement of nuclear weapons, nuclear umbrella, and non-nuclear weapons states as a way to reduce the risk of nuclear war. It will be followed by the publication of 29 NC3 specialist papers.

The report may be downloaded **here** (PDF, 1.3MB)



Acknowledgments: The workshop was funded by the John D. and Catherine T. MacArthur Foundation.

This report was prepared by staff of Nautilus Institute, Preventive Defense Project, and Technology for Global Security. It is published simultaneously here by Technology for Global Security and here by Nautilus Institute and is published under a 4.0 International Creative Commons License the terms of which are found here.

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

Copy editing by Maureen Jerrett and workshop participants.

Banner image is by Lauren Hostetter of Heyhoss Design.

II. NAPSNET SPECIAL REPORT BY PETER HAYES, BINOY KAMPMARK, PHILIP REINER, DEBORAH GORDON

SYNTHESIS REPORT--NC3 SYSTEMS AND STRATEGIC STABILITY: A GLOBAL OVERVIEW

MAY 5 2019

Contents

1. Executive Summary

Today, nine states have nuclear weapons and fourteen states have nuclear command, control, and communications (NC3) systems. How multiple nuclear-armed states interact in nuclear-prone conflicts is poorly understood. National NC3 capabilities are technically dissimilar and operate in different governance and cultural systems. Of note, there are no common standards of NC3 performance. Additionally, the impact of NC3 systems on the risk of nuclear war in regional flashpoints is a new factor in the decisions of the global nuclear weapons states. How NC3 operates in this new complexity, including how new technologies such as social media, quantum computing, cyberwarfare, autonomous vehicles, and artificial intelligence affect “legacy” NC3 systems and organizations, are urgent questions for researchers and practitioners alike.

A two-day gathering held at the Hoover Institution at Stanford University on January 22 to 23, 2019, explored these challenges. It featured intense discussions based on readings and presentations by practitioners, academics, experts, and opinion-makers with specific skill-sets across relevant fields. A standout feature of the gathering was the cross-section of participants who would otherwise not typically converge in discussions, confined, as they are, to their specialist fields (nuclear technology, politics, history, law, engineering, computer science, and security). The gathering sought to engage, interrogate, and explore pathways and approaches to the issues of NC3 from multiple perspectives.[1] The conveners of the workshop were the Nautilus Institute for Security and Sustainability, the

Preventive Defense Project (Stanford University), and Technology for Global Security.

The workshop was conducted under the Chatham House Rule[2] which is observed throughout this synthesis report. This report provides an overview of discussions over the two-day workshop. The papers presented at the workshop will be published in the coming months (listed in Appendix B) and will expand on many of the issues summarized in this report. The report is prepared by the rapporteur and the conveners who are solely responsible for its content.

The following observations and conclusions were made:

- NC3 systems, not only but notably the US NC3 system, require urgent Given the aging of NC3 infrastructure, there is pressure to build new systems before current systems are irreparable or are surpassed by emerging counter-NC3 threat capabilities.[3]

  > The NC3 modernization challenges, however, differ among nuclear weapons states. The United States has a vast array of decades-old legacy systems. China, in contrast, is integrating 21st century technology into a much simpler baseline NC3 architecture, without the magnitude of hindrances facing the US modernization effort. Both efforts, from opposite ends of the spectrum, present differing challenges to NC3 stability and effectiveness. Others – for instance the DPRK architecture – are hard to assess due to inscrutability and uncertainty, although the workshop benefited from informed analysis.

- A global perspective is essential. The historical Soviet-US stability paradigm on the subject of NC3 from the Cold War provides much insight and many lessons learned, not least of which is that the adversary always "gets a vote" in matters of strategic nuclear deterrence. However, NC3 in all nuclear weapons states must be considered in light of modern challenges to NC3, new technologies, and other effects of a multipolar environment with nine nuclear weapons states (each with their accordant NC3 differences and complexities). Workshop participants accepted that this new terrain is vastly challenging.
- A truly global approach demands the compilation and comparison of updated profiles of national NC3 systems. There are no less than fifteen NC3 systems to study. Of these, ten were covered in the workshop. In each case, multiple dimensions need to be characterized, including the role played by non-state actors, and the various technical, cultural, sociological, and institutional matters that govern the way these systems work – and potentially interact at the moment of crisis. Because most NC3 researchers come from outside the systems in question, their analytic claims are necessarily modest due to the secrecy and sensitivity associated with command, control, and communications systems. Conversely, open sources and freedom of information data are still indispensable in developing systematic and global approaches to comprehending the development and implementation of NC3 systems. Such independent and wide-ranging analysis had major policy impact during the Cold War (see Appendix A). It is critically important that such intellectual foment and discovery recur in the next round of NC3 implementation and learning by architects, engineers, commanders, and policy practitioners.
- NC3 systems face common problems – some are shared and shareable matters. The risk of systems failure can be reduced by joint data exchange, establishing links between the national NC3 systems, and confidence building measures. Provision of NC3 assistance by nuclear weapons states to other states, however, is problematic, limited by such instruments as the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). Permissive Action Links, or PALs, were a possible cooperation measure at various times. But discussants suggested that attempts by the United States to share PAL technology with the former Soviet Union during the Cold War, and then subsequently between the United States and Russia, did not succeed. Even talking about such

sharing is blocked since Moscow's annexation of Crimea in 2014, along with its continued modernization of non-strategic nuclear systems and capabilities. It is in the US national interest to address the NC3 problem in such a way that it could assist other nuclear weapons states to also strengthen their own NC3 systems. A separate conversation was also expressed on PALS and how these might be shared in order to increase the resilience and system safety for other nuclear weapons states.

- Although some NC3 matters were considered specific to the United States given the sheer number of systems at play, certain cross domain realities (for instance space, quantum, and cyber technologies) must be considered in the global discussion. These factors could, in turn, alter how NC3 systems and operations are understood in other states. Indeed, to the extent that less developed NC3 systems are rendered less capable or more vulnerable by adversarial acquisition and deployment of such technologies, these factors are as or even more salient to other, less capable NC3 operators and states. Having such discussions has the potential to avoid needless replication and bad practices at the national level on the one hand, and to open up opportunities for collaboration and cooperation where required on the other.
- Other fields of operation involving large-scale networks and supporting command-and-control, sensor, and communication systems, can also shed light in terms of lessons learned and possible alternative design and management practices for NC3, be it in decision-making and operational matters in conventional military systems, disaster management protocols, electricity grid management, and specialist agencies accustomed to operating under extreme conditions of stress (for example, US NASA).
- Complexity is increasing, within and among NC3 systems. A strong theme that surfaced throughout the workshop was the role of complexity: complexity in terms of decision-making; complexity in terms of weapons systems; and complexity in terms of operational matters that might lead to mistakes (broken arrows, accidental launches, and so forth). NC3 systems may need to be simplified to avoid accidents/accidental use, particularly at the moment of crisis when resilience is most salient (from a survival but also a deterrence perspective).
- Emerging technologies may be disrupting and already turning some existing NC3 systems topsy-turvy. Hypersonic weapons, quantum computing, cyber capabilities, and "artificial intelligence" (AI) were seen as simultaneously promising and problematic, possibly stabilizing NC3 systems and thereby deterrence in some respects, yet exposing them to novel vulnerabilities and potential failures in respect to others. The use of such technologies might, for example, cause problems in terms of information and digital systems security, counterfeit information (false strikes), spoofing of interpretation and decision support systems, and
- The relationship between NC3 systems and international law is an important and urgent area for improvement and dialogue. The laws of war regarding proportionality, an obligation to disobey unlawful orders, and limits on targeting all apply to NC3 systems.

The workshop concluded with a wide-ranging discussion of the need for focused follow-up research, for international collaboration and information sharing, and for actuating cooperation mechanisms between NC3 operators in practical ways. Although all participants recognized the sensitive and difficult nature of this latter imperative, everyone also concurred that undertaking this task was a critically important next step.

In addition to recognizing the need for more attention on information systems and flows in NC3 systems, the workshop highlighted – but did not address in depth – the implications of the possible demotion of assured immediate response that likely would follow from a thorough recasting of the functional requirements for NC3. In particular, this discussion focused on the almost certain

demotion of maintaining a launch-under-attack posture, except in circumstances of sustained crisis (that is, discounting bolt-out-of-the-blue scenarios as realistic). Qualitative investigation of assuring effective aids to decision making, no longer overwhelmingly driven by simplistic force-o--force military considerations, also bears further consideration in all NC3 systems. Given the history of near misses, and the anecdotal evidence relating to commander irrationality at various historical moments, the urgency of reconsidering the viability of single-person nuclear commands, with little to zero deliberation, consultation, or checks and balances, was also noted as needing immediate policy attention.

Accordingly, this workshop report and the papers following it are the first, not the last word on NC3 and strategic stability from a global perspective. Rapid follow-up is imperative as national decisions are being made that will have impacts for decades. NC3 decisions made today will reverberate not only in force postures and structures, but will also shape how nuclear commanders manage their nuclear forces routinely and at the brink of war. Informal communication and dialogue between scholars, practitioners, and policy makers from the fourteen NC3 systems in operation today may be a constructive first step to ensuring that NC3 contributes to rather than undermines global strategic stability.

2. Introduction

This synthesis report is structured around the following themes. First are the importance and necessity of NC3 systems. Second are factors that determine the performance and effects of these systems. Third is the role of emerging technologies (prospects and dangers), the cybersecurity challenge, the challenges posed by increasingly complex systems, followed by possible improvements to NC3 and specific country discussions. Fourth are decision-making models considered in deliberations followed by the legal aspects of NC3 systems. Fifth, and finally, is the potential for collaboration and sharing of NC3 technologies and practices that would enhance global stability, lessons-learned, and possible conclusions drawn from a global approach.

3. Critical Issues

This section examines nine critical NC3 issues. These are necessity, system performance, dogmas, cyber dimensions, complexity, needed improvements, country-level observations, command authority, and legal dimensions.

3.1 NC3: Its necessity

A consensus emerged at the outset, at the most senior level, that the use of nuclear weapons remains untenable, and that nuclear war should never be fought, as it could never be won. Paul Bracken’s sagacious insight was reiterated on the importance of understanding processes and systems that would prevent unnecessary catastrophic use of nuclear weapons in a crisis: “Dangerous issues are just below the surface, latent and contingent. The skin of civilization is exceedingly thin. We don’t see this because we worry about the kids, traffic, trade conflicts, and budgets. But if a severe nuclear crisis or a war developed, nuclear issues are not far away. They can come back in a flash if conditions change. So it’s a good time to think about these matters, when we are not in a mass panic or open psychoses of rage and revenge.”[5]

To that end, it is imperative that NC3 systems today be made reliable, robust, and capable for the same reasons adduced by Ashton B. Carter in 1985, viz, that systems for command, control, communications, and intelligence are as important in deterring nuclear strike and escalation as nuclear weapons or strategic doctrine.[6] In effect, the US Department of Defense’s (DOD) recent declaration that NC3 is a weapon system in its own right makes it clear that it is a virtual fourth leg

to the US nuclear triad. Those charged with direct involvement with NC3 systems noted that, from a military perspective, a country will always strive to respond to perceived threats by acquiring the most capable NC3 system. It is primarily for politicians and diplomats to change the threat; the military could merely prepare for those threats.

That NC3 systems are indispensable to the avoidance of nuclear conflict, whether through enhanced deterrence effects or other control reasons, surfaced throughout the workshop discussions. Classic literature in the field remains pertinent.[7] The continued importance of NC3 systems in specific conflict relationships loaded with nuclear threat has also been acknowledged by current practitioners and in academic literature.[8] Everyone recognizes that risks can only be minimized, never eliminated, and that those risks that do eventuate into contingencies must be managed – but doing so relies on commanders having competent NC3 systems to support them. In addition to the requisite hardware in a given state, the knowledge of past practices, errors, and failures of NC3 systems is itself a form of threat mitigation. Thus, provision to NC3 operators and commanders of a "worst practice guide" may improve command and control design, coping with insider threats, errors, preventing and dealing with, for example, broken arrows, irrational behavior, and accidents. German Chancellor Otto von Bismarck was quoted by one participant: "Only a fool learns from his own mistakes. The wise man learns from the mistakes of others." In short, we do not do nearly enough to share our experiences of failure in the no-fail context of NC3, within or among NC3 operators. Although this reluctance to admit to past failures or share information about super-sensitive systems is understandable, updated baseline understanding of the state-of-the-art and the complexity involved among nine nuclear weapons states, including historical documentation of the many still secret NC3 misadventures in at least some, and most likely in all, nuclear weapons states would be a major contribution to mutual NC3 learning in the new area of nuclear-geopolitical competition.

A historical overview was thus also provided in each national NC3 profile. In the case of the United States, it emerged that a period of low morale and dispiritedness followed the end of the Cold War, such that by 2010, US NC3 capabilities in some legs of the triad had atrophied and even failed. But in recent years, US nuclear forces have returned to high levels of confidence and morale. This shift is observable from the attitudes of those at bomber and submarine bases. Such motivation is fundamental in ensuring the safety and security of nuclear weapons.

However, the resurgent geopolitical competition and nuclear threat projection has reinstated stress on NC3 systems that almost disappeared at the end of the Cold War. This trend is particularly pronounced in Russia-US relations since Moscow's annexation of Crimea in 2014 and Russia's continued modernization of non-strategic nuclear systems and capabilities announcing its return to great power competition. China's aspirations to regain a global centrality adds further stress to the system of interlocking NC3 systems at a global level. NC3 systems are a crucial dimension of the risk-taking behavior by Pakistan, India, and North Korea in recent years. Some of these conflicts are now multipolar in ways that further complicate NC3 operations.

3.2 NC3: System, health, stability

The challenges facing NC3 today differ from those associated with maintenance of strategic stability during the Cold War. Threats have diversified (multiple adversaries, non-state actors), and the very concept of stability is less meaningful today than it was during the Cold War. New epistemological and conceptual challenges have emerged. During the course of all sessions, the workshop strove to piece together the elements necessary to build and maintain well-functioning and adaptive national NC3 systems in this global context.

US NC3 practitioners, for example, emphasized the importance of secure and reliable NC3 systems,

including the fact that security is built into the weapons systems – and into command, control, and communications – thereby enabling US STRATCOM to know where US nuclear weapons are, and the conditions for their deployment. It was remarked that a weapons *system* includes not only the nuclear warhead and related hardware. It constitutes all the elements that enable a weapon to be deployed, including appropriately trained personnel, parts, and the systems that allow an NC3 apparatus to work all the way from commander to weapons operator. The fit between the weapon and the NC3 system is never perfect. Nonetheless, it was argued that it was important to see NC3 as a system, not simply disparate parts. As one experienced NC3 practitioner suggested, doing so entails eliminating "stupid things" and "building" the right people and motivations into the NC3 system while holding them accountable. Rather than striving for perfection – perhaps an error made in a number of NC3 systems – it may be more important to understand imperfectability, the role of human error, and the need to have accountability and secure systems to deal with nuclear safety and security to constantly improve performance. Many observations were made relating to understanding error as a constructive theme. To have safe, secure, and reliable systems entails having appropriately trained personnel; but as people are distinctly imperfect, safeguards against mistakes are indispensable.

Undoubtedly, each NC3 system must be safe and secure if they are to underwrite risk and create stability between states. But to this absolute requirement must be added the importance of trust in avoiding catastrophic behavior. Building trust has become far more challenging today. Not only is modern technology used by state actors inherently unreliable in some respects compared to legacy technology. It also processes and communicates information that is itself increasingly of dubious quality. Software permits the building of systems of seemingly unlimited complexity, but it was reiterated time and again that "complexity is the enemy of security." Indeed, catastrophic accidents, it was emphasized, can still occur in cases where nothing actually failed in the components of a system or its operation.[9] Conversely, the exact meaning of simplicity – and what types of simplicity are helpful as against anathema – might be built into a modernized NC3 system – remain to be defined in each national NC3 context.

A range of indicators were deemed important to determining the "health" of an NC3 system. The first entails the need for operational sensing and reporting if there is a system failure in the NC3 system of nodes, processors, and supporting networks. There is an inherent need here for enhanced modeling and simulation of system performance and failure pathways as well as mining historical data. In fact, the view was expressed that it may shock many outsiders the extent to which this modeling capability does not already exist for current NC3 systems. Trend reporting has also been incorporated into the system – which can potentially be facilitated by novel technological means (but comes with the inherent flaws and vulnerabilities mentioned above).

Governance matters are also critical in terms of dealing with prioritization problems – but governance in the US NC3 system – and likely in many others – has to date remained an afterthought, although this situation is currently in the process of being addressed in the United States.

Finally, modernization efforts, in terms of acquisition, documentation, and necessary training for the use of new systems can be taxing at many levels and in many dimensions of implementation, including organizational stress, budget competition, and in managing nuclear deterrence itself due to the impact of modernization efforts on adversarial perceptions. That is, NC3 modernization itself may be a risk factor to be conceptualized, managed, and minimized.

3.3 NC3: Dogma and danger in technology

The nature of 21st century technological change and the extent to which technology determines the effectiveness of NC3 systems in the face of certain change was discussed at some length. Placing bets on technology may be advantageous in terms of the edge it might bring or the speed it may provide relative to adversaries, but it is also dangerous in light of inherent vulnerabilities created by the introduction of the new technology. Quantum communications, for example, might well have strengths – it might, for instance, offer "perfect crypto" – yet undermine the security of less capable nuclear adversaries who may then undertake offsetting, risk-tolerant measures to overcome the perceived vulnerability. There might also be problems of future proofing the system against decryption.

The discussion of China's NC3 infrastructure was heavily tinged with warnings. China's NC3 upgrades rely heavily not only on first-wave "informatization" but also on early introduction of novel technologies such as AI and quantum computing/communications – in many ways a "bottom-up" process. This was contrasted with efforts to upgrade or replace legacy systems in the United States, which also require modernization given their Cold War vintage – a "top-down" process. To that end, it was considered a possibility that the PRC could be more eager to explore new options and technologies, with heavy reliance on technologies such as AI and quantum computing, without a clear sense of the potential vulnerabilities and complexities that follow in their wake. There is already evidence that China is using these technologies for intelligence fusion, data integration, and the pursuit of better and faster remote sensing. Although the use of certain new technologies might be empowering, perhaps even stabilizing in some instances, they might also have the opposite effect. Machine learning, for example, remains untested "in the wild" for the most part, nascent and vulnerable to exploitation of weaknesses and unpredictable outside testing environments. It is unclear whether the PRC has entirely embraced full automation in military thinking, a Russian-style Dead Hand equivalent, or an automated perimeter.

That more powerful technologies might lead to broader vulnerabilities was a recurring theme. Although this theme touched on a range of points, there was no unified or clear set of relationships between them. The risk of accidents was held to remain possible, maybe even enhanced as a result of new technologies, despite the prospect that enhanced NC3 might strengthen strategic stability due to augmented capabilities to conduct data processing, analysis, and early warning. One perspective was that advances in AI, 5G, quantum computing, and big data are all highly likely to revolutionize military affairs as a matter of course, irrespective of NC3 effects. Another loud warning was also expressed many times: be wary of the abundant hyperbole regarding the value of AI. For the foreseeable future, fields such as AI will likely still need to involve some human agency, and that human role will come loaded with its attendant issues. The unavoidable conclusion for nuclear commanders from all these considerations is that they are currently unable to fully understand how their existing system, let alone their future systems, actually work due to these disparate elements; and their NC3 adversaries are unlikely to be in a better position.

The dangers posed to NC3 structures by the entanglement of conventional and nuclear C3, and the concurrent problem of dual-use systems and technologies, were also examined in-depth. Although the risks of such entanglement have existed for decades, increased reliance on technologies such as hypersonic glide vehicles, for example, could introduce new challenges for determining whether a nuclear or non-nuclear attack was being initiated – on short time scales previously unimaginable.

3.4 NC3: Cyber security

The NC3 community, it was urged in the workshop, should view cybersecurity not merely from the perspective of deterrence and its concurrent benefits, but from the dangers it poses to NC3 systems

as a whole. Cyber vulnerabilities specifically pertaining to NC2 matters is something that causes a loss of sleep for many participants, recognized as something distinctly outside their "comfort zone." Cyber-compromised or mal-designed software in early warning systems could mischaracterize an attack, misrepresent launches, disrupt launch systems, or cause nuclear weapons (or entire weapons systems) to simply fail. In not so reassuring fashion, it was remarked that few experts within the government security community in Washington, D.C., really understand the depth and breadth of NC3 and cyber-related problems (outside those deeply ensconced in those roles). Much of this could be put down to the structural impediments placed on sharing information. Offensive and defensive functions, for example, are and will remain classified – but also stove-piped. This compartmentalization has a perverse result: those engaged in tasks related to matters of cyber-offense are not always or wholly able to access information regarding those dealing with cyber-defense and *vice-a-versa*. Although deployment of nuclear weapons in response to cyber-attack as suggested in current US declaratory policy seems disproportionately dangerous, the question of whether it *might* happen in certain, precarious circumstances was left open as a serious potential reality – with open-ended implications for NC3 vulnerability and capability.

3.5 NC3: Complexity as a problem

The role of complexity was a recurrent theme in the workshop dialogue. This included complexity in terms of decision-making, complexity in terms of weapons systems, and complexity in terms of operational matters that might lead to mistakes. One participant expressed concern, in fact terror, that NC3 modernization might so increase complexity as to compromise a nuclear weapon state's security. British computer scientist Tony Hoare was cited: "There are two ways of constructing a software design: One way is to make it so simple that there are obviously no deficiencies, and the other way is to make it so complicated that there are no obvious deficiencies. The first method is far more difficult."[10] Adds Hoare, "The price of reliability is the pursuit of the utmost simplicity."[11]

Although these notions were not originally made in the military context, they have direct applicability to the NC3 "modernization" trajectory for nuclear weapons states in the 21st century – that is, dependence on increasingly software driven enterprise systems of increasing complexity and interdependence.

In line with Hoare's remarks, some argued that agencies such as the US DOD have begun to adopt cheap shortcuts while also building in unnecessary complexity in the NC3 domain – as in many other weapons systems. Conversely, it was noted that the United States had been successful in depending on simple and very clever NC3 solutions, using conservative engineering techniques. Indeed, a "faddish" approach to "sexy" alternatives has taken root in systems development involving "agile" development, rapid fielding, and cutting out of layers of testing. None of these fads are new, but they are no less dangerous today – and possibly more dangerous now that they may affect NC3 modernization. Thus, a paradigmatic shift in engineering solutions in the manner envisaged by Thomas Kuhn is needed, even if individuals or agencies are reluctant to embrace it.[12] Given that this complexity problem is systemic, one cannot decompose systems nor simplify them in a way that was previously possible. A top-down approach and system-wide approach is required to avoid stirring a witch's broth of complexity.

Thus, it was a relief to hear that NC3 modernization need not necessarily imply increasing levels of complexity. The notion was introduced and seized the attention of many participants that it is entirely feasible to build radically simpler systems. These would allow nuclear commanders, including the US President, to communicate with nuclear forces and issue commands to the battle field, even while under nuclear assault. Vast budgets and acquisitions inertia can encourage

complexity; it requires extraordinary management effort not to fall into that trap.

NC3 modernization also entails generic problems in the US DOD acquisition process. DOD's 5000 acquisition regime was offered as an example. The dual-use aspect of NC3 systems, notably in the United States, also encourage complexity (see the entanglement argument made above, as well). Although disentanglement of nuclear and conventional C3 systems is unlikely, there being good reasons not to separate these functions from a deterrence and defense perspective at the national level, certain structural features of NC3 could be designed to prevent complexity from becoming a clear threat to security and stability itself. But such design and engineering must be done most likely not at the acquisition stage but at the prior stage of developing requirements and the derivative research and development process. A focus on simpler NC3 systems from get-go is likely desirable – not *simple* in terms of their makeup, but *simpler* to build, understand, upgrade, and protect. By way of observation, it was suggested that striving to develop and deploy an NC3 system designed to be capable of delivering all functions to all users, with the same terminals and platforms for all users, is bound to create problems.

The FAB-T (Family of Advanced Beyond Line-of-Sight Terminals) is a case in point. The FAB-T was designed to permit US nuclear commanders to supply protected, survivable communication terminals for strategic and joint tactical airborne command and control (C2) for both nuclear and non-nuclear operations using Extremely High Frequency (EHF), wideband, protected, and survival communication terms for beyond line-of-sight communications as an "essential component of the strategic nuclear execution system."[13] Various problems of complexity were subsequently noted by DOD reviewers, including the writing of 1.3 million lines of code between 2002–2010 and over a hundred anomaly reports.[14] A subsequent evaluation report revealed that software problems prevented the receipt of nuclear emergency action messages, and some messages received had corrupted content.[15]

3.6 NC3: Improvements

The broader theme of how improvements to NC3 systems may deter nuclear strike and prevent escalation received much consideration. It was generally agreed that this had to happen across the board, and that it was particularly urgent for the United States to consider modernization of its NC3 platforms. Given the aging of many elements of the NC3 infrastructure, there is an urgent temporal imperative to build new systems before current systems could no longer be repaired or are outstripped by threat capabilities.

On several occasions over the two days, it was remarked that the security environment is increasingly dynamic. New NC3 systems in the United States should be more disaggregated and less dual-use (as noted above). It was held that improved communications to the US President, and survivable communication links, beyond exploitation by adversaries and able to operate in extreme conditions, require patience, time, and significant investment to develop and deploy. This cannot be done in a rush, no matter how much money or personnel are thrown at the problem.

Some suggested that systems had to be designed on the assumption that "bad guys" are likely already inside it and that counter-NC3 operations, especially digital ones, are constantly shifting in a never ending, 24/7 contest for the foreseeable future. Countervailing this porosity will necessitate removal of organizational stovepipes, expert surveillance, and an enduring necessity for "Silicon Valley" types to be involved. Notions of "hacking for good" or a bottom-up approach and bringing in expertise from outside the traditional military and security fold were floated as a means of bringing grassroots innovation into the NC3 system. However, IT security practitioners suggest that only

continuous and high-level commitment by highly trained professionals will suffice to contain cyber threats in the NC3 system. Care must be taken if doing so, and there was a sense that the necessary level of caution might not be exercised in all nuclear weapons states and their NC3 systems.

The workshop also discussed the nature of decision-making. The issue of false positives was discussed anew, with reference to Bayesian analysis, a statistical paradigm that seeks to answer research questions regarding unknown parameters using statements of probability. As Harry Harlem explains, "Bayesian inference offers a method to relate the conditional probability of a certain branch to the probabilities of other branches [in terms of future events]."[16] A False Positives Calculator was demonstrated at the workshop and the implications for decision-making of human propensity to underestimate the probability of false positives were considered.[17]

Looking at nuclear command and control alone was judged to be insufficient in dealing with instances of cross-domain failures. Decision-making processes from other fields, including their history and practice, might provide insights (see below). Conventional command and control options, and states using them, should also be added as a source of understanding and learning. In Israel, for example, it is possible to speak about unauthorized activities in conventional military operations, but not in nuclear matters because of its policy of maintaining near opacity and studied ambiguity as to possession and deployment of nuclear weapons. Some studies of US decision-making in the Iraq 2003 war and of the C3 problems in prosecuting that war have been completed, for example. However, the limited applicability of such studies on conventional warfare and C3, and the salience of this insight and experience to nuclear war and NC3, must be borne in mind.

Thinking more broadly, lessons from non-military fields might also be useful to consider in terms of a network's decision-making and survivability. Consideration might be given, for example, to tsunami warning systems. Fiber optic cables have been severed in massive earthquakes, precipitating a near loss of connectivity with sub-regional commands. Staff versed in extreme conditions and stresses – NASA staff for instance – might be consulted. NC3 and electric energy systems, it was noted, share a common threat in terms of risks posed by, for example, cyberattacks to control software. Connections might be made between those responsible for NC3 cyber-risk management and those working for the US president's infrastructure advisory council. Such systems are continuously performing at the highest level in a changing environment of increasing complexity. The same principle applies to possible discussions within and among NC3 operators and those striving to protect critical infrastructure in each nuclear weapons state.

3.7 NC3: Country-specific observations

The richness of global NC3 systems, the full understanding of which is modified by access to classified information and security restrictions, became clear in presentations, papers, and discussions at the workshop. It was also accepted that preventing potential NC3 mistakes and failures could not just be a matter for one state alone. US and Russian NC3 systems and conduct were premised on Cold War assumptions and the establishment of stabilizing norms from routine testing and crisis-driven learning. Their totally disparate, initially black box approaches in the nineteen fifties gave way to mature NC3 systems, with each system focused on rapid technological change, record keeping, gathering of information, and training of staff.[18]

Although this synthesis report canvasses various aspects of the US NC3 system throughout, many non-US country-specific attributes and issues were also presented in national NC3 profiles and discussion thereof. In particular, the role played by the executive and its direct control over nuclear deployment was discussed extensively. The pressing issue of modernizing legacy systems was also

considered in relation to each national NC3 system, along with its problems of complexity, as were emerging technologies such as cyber, quantum, and automation. Of course, the vast scope of US DOD-led NC3 modernization involving an NC3 enterprise architecture across domains (space, air, ground, and in the oceans) with global reach is distinctive, and far beyond the capacities of the other nuclear weapons states. Nonetheless, the US system needs a system-wide set of adjustments starting with a requirements definition, systems engineering, integration, acquisition, and budgeting.[19]

Discussion on Russia focused on advances in its BMEWS (Ballistic Missile Early Warning Systems) and its role in preserving national security and strategic stability. The system is based on algorithms that automatically interpret early warning sensor information, monitored by a human whose intervention is rarely needed to correct the automated systems. Accurate and rapid reporting requirements, and the synergistic integration of BMEWS with the Ballistic Missile Defense System and Space Surveillance System (SSS), were seen as essential in an informational and functional sense. Constant modernization of the system is also taking place, with the replacement of obsolete radars by the Voronezh type. The Drayal radar (Pechora) and Dnepr radar are also scheduled for replacement by Voroneg-M radars. The existing Oko system is slated for replacement by a prospective unitary space system. Remarks on the Russian BMEW system also pointed to potential malfunctioning from personnel error and interference from unresearched natural phenomena as yet unplugged into the algorithms and a lack of knowledge of ballistic missile capabilities of other states.

For the UK, its simplicity and uniqueness were emphasized on two points. First, its NC3 system focuses exclusively on submarine-launched ballistic missile systems and its processes on how to engage its nuclear deterrent. The authority to own, operate, and manage the UK nuclear deterrent resides in the Prime Minister's Nuclear Directive. The exercise of this authority, in turn, is supported by the UK Nuclear Deterrence Policy, owned by the Cabinet Office. Such weapons are only to be engaged as a matter of "last resort" – with a deterrent feature buttressed by a dormant directive letter that each prime minister authors to each ballistic firing nuclear submarine (SSBN) commanding officer. Its contents, only known to the prime minister, are to be revealed after the deployed submarine's commanding officer exhausts a series of complex processes. Secrecy on these protocols persists, but making command and control the preserve of the prime minister rather than any military wing is a singular feature.[20] The prime minister may nominate nuclear deputies, but the military has no formal role in this decision process.

Pakistan's NC3 system is beset by problems on nuclear management, starting first from a position of conscious strategic ambiguity about its nuclear weapons on the one hand, and the problems posed by poor civilian-military relations functioning in a volatile strategic environment on the other. Such relations are further complicated by tensions between the presidential and parliamentary system and the grant of *de facto* and *de jure* authority to Joint Staff Headquarters (JSHQ)/Strategic Plans Division (SPD) via the National Command Authority Act 2010 "on all matters nuclear." Doctrinally, Pakistan is dedicated to using its nuclear deterrent to offset Indian conventional superiority. The vulnerability of its nuclear forces, and a lack of real time surveillance, and early warning and acquisition, were deemed significant drivers of an imperative to risk early first use in a conflict with India. In the India-Pakistan context, the universal nuclear dilemma – that weapons must always work when directed and never when not – is integral to Pakistan's risk-taking deterrence doctrine. Its NC3 challenges arise foremost from the tension between maintaining central control (negative) and exercising pre-delegation (positive) to fielded nuclear forces. The risks of diplomatic fallout, loss of control due to procedural or technical error, or attack by non-state actors, and of Indian pre-emption after Pakistani forward deployment of nuclear weapons, are all too real.

Although Pakistani civilians have largely been excluded from its nuclear command system, in India, the military has usually felt excluded from this arena. This was not aided by the "opacity" of India's nuclear posture, the details of which are confined to a small number of senior civilian officials, officers in a dedicated Strategic Forces Command, and scientists.[21] To date, it has been accepted in such documents as the draft report on a nuclear doctrine and the formal official statement by India's cabinet committee on national security that "credible minimum nuclear deterrence" will be pursued. The draft nuclear doctrine insists on retaining sufficient, survivable, and operationally prepared nuclear forces; a robust command and control system; effective intelligence and early-warning capabilities; training and planning for nuclear operations; and the will to employ nuclear weapons when needed.[22] The 2003 official statement supplements the DND with a two-layered body known as the Nuclear Command Authority responsible for nuclear and missile arsenals: the Political Council, chaired by the prime minister, and the Executive Council, chaired by the national security advisor to the prime minister. Although the Political Council supposedly retains sole authority in authorizing the use of nuclear weapons, this position, as noted in the 2003 statement, is ambiguous: "arrangements for alternate chains of command for retaliatory nuclear strikes in all eventualities" also exist.[23]

In some cases, national NC3 systems may not be rigorously and constantly tested, and may not be coherent in practical performance under stress. Also, the systems may be insufficiently redundant, and may lack clear lines of responsibility and accountability in nuclear command and control. This latter set of concerns was specifically raised regarding the DPRK, though the riposte was made that the concern about who controls North Korean nuclear weapons is likely less worrisome than the fact that the DPRK lacks long-range early warning systems needed to reassure its leaders that a nuclear attack is not underway in times of tension. Caution on speculating too much on the DPRK command structure on the issue of nuclear security was also expressed. To consider such matters was akin to trying to understand what was in a black box.

Although not as inscrutable, similar concern was also expressed regarding France's nuclear decision-making, notably from the context of its alliance obligations and more general operational issues. This is compounded by the absence of a Freedom of Information Act and a February 2008 law intended to prevent the proliferation of nuclear weapons, enabling authorities to classify any information relevant to the production and handling of such weapons. Despite interlocking obligations with NATO, it remained unclear how the process would unfold in deployment decisions. A further issue with French nuclear practices centers on its descriptive claims on command and control practices versus its performative dimension. The latter is based on the credibility of a nuclear retaliation while allaying fears of accidental explosion, escalation, or nuclear strike caused by breach in the C2 protocol. The performative element limits what can be said descriptively in terms of flaws in the system.

China, in terms of command and control matters, was viewed as determined by the imperative of maintaining strict leadership control by the Chinese Communist Party. The politburo and the central military commission are the primary players, with nuclear forces being exclusively directed by the central commission. There was some disagreement on the issue of priorities – whether negative control remains privileged over survivability. As noted above, a technical dimension of auto-dispatch may be introduced soon into China's NC3 system similar to the use of semi-automated command systems in other nuclear weapons states. Communication would take place using radio and fiber-optic technologies, though other technologies – for example, satellite – are also being considered. The PLA Rocket Forces, formerly known as the Second Artillery, possess multiple redundant forms of communications between the units. The use of liaison officers, dispatched personally to units in the event of being cut off, is also an operational procedure that might come into play. Problems arise in the context of naval operations, and a shift from land-based rocket forces may well take place if

China arms its ballistic missile submarines in peacetime.

There was divergence on how to characterize some aspects of China's nuclear philosophy at the operational level. Commingling nuclear and conventional warheads on missiles, for example, may strive to create deliberate ambiguity to protect conventional missiles. This use of nuclear risk is an idea with some currency based on historical precedent, though workshop participants were not convinced that this rationale pertains today. In theory, China should have an overwhelming incentive to *not* co-locate nuclear and conventional capabilities because doing so can invite unwelcome attack. There was also a question of whether China's practice of separating warheads from deliverable missiles might continue. Putting warheads into separate storage away from missiles is "consistent with planning for a singular campaign intended to launch only a retaliatory strike"[24] which has different NC3 requirements from a more pre-emptively capable posture.

Different approaches and philosophies to the way nuclear assets are handled between security agencies were also compared. The Israeli approach here insists on keeping nuclear and military assets separate, an essential part of its organizational approach. The Israeli nuclear program is to be kept as civilian as possible – the primary domain of the prime minister and his associates – though there is probably a link to a national command center, with the caveat that these arrangements are hard to gauge. Outstanding questions remain on whether there is a full separation between nuclear and military assets and where this dichotomy fits with the state's nuclear-capable submarine capability. (For example, has the British approach for this set of issues been used by Israel in its SSBN deployments?)

Other states with various views and approaches to NC3 infrastructure are also significant, if rarely addressed by scholars or policy practitioners. Turkey is particularly interesting in terms of tactical nuclear weapons (TNW) deployment. Although the Turkish academic and specialist community has yet to establish war studies as a specific branch of study and research, and problems remain with open-source information on the strategic landscape, a few points can be noted. NATO tactical nuclear weapons deployment envisages support by Turkish forces for the presence of US B-61 nuclear bombs in the country, a stance some argue enables NATO to maintain ambiguity about how nuclear weapons might offset Russia's offensive strategic weapons programs centered on non-nuclear WMDs and ballistic missiles. Although control of the B-61 weapons resides with the United States, Turkey is responsible for the airbases and related facilities. In the past, the Turkish Air Force deployed dual-capable aircraft certified for tactical nuclear delivery.[25] Current practice on this remains unclear, however, notably in the context of NATO exercises. This raises the interesting prospect that Turkey, even if not involved in TNW delivery missions, with forward deployment left to the US Air Force, would nonetheless be involved in operational planning and execution at the tactical level. Turkey's host status is also continued by its Weapon Storage Security System (WS3) housed at Incirlik Air Base. The Turkish armed forces and command structure are also highly centralized. Although detrimental to tactical conventional fighting, this command structure may augur well for NC3 and tactical nuclear operations. However, risks remain even in this context when one considers the fact that various highly placed officers within the Turkish Land Forces were able to seize elements of the state's military apparatus via WhatsApp coordination in 2015, the scale of which has been documented.[26] Uncertainty for NC3 operations also derives from the planned acquisition of US F-35 jets and the risks posed to such agreements by the procurement of the Russian-made S-400 missile defense system instead of the equivalent US Patriot system.[27] Data collected from F-35 sensors might be retrieved by S-400 computers once connected to the HvBS (Turkish Air Force information system) network, and pose a risk to NATO as a whole. In this case, therefore, political and military issues reverberate from Turkey back into the NATO alliance and its overall NC3 system.[28]

Historically, South Africa also offers a precedent to consider in terms of the role of commanders in weapons assembly and related NC3 systems. The commissioning of the Kentron Circle facility on May 4, 1981, intended to create deliverable nuclear weapons, was under the control of the defense establishment, with the Prime Minister P.W. Botha seeing such weapons as political rather than military systems.[29] The focus of the Armaments Corporation of South Africa (Armscor) was to produce deliverable warheads from standoff weapons (the video-controlled Raptor glide bombs) launched from Buccaneer bombers. The stress in Armscor's development was on reliability, safety, and security of the nuclear arsenal. Their models were highly reliable, with inbuilt redundancy, decent internal ballistics, mechanical arming, and safety-related operations.[30] Protocols were also put in place on preventing unauthorized assembly of a whole weapon. To ensure negative control, no single government entity could assemble weapons. A system of codes for removal was instituted at each level: The President was to pass an order to the Minister of Defense and Minister of Minerals and Energy Affairs who, in turn, was to pass the order to the Chairperson of the Atomic Energy Corporation and the Chief of the South African Defense Force and to delegated representatives. Even prior to deployment of an assembled weapon by the South African Air Force, the President, as a feature of positive control, had to send affirmative instructions to the air force base possessing the weapon.[31]

3.8 NC3: Decision-making models

As the Cold War began to thaw, the schism between nuclear strategy at the political executive level and the operational nature of war plans to be executed by the military was well recognized. The fear was the risk posed by "a complete devolution of authority" by the presidential or executive authority "to others, intentionally or by default."[32] This problem was compounded by the universal military-civilian division, often each with its own culture and language. Civilians, for example, can struggle with conceptualizing operational matters in some nuclear weapons states. The issue here is not the military over-responding so much as civilians speaking, or often, not speaking, in the clear language of a command and control system.

The workshop sought to refine the understanding of the nature of command and control systems within the broader discussion, using a mix of heuristic and symbolic devices. NC2 systems, for example, should be seen as living, breathing systems rather than fixed entities. These enterprises, particularly in light of emerging technological forces, need to be flexible, reactive, yet still resilient. It was also suggested that the entire NC3 structure should be seen as a "nervous system" or the "fourth leg" of the triad.

Some states, went one view, prefer to retain assertive control over their nuclear forces until they absolutely no longer can do so. But to see delegative structures and assertive structures in strictly separate terms suggests a false dichotomy; the standard assertive-delegated model is simply too rigid. There are many gradations of nuclear command devolution between states, but also within states themselves as was observed above in the case of Israeli submarines. However, at some point, *all* nuclear weapons states plan to delegate authority to use nuclear weapons to weaponeers, irrespective of present legal authority. (Some suggested that crises may drive delegation and pre-delegation as commanders get nervous, but doing so in the moment may not be desirable.) By way of example, one participant went so far as to argue that Pakistan's command authority might insist on maintaining centralized control to the very end (the point of actual use, not just deployment), though this was deemed operationally impossible. The Prime Minister must initiate the process, but what happens in the arming on the battlefield is another matter entirely, particularly under the stresses of actual conflict.

It was noted that there is a temporal dimension as to when delegation and ceding takes place that likely supersedes doctrinal theories of nuclear war and deterrence practices. Forms of actual delegation and control also vary among states. Use-ability might be ceded to submarine nuclear forces; physical controls might be retained over land-based nuclear forces. Spatial variations of delegation with various types of forces can also take place. There are also different forms of delegation or assertive control depending on whether it takes place in times of peace or conflict, though these vary across nuclear weapons states. Taking into account how this temporal dimension plays out in nuclear command in each nuclear weapons state further complicates attempts to understand NC3 in the 21st century context, but it is critical to explore how this dynamic plays out in specific, nuclear-prone conflicts.

Country case studies regarding decision-making were also noted. Pakistan and India seem disposed to assertive models. Pakistan's concern to deter Indian conventional attacks and maintain survival of its nuclear forces suggests a tendency towards assertiveness. Pakistan is a possibly useful comparative example to the DPRK in terms of adopting similar postures. India has an ambiguous posture as to what forms of command and control apply to its nuclear operations. It might, for example, go to an early crisis delegation if needed, but much would depend on its SSBN forces. Counterforce thinking predominates in Indian nuclear circles and how its control systems operate in different circumstances is opaque.

Where exactly the lines on delegation and pre-delegation on the use of nuclear weapons systems might present problems and whether there was a need to have "hair triggers" cropped up many times but especially in the case study of the delegative structures in Pakistan.

Executive decision makers, their authorizing powers, and the descending chain of command for deployment and use of nuclear weapons, and how strike orders are sent, authenticated, and acted upon were found to vary widely across countries. In one account, the connectivity between the US President and the nuclear force, according to current practice, is excellent. Conversely, some argued that even faced with time imperatives to respond to immediate nuclear attack, there could and should be some checks-and-balances system to limit the US president's ability to launch a nuclear attack at any moment. The senior military officers who would receive a presidential nuclear strike order might disobey him, albeit at their own legal risk, but have no veto power *per se* over the order.

Another model was noted that goes much further than "checks-and-balances." This is a countersigning model, perhaps some variant of the French model necessitating three components – the President (with half the codes), the equivalent of the Joint Chiefs of Staff (CEMP or *Chef d'État-major particulier*), and the private chief of staff – might be preferable, diluting power if only modestly.[33]

Other national nuclear decision-making models were noted, the concern being less the "mad commander" than the ill-informed or ill-advised one. Notions of veto and consent in the decision-making process were found to be interesting concepts, with national NC3 profiles offering a set of viable alternatives, as will be seen below. The countering view was that to the extent that people are added to the chain of command, the more complicated process slows down decisions during a crisis – and possibly pushes decision-making into other, even less rational spheres. In short, there is a range of ways to organize command authority across the nine nuclear weapons states, but no clearly preferable option.

The command structures of specific states offer insightful contrasts. The NC3 system in Britain is generally unitary in its decision-making authority relative to other states, having only one type of deployed force (submarines) and designed to focus on exercising command-and-control over SSBN capabilities at sea. Its essence is politically driven; no military involvement in the process of using

capabilities takes place without civilian direction. In contrast, Pakistan's National Command and Authority is uniquely militarized in how power is exercised over the use of nuclear weapons. Although civilians are ostensibly in control of all systems and decisions regarding deployment and use, Pakistan's all-powerful Army remains fully in control despite any facade indicating otherwise. Ambiguity was expressed in India's case, though it was suggested the Political Council of the Nuclear Command Authority could authorize the release of nuclear weapons.

In the case of less established, prototypical NC3 systems – the DPRK was noted specifically in this regard – decision-making structures were less certain, even inscrutable. What might happen should Chairman Kim Jong-un become unavailable or incapable of making a decision regarding command and control matters? Operational, granular matters in battle were also pondered. For example, what might happen to delegated authority in the case when a missile is being transferred to a unit, or a warhead onto a mobile missile deployed in the field or a cave? The risk of accidental release – or unauthorized use – is a serious concern – presumably to Kim Jong Un as well as external players.

Such opacity also extends to other states. Procedures remain unclear, for example, in terms of how nuclear strike orders reach the French SSBNs. The scope and number of nuclear options for the French president are also unclear. There is considerable controversy over various operational specifics. What, for example, is in the French nuclear football, leading to what one observer described as various "pieces of lunacy?" Some view the issue to be inconsequential; others believe it to be a sophisticated coding machine. Then come the structural challenges: the effective communication of codes to succeeding French presidents; codes going missing; and whether military officers would actually implement a given order has come up in war games.

The enigmatic, even mysterious nature of decision-making models might, to some extent, be alleviated. A suggestion for attaining insight into the nature of such command and control structures could involve examining decision-making precedents across fields and systems in the historical context. One might study, for example, how the DPRK leadership has exercised command in conventional and non-conventional fields in the past. Identifying how the orders were formulated, who gave them and how these were issued and implemented (for example, in previous attacks against the ROK in 2010, or the Rangoon Bombing of October 1983), could provide a picture on broader – and possibly nuclear – operational details.[34]

Expressions such as "agile" and "dynamic" have been suggested as important attributes of how nuclear commanders should be able to respond to the new security environment. Equally, some viewed these terms as faddish, and at minimum, requiring specification in depth before they could be used to guide NC3 modernization. The rise of conventional global strike capabilities, the suggestion by Russian President Vladimir Putin that the tactical use of nuclear weapons is tenable, debilitating cyber-attacks, increasing threats of kinetic attacks on space systems, etc., prefigure the kinds of challenges that nuclear commanders face already. As the preliminary session made clear, the 21st century involves multiple domains of weapons deployment, to be seen as enablers and complements depending on the diversity and structure of nuclear forces in a given arsenal. Specific conflict scenarios were floated: Imagine, went one, cyber and anti-satellite capabilities are deployed, followed by conventional strikes. An attack on a communications satellite could degrade nuclear communications; a high-altitude electromagnetic pulse might be used. Escalation to an attack on US territory could (and would likely) begin with just such attacks aimed at degrading NC3 systems, thereby disabling its nuclear forces, at least to some degree. As was remarked in preliminary discussions on day one of the workshop, preventing the use of inadvertently catastrophic cyber and spatial weapons should also be a priority. These rapidly evolving threats imply that NC3 systems must be reconceptualized and reconstructed in ways that support national command systems which, as we have seen, are quite diverse in the way that decisions are made and supported.

A broader question is how to make NC3 systems resilient in the face of attack, notably in the risks to escalation triggered by conventional assault. An additional feature of the discussion focused on the entanglement of complex systems (nuclear with conventional command, control, communication, and intelligence). As mentioned above, dual-use military assets are inherently entangled across the nuclear and conventional divide, notably those linked to the nuclear complex. An attack on conventional C3 could degrade NC3 capabilities, thereby increasing prospects for escalation. Improvements to non-nuclear weapons (anti-satellite capabilities, cyber weaponry, and high-precision munitions) pose serious threats to NC3 capabilities, even if not designed as such. China, Russia, and the United States have adopted conventional war doctrines that envisage attacks on C3I assets, including dual-use ones, that may result in "incidental attacks." There is no unified position shared by nuclear commanders on the use of conventional, global C2 as it pertains to their engagement with dual-use pieces. But given the ample presence of dual-use systems outlined in the Nuclear Posture Review (2018), such dangers are genuine[35] in scenarios such as the shooting down of short range conventional Russian missiles followed by Russian attacks on US satellites. This would be a case of attacking dual-use assets, thereby increasing risk and likely accelerating the escalatory spiral. Much more attention should be dedicated to how nuclear weapons states can endure and sustain a significant conventional attack before they feel obliged to consider escalation to nuclear threat and use.

To the problem of entanglement that now confronts nuclear commanders must be added an overall, associated concern about risks posed by the growing vulnerability of the NC3 systems of other countries. During the Cold War, nuclear weapons states and their allies relied on the credibility of early and deliberate escalation. Now the issue is how to avoid such escalation given the global dangers it entails. All nine nuclear weapons states must henceforth conduct conventional operations without pushing adversaries to use nuclear weapons. This imperative makes the issue of NC3 vulnerability grave. Ameliorating this risk might entail changing the conduct of great power conventional war by foregoing an initial attack on adversarial conventional C3 systems and abandoning efforts by weaker countries to overcome conventional inferiority vis-à-vis the United States because doing so might in turn only exacerbate entanglement and dual use dilemmas. No-one thought that this process would be easy. But equally, no-one dismissed the significance of the risks being run either.

Some geopolitical environments such as the volatile South Asian context may prove to be antithetical to the creation of resilient NC3 systems. In these cases, NC3 systems may need supplementation with de facto mechanisms for "panic control" (this consideration arose even before the broad introduction of "deep fakes" and social media driven instability). The United Kingdom was specifically referenced as an example where continuous reassurance and exercising is undertaken within the NC3 system, with the maturation of threats, both internal and external, included in such testing. Other NC3 operators may need to emulate this stress testing more than is currently the case.

3.9 NC3: Legal dimensions

The legal underpinnings of NC3 rest within the domestic and international laws that define the legality of nuclear weapons as a whole. Immediate challenges were noted, most critically, the issue of targeting in international law and how this was feasible in any law of war context, and the immense suffering that would result from the use of nuclear weapons. A distinction was drawn, for example, between the issue of legality in terms of targeting and the law on the resort to the threat or use of nuclear force. International law on the subject remains governed by the International Court of

Justice's advisory decision that suggested that most uses of nuclear weapons would be unlawful except in instances where the state in question was imperiled. The use of such weapons, the Court concluded, seemed hardly reconcilable with respect for "the principles of international humanitarian law" but only a qualified conclusion could be reached as it did not have "sufficient elements to enable it to conclude with certainty that the use of nuclear weapons would necessarily be at variance with the principles and rules of law applicable in any circumstance."[36] Where nuclear targeting is concerned, attention was drawn to the distinction principle, to the prohibition of indiscriminate attacks and to the requirement that commanders, decision makers, operators, and planners upstream in the NC3 process take constant care to spare civilians and civilian objects. Furthermore, seeing NC3 as a weapons system generates a legal obligation to review it (although some argue that it was already fully subject to legal review under domestic and international law anyway, as an integral part of nuclear weapons operations and systems). If so, the factual question to ask was whether states do integrate legal advice into such systems? And do those that do so pay lip service to the principle finding work arounds on legal restraints in practice?

On this point, contrasting views on how best to classify NC3 were offered. Could it be seen as a system? Or, literally as a weapons system (as it is now designated by the US Air Force)? It has, after all, always been viewed as a "living" part of the nervous system that controls nuclear arsenals. If as was argued many times in the workshop, NC3 is integral to nuclear weapons, then one must conclude that international legal constraints apply to NC3, just as they do to actual nuclear weapons use – but there is little to indicate this is the case in practice in most nuclear weapons states. But the possibility that the political pressure from the Nuclear Weapons Prohibition Treaty may make nuclear weapons states more careful in this regard was also noted, as was the possibility that informal sharing and learning on how to go about such reviews might be a useful cross-NC3 cooperation measure.

The concept of proportionality in relation to nuclear operations and thereby NC3 was also debated, especially any assumption that a nuclear explosion requires a nuclear response. Taken literally, a proportionate response to a nuclear attack would be to use the same number and type of nuclear weapons. The laws of armed conflict are impoverished on this score and provide little in the way of meaningful military guidance on targeting and proportionality calculi.

How civilians and military personnel discharge their duties lawfully further complicates the nuclear command system. Military obedience is circumscribed to lawful orders; manifestly unlawful ones, it was noted, should not be executed under domestic and international law. In some instances, generals might even be rewarded – or at least not prosecuted – for not following certain orders. The fact that states have nuclear weapons and hold that this possession is legal suggests that a legal, authenticated order to use them would not, *per se*, inevitably be treated as *manifestly* illegal. The 2010 US Nuclear Posture Review was cited, making the claim that nuclear weapons would not be directed against compliant states; it followed that any general who did not follow those orders would not be punished. (It is noteworthy, however, that the resulting presidential nuclear employment strategy policy document in June 2013 states that all US nuclear war plans "must also be consistent with the fundamental principles of the Law of Armed Conflict.")[37]

The cyber element pertaining to NC3 may also be covered by existing and nascent international norms and obligatory constraints. The legal constraints on cyber conduct in warfare, for example, are the subject of the Tallinn Manual and would apply to nuclear warfare and thereby to NC3 systems.[38] Such restraints might be viewed as "only" normative in governing nuclear weapons-related conduct but nonetheless already a restraining consideration for nuclear commanders.

Others, especially those steeped in realistic thinking, view such considerations as epiphenomenal, especially when considered in the aftermath of a nuclear war. (And some averred that the Tallin

process is rejected already by key nuclear weapons states such as Russia and China in any case.)

3.10 NC3: Collaboration, consultation and sharing

Throughout the workshop, participants sought ways to nurture communication, cooperation, and even collaboration among operators of NC3 systems, at various levels, and either bilaterally or multilaterally. One starting point is to create channels for data exchange and the simplest types of NC3-related confidence building measures. The primary goal of such measures was to reduce the stress on NC3 and to increase the reliability of these systems, especially during crises when the risk of accidental or nuclear war would be compounded by the need to make rapid decisions in response to a range of potential, pending, or actual nuclear attacks.

The most obvious way to ameliorate such stress may be to foster regular and routine contact between presidents and senior defense ministry officials, but also at the level of the commanders of nuclear forces and their NC3 units. This contact would enable a closer level of situational awareness and contextual understanding – and perhaps the ability to sift through reams of perhaps misleading information at the moment of crisis. The near rupture of US-Russian working level contacts is especially dangerous given these two states' dominance in terms of absolute nuclear armament and possible direct confrontation on multiple fronts. The lack of expert contact, diplomatic engagement on weapons systems, arms treaties, and limitations on military-military contacts compound the prospect of accidental war arising from human or technical failure.

Thus, it will not be easy to induce cooperation between Russia and the United States on NC3 matters. This difficulty is now deepened by the intended termination of the 1987 Intermediate-range Nuclear Forces Treaty. Although nuclear commanders generally favor the use of diplomacy and arms control, they are also reluctant to support it if violations go unchallenged and in light of enforcement failures. Citing repeated Russian violations with its fielding of the 9M729 intermediate-range ground-launched cruise missile in the context of the INF treaty, a one-party treaty, one participant remarked, is invariably a losing treaty. The same fate will apply to NC3 cooperation measures if these become a one-way street – as may happen with the non-interference with national technical means clause in US-Russian strategic arms limitation treaties if these too are jettisoned.

The issue of technological sharing in the field of modernizing NC3 was also discussed. Any way to gain time for decision makers in a nuclear-laden crisis via technical measures might enable nuclear commanders to shift from a time-compressed "multiple choice" test to a more considered essay test before making decisions to use nuclear weapons. Given its technological prowess, US sharing of its control technologies, especially for negative control of accidental, inadvertent or mistaken use of nuclear weapons, seems a logical starting point. Permitting non-US citizens access to such technologies such as permissive action links, and not treating them as ultra-classified, should be considered. Whether such sharing is allowable under the NPT is contentious but should be examined anew given the potential benefits to reducing the risk of nuclear war. The same riposte applies to those states and voices who might object to NC3 sharing and assistance as another example of the established nuclear weapons states asserting their hegemony. In some cases, assistance has been sought in terms of modernizing NC3 systems, only to then be refused (consider China and the United States in this regard). Some nuclear weapons states – Pakistan was cited as an example – have also refused to engage in such exchange after it was offered as doing so might reveal their nuclear weapons design.

Overall, it will be very difficult to induce NC3-related measures in the absence of trust. The reluctance to share information in any respect on sensitive NC3 issues is compounded by the marked difference in attitudes in each nuclear weapons state towards transparency and non-transparency of security information with respect to their own populations.

How much consultation already exists on how states make nuclear weapons decisions and then implement them is a related issue. There may be more exchange of information in specific nuclear-laden relationships than is known, for example, with China, regarding Britain's role in NATO. In Pakistan, one participant joked, the politicians who nominally command are almost incapable of talking to the military, the implication being that international exchange may have multiple channels – or no authoritative partner at all for external engagement.

Closely related to the idea of NC3-related information flows between nuclear weapons states is how the cyber-nuclear nexus may play out in relations between these states. These are muddied waters already due to the different roles of nuclear and cyber capabilities in maintaining a deterrence posture. This barrier to NC3 cooperation in its cyber dimension is as much conceptual as it is practical. On the cyber side, asymmetric information is fundamental from the attacker's position, relying on secrecy and encouraging incentives to escalate. There is no mutual information present in the cyber context in the way nuclear deterrence works. Nuclear weapons bolster deterrence by virtue of advertising the terrible consequences and astronomical costs of possible use. A nuclear weapons state displays such weapons (for example, in Red Square parades, or strategic bombers alerts and flights) without losing the capability to deter by virtue of these revelations. Strategic deterrence creates mutual information between the parties on the interdependent consequences of their actions involving nuclear weapons whereas the cyber domain discourages revealing such capabilities. Doing so would enable the other side to eliminate vulnerabilities, take countermeasures to blunt the capability, or develop covert offensive means of their own. Such measures are appropriate in intelligence matters.

4. NC3: Conclusions and future goals

A few qualifying remarks from the workshop should be noted in summary. It was noted that it had focused primarily on NC2 and C2 matters, rather than NC3 and conventional C3 – that is, it did not address communications-related issues in any depth. That said, there were ample grounds to build upon. NC3 is deemed an essential part of deterrence and is critical to impress upon the adversary's mind that nuclear strikes are credible. Nonetheless, a broadening and rethinking of conceptual frameworks was required. For one, NC3 needs to work under untestable circumstances in peace time; no other system, it was remarked, has such strains placed upon it in an actual crisis. NC3 is generally understood to need to be more "flexible" and a broader NC3 structure is needed – although there is no consensus on what constitutes this flexibility and breadth.

Other countries also possess NC3 systems of largely undisclosed import: Belgium, Germany, Italy, the Netherlands, and Turkey. Thus, case studies would be useful, notably on documenting common experiences and problems from a comparative perspective. Analysis would also be twinned with understanding the political context. Doing so would improve levels of trust because commanders would be able to understand better the underlying cultural, political, and institutional drivers of decisions and actions, instead of mirror imaging their own circumstances onto their adversaries.

The role of history and precedent in averting accident and disaster in a process of learning is also of great importance. The known corpus of "near misses" and organizational pathologies discovered in NC3 operations over the last half century is likely only a fraction of the actual events when nuclear weapons states came close to using nuclear weapons. The August 1976 crisis on the Korean Peninsula was one cited example.[39] It was precipitated by the trimming of a poplar tree in the DMZ blocking the view of the patrolling US-South Korean unit in the Joint Security Area in what became known as Operation Paul Bunyan.[40] The response featured the movement of tactical nuclear forces still in Korea, the deployment of bombers and fighter aircraft overhead, and pre-delegation to

General Joseph Stillwell with authority to target North Korean barracks north of the DMZ in the event of interference with the tree trimming operation. President Gerald Ford effectively granted authority to a commander in the field to commence, if needed, a resumption of conflict on the peninsula, with possible use of tactical nuclear weapons. The NC3 dimension in this operation was central to the risk taken of possible near loss of control. Yet this incident, critical to understanding the mindset of North Korean's leaders, is almost forgotten in Washington and is never listed in "near miss" studies. Assuredly, there are many others buried in the archives of nuclear weapons states.

The scholarly and policy analysis of NC3 systems is also limited by the insider-outsider problem and the significant levels of classification of system operations. Although classification is important – indeed critical – to nuclear security, the fact remains that the equally critical "outsider" material is often not known to insiders, especially that related to the adversary. Open source material and what is obtained via Freedom of Information are available to support enquiry into NC3 systems and NC3-related history. A digital reading room for researchers in the field would be of great benefit, especially as it could be shared across borders, be accessible on a global basis, and potentially be multilingual. To documented history can be added oral history as well, which often captures key anecdotes or instances that were regarded as too political or embarrassing to document, or were subject to outright suppression. Operators may also remain silent for decades, fearing retribution or prosecution if they reveal their knowledge of NC3 failures.

Emerging technologies (for instance hypersonic weapons, quantum computing, and cyber challenges) are particularly pressing due to their potential to destabilize existing NC3 systems. Game changing technology will alter the nature of the nuclear decision-making process and its temporal dimension. The role of decision-making and the structure of decision agents in the command structure, their accountability, and whether cyber and nuclear, and conventional and nuclear forces should be integrated or fused, or separated and disentangled, all demand further exploration.

The imperative of investing in a capable workforce also emerged in discussions, with particular need to concentrate on NC3 personnel education and learning. More consideration and attention also had to be given to the learning process dealing with command and control. The film medium, for example, might be used as well as participatory agent-based modelling.

The tradeoffs between delegative or assertive controls were much discussed. This has been called the always-never problem; you simply do not want weapons to go off by accident. If used, they should only be used at the highest level and if relied upon for deterrence and must be always available. Some remarked that we find ourselves in a new James Schlesinger period on a daily basis, where military orders on nuclear matters coming from the White House (or from other global leaders) might have to be ignored.[41] The balance between negative and positive controls in NC3 systems, and between organizational and technical control measures within negative and positive controls, varies greatly between states; yet there is almost no study of how these different "NC3 stability biases" influence how specific nuclear-prone conflicts may evolve, either routinely or in crisis.

It was also suggested that NC3 had to be considered working backwards. In some NC3 systems, legacy systems predominate or are combined with ultra-modern systems. The way that these combinations may inflect decisions or their implementation is little studied and poorly understood, even in the United States, let alone in the other nuclear weapons states. Similarly, the entanglement of nuclear with conventional C3 has to be seen not merely from the perspective of tactical warnings but from a strategic standpoint. Consideration must always be given to what the other side might be thinking, leaving a pressing problem. Who would be responsible for giving the appropriate indicators and signals given that the role of false information – delivering social and textual media that might

be counterfeit – is a significant and increasingly troublesome factor.[42] If we are interested in appropriate pre-emption and alert activities, then all these elements must be considered.

Other specific NC3 topics for ongoing research and exploration include:

1. The meaning of greater NC3 agility and the imperative to constantly and rapidly respond to mission changes. This would, for example, involve broadening NC3 to consider cyber-physical system challenges and opportunities. New norms may be needed to achieve stability in the NC3 dimension.
2. Ways to build the necessary trust and non-repudiation in the NC3 dimension, in spite of the immense difficulties of doing so given geopolitical trends, and the disruptive and inherently untrustworthy digital environment.
3. Ways to routinely upgrade NC3 system(s) given the pace of technological development relative to the speed of uptake in nuclear weapons states and NC3 agencies.
4. Understanding the significance of NC3 vulnerability is fundamental. One insider, suggested one participant, is another's outsider. Launch codes can be surrendered (the case of John A. Walker, Jr. was cited). In some instances, the solution may lie in disentangling and isolating systems. NC3 systems, for example, can be disconnected from the Internet and defense intra-nets (but even "air-gapped" systems remain at risk). The use of redundancies may also assist, at least up to a point. The strategic impact of inevitable, evolving NC3 vulnerabilities needs to be examined closely, especially whether vulnerability may strengthen rather than weaken deterrence, the opposite of conventional wisdom.
5. Endurance/resilience was specifically noted as a critical attribute of NC3, leading to the fundamental question: How much resilience is enough, and can too much resilience lead to increased not decreased risk of nuclear war?
6. NC3 needs to be visible to the adversary as an essential element of deterrence. What attributes should be revealed, possible in some regime of NC3 cooperation, and what set of tacit or explicit NC3 norms might be developed, is an urgent question.
7. All nuclear commanders must understand that a nuclear war cannot be won. Only with that deep understanding can come the building of necessary NC3 measures to work towards avoiding that catastrophic outcome.

APPENDIX A: SCENE SETTER—NC3 AND STRATEGIC STABILITY: A GLOBAL OVERVIEW

Peter Hayes, Nautilus Institute

January 22, 2019

Welcome to the NC3 AND STRATEGIC STABILITY workshop, this one A GLOBAL OVERVIEW.

I'd like to outline the three reasons why we framed this workshop with a global perspective.

First and foremost, we need updated baseline NC3 profiles. When the five NATO nuclear delivery states (Belgium, Germany, Italy, The Netherlands, Turkey) and South Africa's dismantled NC3 system are added to those of the nine nuclear weapons states, we find there are fifteen NC3 systems to study. Here, we managed to cover ten of these fifteen NC3 systems.

Non-state actors also aspire to nuclear armament and present distinctive NC3 dilemmas and

imperatives, and they must also be studied carefully for potential catalytic effects on state-based NC3 operations.

There are many methodological issues involved in compiling, and then comparing and contrasting NC3 systems. These are not just technical systems. They are cultural, sociological, and institutional systems at core and to understand them, we need insight from many disciplines. And, given the secrecy and sensitivity surrounding NC3 in each country, we must be modest about the claims that can be advanced by scholars outside the system, and within the boundaries of classification, draw on the willingness of serving and retired military participants to share their insight and knowledge.

To this end, I remind everyone that we meet under strict application of the Chatham House Rule.

Second, we want to understand better how NC3 affects strategic stability, in different contexts and conditions, across the entire set of 15 NC3 cases, not just the best studied case, US NC3.

Thirty-five states (being the nuclear weapons states + NATO allies + Japan, ROK, Australia) depend directly on nuclear deterrence and thereby on the performance of national NC3 systems.

The effects of nuclear threat are horribly complicated and, in specific instances, much disputed. Moreover, deterrence is a matter in which the adversary gets a vote, and it may not always behave as expected. Separating out cause from effect, in particular, NC3 effects from other force posture effects, on an adversary's perceptions and actions, is difficult, even for participants, let alone observers.

One can reasonably argue that NC3 capabilities have attributable effects on deterrence, compellence, and reassurance outcomes.

Thus, NC3 may be integral to the immediate and general ***deterrence*** of one or more parties to a nuclear-prone conflict by enhancing the credibility of nuclear threat, including:

- the ability to positively and negatively control forces,
- the avoidance of false positive and false negative errors in early warning systems and decision-making,
- the signaling of intent, and
- the demonstrated ability to survive attack and retaliate.

All of which arguably *reduce* the risk that one or more party may use nuclear weapons. The epitome of the NC3-deterrence effect might be the rapid hardening of command posts and communications for EMP effects in the Cold War and the effect that this change in NC3 systems had on US-Soviet perceptions of strategic forces.

Conversely, NC3 systems may support use of nuclear threat to realize ***compellence,*** which is arguably harder to achieve and even harder to document than deterrence. Moreover, striving for compellence arguably *increases* the risk that one or more party may use nuclear weapons. An example would be the use of countervailing compellent nuclear threats by North Korea and the United States for the last 28 years; and whatever glimpses, intended or inadvertent, each side gained of the other's NC3 operations at times of maximum tension.

A third broad effect, the ***reassurance*** of self, allies, third parties, and adversaries, may be realized due to NC3 operations that support the implementation of nuclear arms control and disarmament

agreements.

Arguably, this usage creates strategic stability and *reduces* the risk of nuclear war – although this contribution is now challenged by the increasing fluidity of nuclear conflicts and the demise of much existing arms control.

An NC3-related example might be the non-interference with NTM clause in strategic arms treaties; the use of the I in NC3-I to monitor and verify treaty commitments. Hot lines are another example.

How the US NC3 system has performed with respect to these three effects has been much studied, both internally, resulting in studies such as the now declassified Joint Chiefs review of strategic connectivity in 1982, and by scholars using open source literature and the US FOIA.

The same is not the case for the other thirteen NC3 systems, and there is much to learn about how NC3 systems affect strategic stability in the multiple nuclear prone conflicts that exist today, not just those involving the United States directly.

Jerry Conley and PASCC came up with a working taxonomy of NC3 control orientation that is a good heuristic device.[43] But we need to dive much deeper to identify the full range of possible NC3 effects.

Moreover, when everything is changing at the same time, especially when the underlying technologies themselves are changing so fast and profoundly, what worked in the past may be obsolete – or the only thing that still works.

The third reason to approach the topic from a global perspective is that all NC3 systems face common problems, and some solutions also may be shared.

There are many urgent and difficult issues to resolve in the US NC3 system, which presenters, especially on Day 2, will address.

Some of these may pertain only to the United States' system, given its unique combination of 107 plus NC3 systems[44] that integrates legacy with advanced technologies aimed at addressing the overall challenge of the new cross-domain reality – and is about to undergo a total remake incorporating emerging AI, quantum, and cyber technologies, each of which is only beginning to be understood and could arguably fundamentally alter our current understanding of NC3 and its effects.

Yet, many of these issues are equally or even more salient to other NC3 operators. Consequently, there is a potential opportunity to avoid needless replication of bad practice, at a global level.

Thus, we want know if there are potential, possibly fleeting opportunities for communication, cooperation, and collaboration on NC3 issues?

Some possibilities include:

- Producing a common vocabulary between NC3 operators, starting with the definition of NC3;
- Creating a reading room of key documents in original languages;
- Developing bilateral NC3 frameworks, perhaps starting with more and better hot lines to create weak links for crisis management;
- Developing impartial, third party information sources on the status of nuclear weapons to address the new informational environment permeated by social media;

- Developing a multilateral NC3 Code of Conduct that would propagate harmonized standards, best practices, rules of the road, and nascent NC3 norms, etc. (similar to the 2002 International Code of Conduct on Missile Proliferation, now adhered to by 138 states);
- No doubt other ideas will emerge at the event, perhaps related to legitimacy and the LOAC, or on checks and balances on nuclear commanders in NC3 systems.

***

I'd like to move now to another reason we are here.

I recall that during the Cold War, the "NC3 originals" had a huge impact. To mention only a few:

- Des Ball, *Can Nuclear War Be Controlled*[45]
- Paul Bracken, *The Command and Control of Nuclear Forces*[46]
- Bruce Blair, *Command and Control of Strategic Nuclear Forces*[47]
- Elizabeth Pate Cornell, "Reliability Model for the Command and Control of U.S. Nuclear Forces"[48]

culminating in the benchmark volume, I am sure you all have it:

- Ash Carter, John Steinbruner, and Charles Zraket, eds, *Managing Nuclear Operations.*[49]

Des, Charles, and John are gone and Bruce could not join us and sends his apologies.

Fortunately, we have Scott Sagan here whose *The Limits of Safety* is required reading for anyone serious about organizational theory and NC3 systems performance.[50]

These NC3 originals redefined the terms of the Cold War and the role of NC3 from counterforce targeting, graceful collapse, the vulnerability of NC3, to widespread acceptance that nuclear warfighting was not controllable.

A similar evolution was under way in the former Soviet Union, as recounted in Vladimir Yarynich's 2003 study, *C3: Nuclear Command, Control, Cooperation*[51] – almost completely unknown in the West.

Like the early 1980s, and right on time, we see a new crop of theses dealing with NC3:

- Daniel Volmar at Harvard;
- Jared Dunnmon's thesis here at Stanford;
- Brian Radzinsky's dissertation underway at GWU on civil-military politics;
- Fiona Cunningham's just completed MIT dissertation on China that includes NC3;
- Elsa Kania's dissertation underway at Harvard on China that surely will also include NC3;
- James Fern's jewel of a dissertation at Capella University, a case study of proficiency loss and recovery of NC2 personnel in PACOM during disaster relief in 2009;[52]
- Salma Shaheen's dissertation at Kings College, just published, *Nuclear Command and Control Norms.*[53]

These and no doubt the many more that will follow are just in time, given the urgent need to reconceptualize NC3 from top-to-bottom and inside-out, as Commander Hyten said in his November letter seeking input to his NC3 project.

Concurrently, we see a new effort to educate NC3 professionals who will draw on this scholarly enquiry. Three NC3 educational support efforts working with Strategic Command are represented today: the Naval Postgraduate School, Louisiana Tech Research Institute, and Eisenhower School at NDU.

I will leave the last word to Paul Bracken. Ever the Yale Professor, when he agreed to mark all your papers in a review essay he will prepare in February, he said:

"Dangerous issues are just below the surface, latent and contingent. The skin of civilization is exceedingly thin. We don't see this because we worry about the kids, traffic, trade conflicts, and budgets. But if a severe nuclear crisis or a war developed, nuclear issues are not far away. They can come back in a flash if conditions change. So it's a good time to think about these matters, when we are not in a mass panic or open psychoses of rage and revenge."[54]

On that cheerful note, I'd like to ask our host to make his opening remarks.

Thank you.

APPENDIX B: NC3 and Global Stability Papers Forthcoming

The following papers from the workshop will be published in 2019, starting in May 2019. Please check www.nautilus.org and www.tech4gs.org for the latest posting.

Ackerman, Gary A.: The Non-State Dimension of Nuclear Command, Control, and Communications

Acton James M.: For Better or For Worse: The Future of C3I Entanglement

Boothby, William H.: Law, Targeting and Nuclear Operations

Bracken, Paul: NC3 in a Multipolar Nuclear World: Big Structures and Large Processes

Cheon, Myeongguk: DPRK's NC3 System

Cohen, Avner: Israel NC3 Profile: Opaque Nuclear Governance

Cunningham, Fiona S.: Nuclear Command, Control, and Communications of the People's Republic of China

Davis, Paul K.: What Do We Want from the Nuclear Command and Control System?

Gardner,Col Elvert L.: An Examination of the NC3 Industrial/Innovation Base

Gower, John: United Kingdom Nuclear Weapon Command, Control, & Communications

Grosse, Eric: Security at Extreme Scales

Harvey, John R.: U.S. Nuclear Command and Control for the 21st Century

Jones, Carol Ann: Counter Nuclear Command, Control, and Communications

Kania, Elsa B.: Potential Technological Augmentation of PLA NC3 Architectures

Kasapoglu, Can: Turkey and the Nuclear Command, Control, and Communications

Khan, Feroz Hassan: Nuclear Command, Control and Communications (NC3): The Case of Pakistan

Larsen Jeffrey A: Nuclear Command, Control and Communications: U.S. Country Profile

Leveson, Nancy,: An Engineering Perspective on Avoiding Inadvertent Nuclear War

Lindsay, Jon R.: Cyber Operations and Nuclear Weapons

McGiffin, Curtis D.: Next Generation NC3

Narang, Vipin: A New Framework for Thinking About Regional NC3

Pelopidas, Benoît: France: Nuclear Command and Control

Press, Daryl G.: NC3 and Crisis Instability Growing Dangers in the 21st Century

Ramana, M.V. & Borja, Lauren J.: Command and Control of Nuclear Weapons in India

Ryabikhin, Leonid: NC3 and Ballistic Missile Early Warning System

Savage, Sam: Early Warning Detection Problem, Solution, False Positives

Schouten, Ronald: NC3 Insider Threats

Wellerstein, Alex: NC3 Decision-making: Individual Versus Group Process

Willrich, Mason: Innovation and Adaptive Control in America's Electric Infrastructure: Parallels to NC3

APPENDIX C: ABOUT THE WORKSHOP

NC3 SYSTEMS AND STRATEGIC STABILITY: A GLOBAL OVERVIEW

What: A 2-day closed, Chatham House rules (unclassified) workshop of about 30 experts plus observer participants from relevant agencies

When: January 22–23, 2019

Where: Hoover Institution, Stanford University

Why: During the Cold War, US and Soviet NC3 systems were integral to controlling nuclear weapons and avoiding inadvertent nuclear war. NC3 systems presented an incentive to strike first and therefore were destabilizing. At the same time, NC3 systems were key to assured massive retaliation under attack, and therefore were stabilizing. Tens of billions of dollars were invested by both superpowers so that they could harden NC3 systems to fight nuclear wars. Both experienced false alarms and alerts due to NC3 system failures that could have led to nuclear war and

catastrophe.

Today, nine states have nuclear weapons and NC3 systems. How multiple nuclear-armed states interact in nuclear-prone conflicts is poorly understood. National NC3 capabilities are technically dissimilar, operate in different governance and cultural systems, and there are no common standards of NC3 performance. The impact of NC3 systems on the risk of nuclear war in regional flashpoints is a new factor in the decisions of the global nuclear weapons states. How NC3 operates in this new complexity, including how new technologies such as social media, quantum computing, cyberwarfare, autonomous vehicles, and artificial intelligence affect "legacy" NC3 systems and organizations, are urgent questions for researchers and practitioners alike.

The United States alone spends more than $5 billion per year on NC3 modernization. How NC3 can serve as a force multiplier and reducer while remaining resilient in the face of inevitable stress, shocks, and uncertainty, is an urgent policy question in all nuclear weapons states. The new complexity of the operating environment suggests that performance metrics, norms, and standards might be promoted across all NC3 systems as an antidote to NC3-induced strategic instability at the global level.

Day 1: Scholars and practitioners will present profiles of nine national NC3 systems including technical, organizational, legal, and political military dimensions, as well as of allied "nuclear umbrella" states, and of non-state actors with nuclear weapons aspirations. They will also examine theoretical and practical aspects of NC3 controls of nuclear weapons and the effect of NC3 system performance on "strategic stability" and the risk of nuclear war.

Day 2: Scholars and practitioners will examine US NC3 systems, performance metrics, modernization, nuclear conventional-entanglement, and related issues in greater depth. They will also present case studies from other complex technological enterprises that exhibit tight coupling in the search for insight into the interplay of national NC3 systems that constitute a global or meta-NC3 system today.

Who: This workshop is convened by:

- Nautilus Institute for Security and Sustainability
- Technology for Global Security
- Preventive Defense Project, Freeman Spogli Institute for International Studies, Stanford University

Funded by The John D. and Catherine T. MacArthur Foundation

III. ENDNOTES

[1] The gathering was held at the Annenberg Conference Center, 105 Lou Henry Hoover Building, Stanford University, California, January 22-23, 2019.

[2] The Chatham House Rule is stated at: https://www.chathamhouse.org/chatham-house-rule

[3] Unless otherwise referenced, the entirety of this report is based on the discussion and insights made during the two-day workshop.

[4] Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (New York:

Times Books, 2012).

[5] Email message to Peter Hayes, December 24, 2018.

[6] Termed C³1: Ashton B. Carter, "The Command and Control of Nuclear War," *Scientific American* 252, 1 (Jan, 1985): 32-39, 32.

[7] Desmond Ball, *Can Nuclear War be Controlled?* (Adelphi Papers, International Institute for Strategic Studies, September, 1981); *Targeting for Strategic Deterrence* (The Adelphi Papers 1983); Paul Bracken, Bruce Blair; Scott Sagan, *The Limits of Safety: Organizations, Accidents and Nuclear Weapons (*Princeton, NJ: Princeton University Press, 1993).

[8] For example, Fiona S. Cunningham and M. Taylor Fravel, "Assuring Assured Retaliation: China's Nuclear Posture and U.S.-China Strategic Stability," *International Security* 40, 2 (2015): 7-50.

[9] For further discussion, see N.G. Leveson, "A New Accident Model for Engineering Safer Systems," *Safety Science* 42, 4 (April, 2004): 237-270 and *Engineering in a Safer World* (Cambridge, MA: MIT Press, 2011).

[10] C. A. R. Hoare, "The Emperor's Old Clothes," The 1980 ACM Turing Award Lecture, Delivered at ACM '80, Nashville, Tennessee, October 27, 1980, available in *Communications of the ACM* 24, 2 (Feb., 1981): 75-83, 81.

[11] Hoare, "The Emperor's Old Clothes," 82.

[12] Thomas Kuhn, *The Structure of the Scientific Revolutions* (Chicago: University of Chicago Press, 1962).

[13] On problems with FATB, see U.S. Department of Defense, Developmental Test and Evaluation and System Engineering, FY 2011 Annual Report, March 2012, 191. Full report available at: https://www.acq.osd.mil/dte-trmc/docs/FY2011_DTE_SE_AnnualReport.pdf

[14] U.S. Department of Defense, Developmental Test and Evaluation and System Engineering, FY 2011 Annual Report, March 2012, 192.

[15] Director, Operational Test and Evaluation, "FY 2015 Annual Report," January 2016, 316. Full report available at: https://nautilus.org/wp-content/uploads/2019/05/DOD-Developmental-Test-and-Evaluation-and-Systems-Engineering-FY-2011-Annual-Report.pdf

[. 16] Harry Halem, "Statistical Diplomacy: A Bayesian Inference Tool for the P5+1+Iran Negotiations," *Arms Control Wonk*, October 14, 2013, https://www.armscontrolwonk.com/archive/604031/statistical-diplomacy-a-bayesian-inference-tool-for-the-p51iran-negotiations/.

[17] See the FlawOfAverages.com and Sam L. Savage, *The Flaw of Averages: Why We Underestimate Risk in the Face of Uncertainty* (New York: John Wiley & Sons, 2009, 2012).

[18] See A. D. Shaw, "Command, Control and Communications: Basic Concepts and Characteristics," *Scientia Militaria: South African Journal of Military Studies* 10, 3 (1980): 48-60. The US perspective is also considered in this report in the section titled "NC3: Its necessity."

[19] John E. Hyten, General, USAF, Memorandum, "Subject: Next Generation NC3 Enterprise," November 21, 2018. In this report, see also "NC3: Decision-making models."

[20] For a history of NC3 thinking in Britain, see Peter Hennessy, *The Secret State: White Hall and the Cold War* (London: Allen Lane, 2003).

[21] See Vipin Narang, "Five Myths about India's Nuclear Posture," *The Washington Quarterly* 36, 3 (2013): 142-157. See also M. V. Ramana, "India's Nuclear Enclave and the Practice of Secrecy," in *Nuclear Power and Atomic Publics: Society and Culture in India and Pakistan*, Itty Abraham, ed. (Bloomington, Indiana: Indiana University Press, 2009), 41-67.

[22] NSAB (National Security Advisory Board), *Draft Report of National Security Advisory Board on Indian Nuclear Doctrine* (New Delhi: National Security Advisory Board, August 17, 1999).

[23] Ministry of External Affairs, Government of India, "The Cabinet Committee on Security Reviews Operationalization of India's Nuclear Doctrine," January 4, 2003, https://mea.gov.in/press-releases.htm?dtl/20131/The_Cabinet_Committee_on_Security_Reviews_perationalization_of_Indias_Nuclear_Doctrine+Report+of+National+Security+Advisory+Board+on+Indian+Nuclear+Doctrine.

[24] Fiona S. Cunningham and M. Taylor Fravel, "Assuring Assured Retaliation: China's Nuclear Posture and U.S.-China Strategic Stability," *International Security* 40, 2 (2015): 7-50.

[25] Mustafa Kibaroglu, *Orta Doğu'da Nükleer Teknolojinin Yayılması ve Türkiye'nin Olasi Yanıtları* (EDAM, 2012).

[26] See documents on communications obtained in Christian Triebert, "'We've shot four people. Everything's fine.' The Turkish Coup through the Eyes of its Plotters," Bellingcat, July 24, 2016, https://www.bellingcat.com/news/mena/2016/07/24/the-turkey-coup-through-the-eyes-of-its-plotters/

[27] Debalina Ghoshal, "Why did Turkey Choose the S-400?" *DefenceIQ*, October 15, 2018, https://www.defenceiq.com/air-land-and-sea-defence-services/news/will-turkey-buy-th--patriot-system.

[28] Hava Kuvvetleri Bilgi Sistemi – Muharebe Yönetimi: the Air Force Information System – Battle Management: see Burak Ege Bekdil, "Turkey wants to link F-35 jets to its Air Force network," *Defense News*, January 9, 2018, https://www.defensenews.com/air/2018/01/09/turkey-wants-to-lik-f-35-jets-to-its-air-force-network/.

[29] David Albright and Andrea Richter, *South Africa's Nuclear Weapons Program: Its History, Dismantlement, and Lessons for Today* (Washington, D.C.: Institute for Science and International Security (ISIS) Press, 2016), 92.

[30] Albright and Richter, *South Africa's Nuclear Weapons Program*, 104.

[31] Albright and Richter, *South Africa's Nuclear Weapons Program*, 108-9.

[32] Janne E. Noland, *Guardians of the Arsenal: The Politics of Nuclear Strategy* (New York: Basic Books, 1989).

[33] For more on the use of these three agents in engaging French nuclear forces, see Bruno Tertrais and Jean Guisnel, *Le Président et la bombe. Jupiter à l'Elysée* (Paris: Odile Jacob, 2016).

[34] For details on such attacks and interventions by the DPRK, see Joe Freeman, "A History of North Korean Misadventures," *The Atlantic*, March 19, 2017.

[35] Office of the Secretary of Defense, *Nuclear Posture Review* (February, 2018), available at:

https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

[36] International Court of Justice, *Legality of the threat or use of nuclear weapons*, Advisory Opinion of 8 July 1996, Opinion of the Court, Para. 95.

[37] *U.S. Department of Defense, Report on the Nuclear Employment Strategy of the United States*, June 12, 2013, pp. 4-5, at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a590745.pdf

It continues: "Accordingly, plans will, for example, apply the principles of distinction and proportionality and seek to minimize collateral damage to civilian populations and civilian objects. The United States will not intentionally target civilian populations or civilian objects."

[38] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press 2013); *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd edition (New York: Cambridge University Press, 2017).

[39] Peter Hayes, "The August 1976 Incident Revisited – The Last Nearly Nuclear War in Korea," *NAPSNet Special Reports*, March 3, 2018, https://nautilus.org/napsnet/napsnet-special-reports/the-august-1976-incident-revisited-the-last-nearly-nuclear-war-in-korea/.

[40] Conrad DeLateur, *Murder at Panmunjon: The Role of the Theater Commander in Crisis Resolution*, US Department of State Foreign Service Institute Research Paper, 29th Session, 1986-7, released under US Freedom of Information Act information request, at: https://nautilus.org/foia-document/murder-at-panmunjom-the-role-of-the-theater-commander-in-crisis-resolution/.

[41] See Gil Troy, "The Most Patriotic Act of Treason in American History?" *Daily Beast*, Feb 11, 2017; Garrett M. Graff, "The Madman and the Bomb," *Politico*, August 11, 2017, https://www.politico.com/magazine/story/2017/08/11/donald-trump-nuclear-weapons-richard-nixon-215478.

[42] Nautilus Institute, Technology for Global Security, Preventive Defense Project, "Social Media Storms and Nuclear Early Warning Systems: A Deep Dive and Speed Scenarios Workshop Report", *NAPSNet Special Reports*, January 08, 2019, https://nautilus.org/napsnet/napsnet-special-reports/social-media-storms-and-nuclear-early-warning-systems-a-deep-dive-and-speed-scenarios-workshop-report/

[43] See, Jerome Conley, "Nuclear Command and Control in the Twenty-first Century: Trends, Disparities, and the Impact on Stability," in Owen Price and Jenifer Mackby, Eds., *Debating 21st Century Nuclear Issues, CSIS,* Washington DC, 2007, at: https://www.csis.org/analysis/debating-21st-century-nuclear-issues and *Nuclear Command, Control, and Stability Framework*, Center on Contemporary Conflict PASCC report, Naval Postgraduate School, Monterey, December 29, 2015, at: http://hdl.handle.net/10945/48707

[44] Presentations at this workshop state that the figure is slightly higher today—109 NC3 systems in one paper, as many as 160 NC3 systems in another. General Rand stated in 2017: "NC3 weapon systems is made up of multiple different types of weapon systems, everything from [military satellite communications systems] to the command post terminals ... There are a huge number — 107 different systems to get our hands around. And I will be honest with you, the system atrophied for a lot of different reasons." In S. Magnuson, "Exclusive: Interview with Gen. Robin Rand, Head of Air Force Global Strike Command," *National Defense Magazine*, November 14, 2017, at: http://www.nationaldefensemagazine.org/articles/2017/11/14/global-strike-command-tackles-atrophy

ing-nuclear-command-control-systems.

[45] Des Ball, *Can Nuclear War Be Controlled,* Adelphi papers 161, 1981.

[46] Paul Bracken, *The Command and Control of Nuclear Forces*, dissertation, Yale University, 1982, available from Proquest Dissertations, and published by Yale University Press, 1985.

[47] Bruce Blair, *Command and Control of Strategic Nuclear Forces*, dissertation, Yale University, 1984, available from Proquest Dissertations, and published by Brookings Institution, 1985.

[48] Elizabeth Pate Cornell, "Reliability Model for the Command and Control of U.S. Nuclear Forces," *Risk Analysis,* 5:2 *1985*, pp. 121-138.

[49] Ash Carter, John Steinbruner, and Charles Zraket, eds, *Managing Nuclear Operations*, Brookings Institution, 1987.

[50] Scott Sagan *The Limits of Safety, Organizations, Accidents, and Nuclear Weapons,* Princeton University Press, New Jersey. *1993.* Another important dissertation was S. Gregory, *Nuclear command and control in NATO and the strategy of flexible response,* Dissertation, Tennessee State University, 1991, published by Palgrave McMillan, London, 1996.

[51] Vladimir Yarynich, *C3: Nuclear Command, Control, Cooperation*, Center for Defense Information, Washington, 2003, available here: https://www.scribd.com/doc/282622838/C3-Nuclear-Command-Control-Cooperation

[52] James Fern, *Case Study of Proficiency Loss and Knowledge Recovery of People In Nuclear Command And Control Critical Jobs,* Dissertation, Capella University, 2009, available from Proquest Dissertations.

[53] Salma Shaheen, *Nuclear Command and Control Norms,* dissertation, Department of War Studies, Kings College, London, published by *Routledge* Global Security Studies, 2019.

[54] Email from Paul Bracken to Peter Hayes, December 24, 2018.

IV. NAUTILUS INVITES YOUR RESPONSE

The Nautilus Asia Peace and Security Network invites your responses to this report. Please send responses to: nautilus@nautilus.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent

---

View this online at: https://nautilus.org/napsnet/napsnet-special-reports/synthesis-report-nc3-systems-and-strategic-stability-a-global-overview/

Nautilus Institute
2342 Shattuck Ave. #300, Berkeley, CA 94704 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org