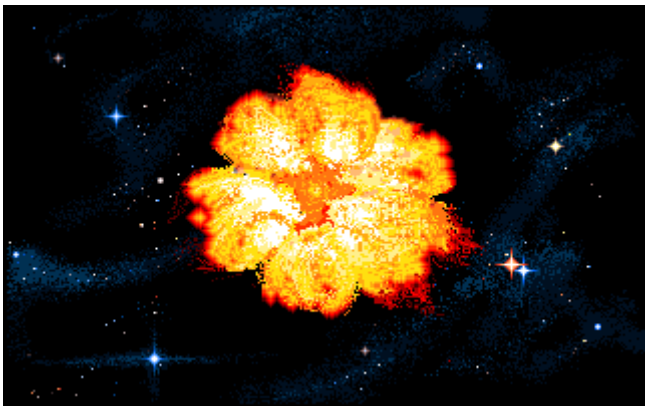
Nuclear command-and-control in the Millennials era



Recommended Citation

Peter Hayes, "Nuclear command-and-control in the Millennials era", NAPSNet Special Reports, February 17, 2015, https://nautilus.org/napsnet/napsnet-special-reports/nuclear-command-and-control-in-the-millenials-era/

by Peter Hayes

17 February, 2015

Text updated: 17 February, 11pm PST

I. Summary

In this report Peter Hayes writes about the risk of nuclear war and complexity. He states that “very few leaders or even strategic scholars pay attention to the new complexity of the operating environment in which national nuclear command-and-control systems operate, or the new characteristics of the command-and-control systems and their supporting CISR systems that may contribute to the problem of loss-of-control and rapid escalation to nuclear war."

“Today, the underlying ground is moving beneath the feet of nuclear-armed states. The enormous flow across borders of people, containers, and information, and the growth of connectivity between cities, corporations, and communities across borders, is recasting the essential nature of security itself to a networked flux of events and circumstances that no agency or state can control. The meta-system of nuclear command-and control systems has emerged in this new post-modern human

condition."

Peter Hayes is Co-founder and Executive Director of Nautilus Institute for Security and Sustainability; Honorary Professor at the Center for International Security Studies, Sydney University, Australia.

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.

Acknowledgement: The author is grateful for review comments on earlier drafts by Paul Bracken, Roger Cavazos, Elbridge Colby, Todd La Porte, Nancy Leveson, Jeffrey Lewis, Patrick Morgan, and Richard Tanter. Naturally, the author is solely responsible for any errors of fact or analysis that remain herein.

II. REPORT BY PETER HAYES

Nuclear command-and-control in the Millennials era

Introduction

A 1989 computer game, *Nuclear War,* released in 1989 and played on DOS, set different nuclear weapons states against each other, each trying to blow the other to smithereens. In this game, random events interrupted the "normal" business of nuclear war. Exemplary wild cards including the arrival of aliens and rapidly growing populations, or firing a cow against an opponent which leads to a stampede that kills millions of people. If the game is drawn, everyone loses and the Earth explodes—which is the cheerful screenshot image used to illustrate this essay.[1] These metaphorical allusions incorporated real aspects of the Cold War nuclear balance of terror: alien populations stand in for grossly inflated threat estimates; and hurtling cows to the risk of inadvertent war due to false alarms by the early warning systems then in use, for example.

In contrast, the premise of strategic theory is the anti-thesis of this game: no-one loses when the game is drawn due to reciprocal and unavoidable threat of nuclear annihilation which creates a condition of strategic stability. However, the perceived security derived from the "delicate balance of nuclear terror" in the real world rested on managing and exploiting the risk of nuclear war at the same time. As the cost of nuclear war between great powers was essentially infinite, all that could be manipulated in their direct relationship was the probability of war and escalation to nuclear war. This left little room for coercive diplomacy based on the threat of nuclear war between the great power nuclear weapons states, and displaced much of their competition into peripheral contested zones involving non-nuclear forces and non-nuclear states.

Thus, the United States attempted more than once during the long Cold War to use nuclear threat to effect but failed to coerce non-nuclear adversaries to capitulate. The credibility of nuclear threats against conventionally armed adversaries, big and small, rested on the simple notion that being unable to retaliate after a US first strike, the United States was unconstrained in its possible use of nuclear weapons. As the silk-screened tee-shirt illustrated with a mushroom cloud captioned "Hiroshima-Nagasaki" sold to visiting US sailors at Olongapo port in the early eighties put it: "Fuck with us and we'll do it again." In reality, however, whenever US leaders looked over the brink at using nuclear weapons against non-nuclear states during various wars and crises, they backed

off—in the 1958 Quemoy-Matsu conflict, the Korean War, the Vietnam War, the 1969 seizure of the Pueblo, and the August 1976 Panmunjon crisis, for example.[2]

Since the Cold War, the risk of global nuclear war is generally held to have fallen, due primarily to the reduction in probability arising from the disappearance of the former Soviet Union. Although the consequences of the still conceivable all-out nuclear exchange between the United States and Russia remained essentially infinite, both nuclear superpowers shifted their intentions and signaled that their propensity to engage in such a war had dwindled to so remote that, as Vice Commander of US STRATCOM stated in 2013, it is "hardly worth discussing."[3] This trend is embodied in the dramatic and significant strategic arms reductions since the early nineties by these nuclear weapons states.

Over the same period, the risk of local and regional nuclear war has arguably increased due to five factors: a) horizontal nuclear proliferation by small states (especially the DPRK); b) vertical nuclear proliferation (especially expansion and modernization of nuclear forces by China and Russia); c) the accelerating lead of US advanced conventional forces inducing horizontal and vertical proliferation by US nuclear adversaries; d) the failure of the great powers to avoid this horizontal and vertical proliferation; and e) the risk of "local" nuclear war, that is, terrorist use of nuclear weapons by non-state actors.[4]

The net result is a more complex relationship between the nuclear forces of the three primary nuclear weapons states, the United States, Russia, and China, with those of second tier (the United Kingdom, France), third tier (Israeli, Pakistani, Indian) and fourth tier emerging (North Korea) nuclear weapons states.[5] Arguably, these global and regional nuclear-threat relationships are increasingly linked, and as a result, the immense risk of global, regional and local (terrorist) nuclear war is rising.

The evolving nature of this risk is reflected in another popular computer game, *DEFCOИ Everybody Dies,* a real-time strategy game released in 2006.[6] Once war begins, all sides take heavy losses ("mega-deaths") but the winner is whoever has the most survivors (fractionally) left on their territory at the end. Survival, not the elimination of opponents in a nuclear shootout as in *Nuclear War*, is the dismal objective of this post-Cold War game.

East Asia is one of the regions that exemplify these global trends and is the geopolitical focus of this essay on the risk of nuclear war and complexity.

This complexity is poorly understood.[7] Western strategic deterrence theory is based on the notion of assured destruction as if the United States is still fighting the bipolar Cold War. The impact of conventional forces on the nuclear proliferation decisions of adversaries and allies remains an after-thought in American doctrinal, budgetary, and war-planning since 1992. Thus, the US nuclear force posture remains triadic with roughly 20-fold overkill relative to a minimum number of warheads required to achieve strategic deterrence against existential threats aimed at the United States or its allies. Meanwhile, US and allied conventional forces have increased the precision and lethality of their munitions by at least two and possibly three orders of magnitude since 1992, while those of potential adversaries (North Korea, Russia) have declined dramatically or are expanding rapidly (China).

Concurrently, the United States has abolished some nuclear missions, substituted conventional forces for the bulk of previously nuclear war-fighting missions in war-plans; and rear-based almost all its nuclear weapons. US conventional forces in Pacific Command operate increasingly in networked manner, exploiting joint, cross-service, and allied inter-operability, and have begun to deploy autonomous aerial, surface and sub-surface naval, and ground vehicles in large numbers. In turn, this net-centric and more agile approach is embodied in the regional "rebalancing" of US

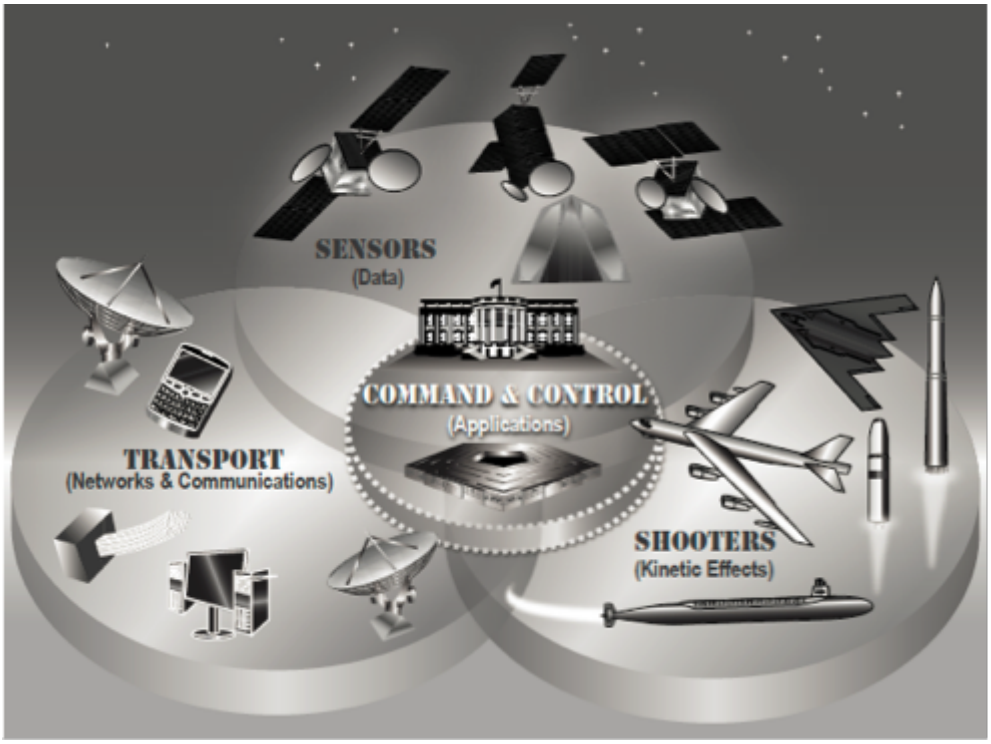
forces and basing options known as the “pivot;” and in the AirSea Battle operational concept. The latter is designed in part to impose the Joint Chief’s control on service implementation of new technologies in forward-deployed forces, especially in the Navy and Air Force. It's implementation in practice may enable US forces to offset some of the area-denial capabilities accruing to China as it grows and modernizes its military. Many of these technologies are emulated by or transferred to US allies at the same time as they are developed and deployed in US forces, resulting in a very high diffusion rate.

A particularly important dimension of this already existing technological transformation is the fantastic proliferation of virtual US command, control, and communications systems and intelligence (C3I), along with the related computers, intelligence, reconnaissance, and surveillance systems (CISR), which when combined with C3I, becomes C4ISR.[8] In US interventions since the Gulf War, the major problem with these systems may be that they provide too much information that overwhelms commanders, damage assessment teams and targeteers. The ironic result is that networked C4ISR systems may deepen rather than overcome the difficulty of services in communicating and coordinating forces involved in regional contingencies or participating in military operations.[9]

A separate flaw, noted by the the US Defense Science Board, is that the US military communications architecture incorporates many foreign-made components loaded with malware and /or counterfeit components.[10] Many of these systems may be vulnerable to cyber-attack, nuclear attack, and conventional attack, and may be far less resilient than networked command-and-control enthusiasts realize.[11] As US Pacific Commander Admiral Locklear stated, “We have built cyber on a house of cards” that could collapse at time of war,[12] forcing PACOM or service commanders to anticipate having to revert to operating separate task forces without the communication and information support needed to execute a net-centric warfare strategy.

Thus, because the C4ISR force multiplier is vulnerable to failure, the conventional force foundation of strategic stability today is brittle. It is also integrates what the Defense Information Systems Agency calls a “patchwork of disparate systems” that includes legacy nuclear-C3I systems run by Strategic Command.[13] Via this patchwork, the virtualized, “horizontally networked” conventional C3I systems that support forward-deployed conventional forces armed with precision-guided munitions of many types, and reliant in some cases on autonomous vehicles carrying sensor systems at the periphery of these vast, dispersed networks, interact with the “vertically segmented” largely teletype and telephone nuclear-C3 systems that still sustain US strategic nuclear forces. Other great and small nuclear armed states follows this pattern to varying extent. As DOD explains, it is attempting to transition the US nuclear-C3I system to become “capable of operating on internet-like networks that provide survivable, reliable support for U.S. Government officials, the U.S. military, and allies, as appropriate,” that is, to operate over net-enabled or net-centric infrastructure that may be cyber-vulnerable to attack or failure.[14] Moreover, the most mature form of complex command-and-control for conventional forces recognizes that each command entity will have their own approach to command-and-control, there will be multiple planning and execution processes, critical information and expertize needed to understand the situation will be non-organic to many entities, and actions to be effective requires developing synergies between entities—all command-and-control attributes that controvert the principle of unified and singular nuclear command-and-control.[15]

[caption id="attachment_41537" align="aligncenter" width="493"]



Source: US DOD, The Nuclear Matters Handbook[/caption]

The Cold War demonstrated that there are multiple possible pathways to nuclear war, including strategically motivated choice to protect vital national interests against unacceptable threats, even against overwhelming odds; inadvertent escalation; and accidental nuclear war. Hypothetical or actual "trigger events" that could have induced states to launch nuclear weapons (but fortunately, were never sufficient to start a nuclear war) included:

1. Dysfunctional and "cybernetic" organizational dynamics in crisis management due to inadequate design or mis-specification or inadequate implementation of procedures;
2. Flawed information and degraded decision-making;
3. Technological component failure in nuclear weapons-system and related C4ISR systems;
4. Accidental nuclear detonation;
5. Warhead loss of control, and/or non-state actor acquisition and use

Trigger events are particularly dangerous if they occur in crisis situations in which states have vital national interests at stake, in which nuclear forces are postured and deployed in a manner that threatens imminent pre-emptive strike aimed at decapitating the leadership of an adversary, and in conditions in which control of nuclear forces could not be assured as soon as nuclear weapons are released for use, including the difficulty of assuring continuing control of the weapons, and of assured communication with nuclear forces at the brink or in the midst or at the end of nuclear war because of the vulnerability of in a national nuclear-C3I systems to disablement by nuclear weapons effects. The pre-eminent example of such a crisis remains the Cuban Missile Crisis. Unfortunately, it is not the only such event in Cold War history.[16]

Each of these trigger events could disrupt implementation of the five core functions of US (and presumably others) nuclear-C3I, namely, force planning (for example, an unanticipated contingency could render all the plans irrelevant due to underlying assumptions and derivative rigid force

deployments); situation monitoring (for example, early warning systems can provide false positives on multiple systems at the same time causing commanders to raise alert levels, thereby increasing the risk of other trigger events coming into play); national command decision-making (for example, attribution of nuclear attack to a state based on a false positive of a nuclear accident in forensic analysis); force direction and management (for example, dual use communication systems may fail at critical junctures; or use of dual-use, networked communication systems rather than dedicated nuclear communications systems such as TACAMO may be misread by nuclear adversaries as an indicator of pending nuclear strike); and force management (poor training and non-implementation of procedure leads to loss of security and assured control of delivery systems and/or warheads).[17]

In a crisis, single or coincident trigger events may increase strategic instability by disrupting the nuclear-C3I system and increasing the propensity of one or more nuclear-armed states to escalate to nuclear attack. Considered separately, each of these types of trigger events were recognized at the time and managed during the Cold War—although there were some near misses that might be ascribed more to good luck than good management. But vast, sprawling nuclear weapons enterprises always posed the possibility that improbable trigger events would occur coincidentally, simultaneously, and concurrently with crisis conditions in which nuclear weapons states were colliding over vital, sometimes existential interests. In such conjunctures, the sheer complexity of the interacting factors was beyond comprehension. At such moments, an otherwise “innocent” singular event such as an accidental nuclear detonation might have prompted a decision to launch pre-emptive nuclear attack.

Today, the primary risk of nuclear war originates in local or regional conventional war, rather than an all-out global nuclear war (one of the real primary Cold War risk pathways). The structure of world affairs today is such that the nuclear-strategic relationships between the nuclear weapons states are largely insulated from direct embroilment in local and regional conflicts that were contested hotly during the Cold War. But the Cold War-era trigger events that could have led to use of nuclear forces are still salient today, only in conditions of greater complexity. Moreover, recent developments in Europe and the deteriorating security relationship between the United States and Russia, and Russia’s pursuit of “hybrid” nuclear-conventional war strategy may have revived some Cold War elements to the global nuclear balance-of-terror that appeared to be recessed in the last two decades.[18]

This essay addresses the relationship between this complexity of nuclear armament and interstate relations witt regard to only one of these trigger events, the interplay of advanced conventional forces with nuclear forces in East Asia via nuclear-C3I system effects, and the impact of this interplay on strategic stability. By the latter is meant the absence of war or major crisis; and in terms of nuclear posture, no incentive to conduct a pre-emptive first strike in a major collision between nuclear-armed states in the region. In this context, a nuclear-C3I system operation is deemed to have operated successfully to the extent to which it reduces the use of nuclear weapons to avoid war in general, and the immediate use of nuclear weapons in a conflict in particular.[19]

Cold War Nuclear Command-and-Control Lessons

During the Cold War, the coupling of national nuclear C3I systems created a “system of systems” that generated the overall risk of system failure and related catastrophic hazard (nuclear war) even if each separate system and all components therein had “worked.” American regional and service commands were devolved and decoupled, dampening error propagation. Soviet systems, by contrast, were centralized, integrated, and rapidly propagated error. American and Soviet early warning systems became increasingly capable at the same time as missiles reduced warning and decision-making times to almost zero. Compound drivers, sometimes the combination of unanticipated interactions and multiple human and technical errors, triggered organizational, bureaucratic, and

military responses based on incorrect diagnoses of apparent attacks, in turn prompting actions that were unrelated to reality, or even worse, accelerated mobilization and alert levels.[20] US and Soviet nuclear command-and-control posts and supporting systems were vulnerable and could not provide assured communications to guarantee a retaliatory response to a pre-emptive nuclear strike, even after decades of upgrades, reducing confidence that national command authorities could control their nuclear forces before, during or after a nuclear war.[21] Thus, nuclear C3I was both cause and effect of the risk of nuclear war.

A critical issue is to what extent lessons from periodic Cold War nuclear "near miss" experiences are salient to post-Cold War conditions in which this concurrent modernization of nuclear command-an--control systems by some nuclear weapons states and deterioration of these systems in other nuclear weapons states? Do any of their nuclear weapons forces exhibit the organizational performance required to operate nuclear weapons forces reliably and to necessary standards of safety and control?[22]

Impact of US Advanced Conventional Weapons on Regional Military Forces

Before the Cold War, nuclear weapons were briefly treated as an extreme type of conventional weapons. During the Cold War, they became a class apart, and strategic forces were largely segregated from conventional forces. After the Cold War ended, the United States exploited the complementarity of conventional and nuclear weapons where it was introduced in the "new triad" (2001) that explicitly outlined how conventional forces bolster nuclear strategic deterrence, rendering the latter less important and in some cases, unnecessary. This posture was conceptually enshrined in the 2010 Nuclear Posture Review and resulting presidential guidance as to how the US should reform its nuclear forces.

Thus, for the United States, overcoming the area-access-and-denial capacity of Chinese naval, air and missile forces drives the deployment of networked communication and data-intensive systems over vast distances, across domains, between services, and among allies and coalition forces. Accordingly, since the early 1990s, the US military sought to foster a joint information environment in which common standards, protocols, software, servers, and routers in space, on bases, on aircraft and on ships, enable forces to communicate seamlessly across the full range of functional requirements, while offering the ability to secure and protect this network against cyber-attack, all at affordable cost in an era of massive budget cuts. Pacific Command seeks comprehensive and "plug-and-play" interoperability between services and with allies (although this is unlikely to ever be achieved because when disparate systems are connected, cross-cutting system properties arise that disrupt inter-operability anew).

The United States is modernizing its nuclear and conventional C4ISR systems[23] but these systems remain as or even more vulnerable today in many respects as they were during the Cold War. In contrast, the Russian nuclear command-and-control system is degrading, especially its early warning component (which has only begun to improve recently after many years of decay[24] but as of writing, relies solely on ground radar[25]) even as it re-emphasizes the role of nuclear weapons in its security posture.[26] China is also modernizing its nuclear command-and-control system, but it is interwoven increasingly with conventional forces.[27] North Korea's nuclear command-and-control imperative may pose particular problems for a regime as personalized and centralized as found in the DPRK. Accordingly, the DPRK's nuclear-C3I system is a source of instability and unknown contingencies for all states in the region.[28] All states in Northeast Asia with the notable exception of North Korea are upgrading and overhauling their conventional forces, and shifting towards networked strategies that rely upon highly connected technical systems, subject to all the dynamics noted earlier.

From the viewpoint of US adversaries, deployed or developing US conventional capacities such as missile defenses, prompt global strike technologies, submarine, naval surface, and aerial long range and networked drones; and, deployment of new intelligence capabilities such as underwater surveillance from space may threaten their nuclear forces with a disabling first-strike. Although no American leader would entertain this option, in theory at least, the United States could strike first to try to limit damage from a pending attack on the US and/or its allies, or in order to execute a decapitation strike as part of a preventive war, even against Russian nuclear forces today.

For small nuclear-armed states (such as North Korea), obtaining and fielding nuclear weapons may appear to be the most powerful response in the face of US-ROK-allied conventional forces. In such cases, nuclear weapons may encourage a small state to undertake low-level overt and covert military actions in the belief that the threat of nuclear escalation limits any possible retaliatory response. This posture also increases the risk of war; *and*, increases the propensity of such a state to use nuclear weapons first (at least in a limited manner) should conventional retaliation exceed this threshold and threaten the existence of this state.

Even for China, it is possible that the only way it could stop a US carrier group steaming toward its coast at 30 knots would be by bracketing it with 10-12 airburst nuclear weapons. Indeed, China may be increasing its relianceon nuclear weapons in the context of countering the increased lethality and precision of US conventional forces in the western Pacific.[29]

In East Asia, advanced conventional forces have the biggest impact on the risk of nuclear first-use in four conflict situations, namely, in Korea, in the Taiwan Straits, in “trigger” situations such as contested islands or unanticipated contingencies, and especially after a mega-terrorist attack by a non-state actor. In all four cases, how conventional forces affect the perception of immediate threat, the control of forces, and the execution of countervailing strategies determines the risk of escalation to war and thence to nuclear war, assuming that the pathway to nuclear war is via conventional conflict rather than a nuclear first-use without prior conventional combat. In these contexts, the decision to escalate further depends as much upon how the nuclear-C3I system performs as it does on the direct impacts of use of nuclear or conventional forces on the battlefield, which may be purely hypothetical, shrouded in ambiguity, or completely unknown. These decisions rely on the respective command and control systems of the political-military leaders of states that are party to these major conflicts, and their respective communications, intelligence, surveillance and reconnaissance systems, which in turn feed them streams of data and analysis on the posture, position, and status of countervailing nuclear and conventional forces that pose the threat of first-use.

This interplay of conventional and nuclear forces and their C4ISR systems generates a set of cascading critical research questions. To what extent are US, allied, and adversary militaries rebuilding their respective communication, intelligence, and computer systems to support their respective conventional and nuclear command and control functions? What are the critical military imperatives that shape these choices? And do the resulting architectures reflect the threat posed by conventional forces in ways that contribute to strategic instability, that is, would increase the fear of pre-emptive strikes by adversaries at the brink of a war?

Interplay of US Nuclear and Conventional Command and Control Systems

The United States, its allies and security partners, and its potential adversaries such as China, have implemented modernization programs to their respective nuclear command-and-control systems, and by linking them to formerly segmented nuclear forces, introduced new levels of complexity and vulnerability to these decision-support systems.[30] In some cases, conventional and nuclear forces are loaded on the same delivery platform. The US nuclear command-and-control system increasingly supports many conventional mission requirements, not only uniquely nuclear forces. The current

system supports at least five different functions (listed above),[31] and some of these may compete with each other organizationally for resources, command attention, and strategic priority.

However, until the upgraded American nuclear C3I system is fully operational and thousands of legacy systems are retired (as recommended by the US Defense Sciences Board[32]), it also poses the possibility that not only will cyber-attackers gain access to these networks and disable significant portions of it when it is most needed, but it may also propagate failures across the whole system, conventional and nuclear. To the extent that dual use platforms are used to support nuclear missions, the risks of cyber-disablement entering into nuclear forces are real, and suggest that dual use platforms and decision-support systems for conventional and nuclear systems are a high-risk proposition for all national nuclear commands.

The emergence of a meta-system of nine national nuclear command-and control systems (plus linked sub-national non-state actors with their own crude nuclear command-and-control systems) is what makes the post-Cold War nuclear war management issue so complex. It gives rise to a series of sobering questions to which no one has an answer today including: what are the performance requirements in virtual nuclear command-and-control (and related CISR) systems in organizations that must meet near perfect standards to avoid catastrophic failure (such as nuclear accidents or war)?[33] How well is the social enactment of such exacting systems understood in militaries heavily reliant on automated and computerized control systems? Do these systems give rise to the illusion of central control over conventional and nuclear operations?

Relatedly, organizational experts as La Porte argue that tacit knowledge and cultural factors are critical to avoiding catastrophic failure in complex technological systems.[34] The distinct organizational cultures of the US, Russian, Chinese and DPRK militaries and their related CISR systems are poorly understood. Given their substantial differences in style and performance, what are the implications for strategic stability that arise from their interaction, and what should be done to rectify organizational differentials—especially their possibly matching rather than offsetting deficits that could generate trigger events or amplify the effects of such events in a crisis?

What Measures Reduce the Risk of Nuclear War Arising from this Interplay?

The issues outlined above pose serious questions about how best to manage this meta-system rather than leaving it to each national nuclear-C3l system to fend for itself. It is sobering to recognize that many high-technology systems fail even though individual components perform perfectly as designed. Tightly coupled systems are even more daunting to manage, especially when components are allowed to interact in ways that may be harmful to the operation of the system, and may defeat each other without the slightest intention of the system designers or operators (as occurs, for example, in mid-air civilian airliner collisions). Thus, improving the organizational performance of national nuclear organizations, as is currently the focus of the US Air Force in the aftermath of loss of control of live warheads, cheating in performance reliability tests, and removal of senior commanders due to unstable behavior, while laudable and necessary, is not sufficient to manage the risk of nuclear war in contemporary conditions. Such improvement, if implemented in a nuclear-C3I system that propagates error, could even increase overall probability of a decision to escalate to nuclear war.

Some general principles aimed at improving system safety, especially via retrofit for systems that have been built and deployed already, may be salient. In particular, finding ways to minimize “live” contact by ensuring physical separation and decoupling of these systems may be useful, implying a range of spatial and temporal “rules of the road” not only for delivery platforms such as bombers, submarines, surface vessels, and even missiles (relative to missile defense systems); but also the location and separation of the sensors and platforms supporting the ISR components that provide

almost instantaneous battlespace awareness that may be misconstrued by users unaware of context at point of collection, or misled by various layers of intermediation and misinterpretation due to algorithms and human processing at various nodes in the system.

Some exemplary steps to this end are separation of nuclear and conventional weapons stockpiles; of warheads from delivery systems; and of nuclear from conventional command-and-control as well as CISR systems that support nuclear command-and-control functions. Agreements and procedures to separate military forces may also reduce the risk of physical contact. Clear operational procedures are also needed when these forces be co-located or operated in close proximity. Coordination of activity and commands on a constant basis is often valuable both in identifying existing and potential arenas of conflict. Transparency with regard to the capacity and deployment of conventional and nuclear forces may also increase confidence and reduce propensity to use conventional or nuclear forces.

In terms of nuclear and conventional decision-making, slowing down the speed at which nuclear C3I systems work may reduce the data overload, sorting, and recognition problem created by ubiquitous virtual CISR decision-support systems. Doing so may seem counter-intuitive given the decades of effort and billions of dollars devoted to overcoming the shortage of time for critical decisions. Given the 5-15 minute time that would elapse between early warning for submarine-launched missiles and detonation over the heads of decision-makers, the pressure has usually been to provide more and more accurate data almost instantaneously. However, such short decision times make more or less data, whatever its quality, only partly useful, and may also lead to false confidence and overly decisive decisions in the face of radical uncertainty created in part by the support systems themselves that could drive decision-makers to the nuclear brink. The provision of impartial third party information may be particularly helpful in this regard, either by disinterested parties in various types of supervisory commissions; or via intergovernmental agencies (the long-standing Canadian proposal to establish a space-satellite intelligence system run by the United Nations springs to mind, as does converting the US intelligence bases at Pine Gap from servicing only the United States and its senior allies to a broader consortium of users on a cooperative security basis). The goal is to slow events and gain real time so that all states party to a conflict can avoid the brink altogether.

At a higher level of collaboration, as against merely improving communication and coordination as suggested above, it is worth asking what maritime, aerial, and land-based confidence building measures involving the nuclear and conventional forces US, its allies, China, Russia, and North Korea could reduce the risk of nuclear war triggered by conventional war? Foregoing classes of conventional weapons, area exclusions such as anti-submarine warfare-free or nuclear weapons-free zones, and other approaches used in European conventional arms limitation agreements with the former Soviet Union during the Cold and post Cold War, may establish some elements of joint management that curtail threatening behaviors and limit capacities for all players in the region to induce strategic instability between nuclear-armed states.

Collaborative and even interoperable military C3I and even CISR systems may be constructed with possible nuclear adversaries for peacetime humanitarian and disaster response operations in order to determine if they work together under stress. These could prove invaluable in providing for communication channels that slow decision-making in times of high tension or when combat-support systems are committed, over-whelmed, or collapsed. Other generic safety design principles that might be drawn from the engineering systems analysis and applied in the realm of nuclear-C3I are simplicity, non-cyber backups, and separation of critical from non-critical sub-systems.[35] Thus, for example, the US Defense Science Board suggests that some currently dual-use strategic bombers be dedicated solely to nuclear missions; and that strategic submarines that are already almost completely separated from connectivity during deployment be a primary launch platform.[36] (Of

course, this separation ducks the issue of the vulnerability to failure or mal-performance of all the "thin" wartime nuclear-C3I systems that direct these delivery platforms to position and fire their nuclear weapons).

One empirical survey of network information effects in a modern conventional military (Australia) noted that devolution of authority is a necessary attribute of effective empowerment of lower level units, but this devolution is likely to be accompanied by misinterpretation that cuts across clarity of intent. The authors concluded: "The longer and more complex the C2 line, the greater the opportunities for minor distortions and the greater may be the sum of those distortions."[37] These results suggest that a dedicated nuclear-C3I with shorter and simpler lines of command and control may be least susceptible to loss of clarity of intent and to distorted information transmission than one that has long lines of communication that intermingles with conventional CISR systems.

Conclusion

Many observers have noted the analogy between the situation leading up to the outbreak of World War I and today. However, there was no equivalent at that time to the existence of nuclear weapons today. In comparison, events moved at a glacial pace compared with the seconds, minutes, and hours, and at most, days, in which a nuclear war would start, be fought, and end. And, information moved relatively slowly in the pre-digital era.

Where the analogy may be apt is the fact that the trigger event that led to World War I was not anticipated at the time. Similarly today, very few leaders or even strategic scholars pay attention to the new complexity of the operating environment in which national nuclear command-and-control systems operate. There are very few modern or post-Cold War studies of the new characteristics of the command-and-control systems and their supporting CISR systems that may contribute to the problem of loss-of-control and rapid escalation to nuclear war in spite of all the putative caution-inducing attributes of nuclear weapons, including the multiple safety and control systems that might disable their usage even if ordered.

Just as we now live in one global city in which New York is a suburb of Karachi, Kiev is a suburb of Melbourne, and Tokyo is a suburb of Lagos, so we now live in a globalized world of states armed with nuclear weapons. Albert Wohlstetter famously called this living in a nuclear-armed crowd.[38] However, this phrase doesn't capture the modern meaning of a globalized nuclear-armed world which goes far beyond the nth-country problem of horizontal proliferation by states. The problem is more akin to managing nuclear weapons in a world of hyper-connectivity, perhaps characterized as one of Millennials nuclear command-and-control. It is also one that is embedded in the broader social context. To my knowledge, no-one has examined how smart-phone equipped nuclear missile silo operators may interact via social media such as Twitter to add a non-military form of early warning that may move even faster than satellite and radar based early warning systems, to transmit information into nuclear-C3I systems.

Today, the underlying ground is moving beneath the feet of nuclear-armed states. The enormous flow across borders of people, containers, and information, and the growth of connectivity between cities, corporations, and communities across borders, is recasting the essential nature of security itself to a networked flux of events and circumstances that no agency or state can control. The meta-system of nuclear command-and control systems has emerged in this new post-modern human condition.

The humbling truth is that strategic analysts have no clue as to what unanticipated event or events in combination may trigger nuclear war in the 21st century. It behooves us to start thinking about it.

III. References

[1] "Nuclear War" developed by New World Computing and released by Amiga in 1989.

[2] Details of these attempted or considered usages are found in: P. Hayes *et al*, *American Lake, Nuclear Peril in the Pacific,* Viking Penguin, New York, 1987 (available in four parts here, scan down to 1987); P. Hayes, *Pacific Powderkeg, American Nuclear Dilemmas in Kor*ea, Lexington Books, 1990; and "Essentially Annihilated," the Nautilus Institute website that recounts and documents the 1967 Jason study of the possible use of nuclear weapons in the Vietnam War.

[3] Lt. General James Kowalski, transcript, NDIA/AFA/ROA July 31, 2013 breakfast forum.

[4] P. Morgan, *Deterrence Now*, Cambridge University Press, 2003.

[5] During the bipolar maximum Cold War, the number of active mutual nuclear threat relationships was seven (between the US, UK, France, former Soviet Union, and China, treating NATO and Warsaw blocs as part of their superpower uber-ally), it went up to ten (before Pakistan went nuclear in 1998) and is now sits at sixteen (after Pakistan and North Korea went nuclear but some states in allied blocs were de-targeted; note all these figures relate only mutual nuclear threat dyads. Israel's nuclear targeting of non-nuclear states is not included, for example). Over the same period, the number of nuclear-armed states went from one (1945) to nine today (ten states were nuclear-armed at some point, but South Africa dropped out); and the number of targeted states (again, treating the Cold War blocs as one each) has increased from one (former Soviet Union in 1945) to thirty-one today. This complexity is compounded further by the addition of non-state nuclear targets by at least the United States; and the potential risk that non-state actors could target states.

[6] Introversion Software, *DEFCOИ*, 2006.

[7] See P. Morgan *et al*, *Complex Deterrence*: *Strategy in the Global Age*, University of Chicago Press, 2009.

[8] The best unofficial overview of the current nuclear-C3 system is "Nuclear Command, Control and Communications System," Chapter 4 of The Nuclear Matters Handbook, Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs, US Department of Defense, 2011.

[9] As recounted in US Air Force, *Gulf War Airpower Survey*, volume 1, part II, Command and Control, Washington DC, 1993.

[10] Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat*, DSB Task Force on Resilient Military Systems and the Advanced Cyber Threat, January 2013, p.4.

[11] For example, most military communications to Korea were unavailable after the March 2011 earthquake in Japan which cut or damaged 8 undersea cables and reduced to 3% normal commercial connectivity to Japan. If this event had coincided with war in Korea, US communications to support the Korean theater would have been stretched thin. See G. Seffers, "Tsunami Short-Circuits Military Communications in Japan and South Korea," *SIGNAL Online,* March 23, 2011.

[12] R. Ackerman, "Asia-Pacific Challenges Reshape US Military needs," *Signal,* December 4, 2013.

[13] DISA uses the phrase “patchwork of disparate systems” in response to question 1, Defense Information Systems Agency, “Nuclear Command, Control, and Communications System Operational Assessment Program,” Solicitation Number: HC104710R4009, August 1, 2010.

States DISA: “Included in the Nuclear C3 System are the Survivable Mobile Command and Control Centers consisting of airborne resources, selected fixed and mobile ground command centers, the strategic and non-strategic (theater) nuclear forces, and surviving command elements (including shipboard) of the nuclear and non-nuclear Combatant Commanders, the military services, and the DoD agencies as defined in the Emergency Action Procedures of the Chairman, Joint Chiefs of Staff (EAP-CJCS Volumes VI and VII) and the National Military Command System/Department of Defense Emergency Communications Plan (NMCS/DoD Emergency Communication Plan).”

[14] “Nuclear Command, Control and Communications System,” Chapter 4 of The Nuclear Matters Handbook, Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs, US Department of Defense, 2011, p.53.

[15] See D. Alberts, “Module 3, Complex Endeavors, Networked Enabled Command and Control Short Course,” October 2009.

[16] P. Lewis et al, “*Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy*” Royal Institute of International Affairs, April 2014.

[17] The five functions are delineated in “Nuclear Command, Control and Communications System,” Chapter 4 of The Nuclear Matters Handbook, Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs, US Department of Defense, 2011, pp. 54-55.

[18] “Topol, Yars ballistic missile launchers on combat patrol in 6 Russian regions,” TASS Russian News Agency, February 4, 2015; A. Croft, “Russia's nuclear strategy raises concerns in NATO,” *The Independent*, February 5, 2015; A. Golts, “Russia is Preparing for a New Arms Race,” *Moscow Times*, December 15, 2014; “Russia’s National Defense Control Center officially takes up combat duty,” TASS, December 1, 2014.

[19] See E. Colby, M. Gerson, *Strategic Stability, Contending Intepretations*, Strategic Studies Institute, U.S. Army War College Press, February 2013.

[20] Paul Bracken, “Instabilities in the Control of Nuclear Forces,” in A. Gromyko, M. Hellman, ed, *Breakthrough, Emerging New Thinking*, Walker and Company, New York, 1988.

[21] L. Wainstein et al., *The Evolution of U.S. Strategic Command and Control and Warning, 1945-1972,* Institute for Defense Analyses, June 1975, p. xxvi; Joint Chiefs of Staff, Historical Division, *Joint Chiefs of Staff Special Historical Study, A Historical Study of Strategic Connectivity, 1950-1981* July 1982; R. Finkler, *Command, Control, and Communication Problems,* Weapons Systems Evaluation Group WSEG 159, IDA, 1971.

[22] This section draws on the parallel conceptual literature on risk and regulation in industry and technological design. See the special issue of *Risk and Regulation* on “Close Calls, near Misses and early Warnings,” ESRC Centre for Analysis of Risk and Regulation, July 2010 as well the many accounts of nuclear new misses such as P. Lewis et al, “*Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy*” Royal Institute of International Affairs, April 2014. For reliability culture and high performing organizations with strong parallels to the operating standards required of nuclear weapons organizations, see T. La Porte, “High Reliability Organizations: Unlikely, Demanding and At Risk,” *Journal of Contingencies and Crisis Management*, 4:2, June 1996,

p. 64. Note that the issue here is not one of nuclear safety in operating nuclear forces, although that is one important component of reliability in that unsafe nuclear weapons and delivery systems could generate a "trigger event" that increases the risk of war in a crisis. Rather, the issue is whether any human organization over long periods of time can ever sustain the performance required to avoid shortfalls or unintended outcomes that may contribute to the risk of nuclear war by undermining strategic stability.

[23] G. Seffers, "Modernizing Nuclear Bomber Command and Control," *Signal*, May 1, 2014.

[24] "Russia to restore space echelons of missile defense system," TASS, October 30, 2014.

[25] "Russian Nuclear Missile Detection Capability Limited by Satellite Launch Delays," *The Moscow Times*, February 11, 2015

[26] S. Blank, ed, *Russian Nuclear Weapons: Past, Present, And Future,* Strategic Studies Institute, November 2011; and D. Hoffman, "The Russian Nuclear Button, New questions about the Soviet legacy of three briefcases," Foreign Policy, May 27, 2010.

[27] S. Polk, "Chinese Nuclear Command and Control," in *China's Nuclear Force Modernization*, Lyle Goldstein, *ed*, Naval War College Newport Papers 22, 2005, p. 17.

[28] J. Meyerle et al, *Nuclear Weapons and Coercive Escalation in Regional Conflicts, Lessons from North Korea and Pakistan*, CNA, Research Memorandum, November 20, 2014.

[29] See Li Bin, "Major problems with minimum deterrence," *The Bulletin of the Atomic Scientists*, Roundtable, August 21, 2014.

Also, L. Worzel, *China's Nuclear Forces: Operations, Training, Doctrine, Command, Control, and Campaign Planning*, Strategic Studies Institute, US Army War College, Pennsylvania, May 2007.

And L. Saalman, "Placing a Renminbi Sign on Strategic Stability and Nuclear Reductions," pp. 347-350, 357-361, 368, in E. Colby, M. Gerson edited, *Strategic Stability: Contending Interpretations*, Strategic Studies Institute, US Army War College, February 2013.

[30] Robert Critchlow, *Nuclear Command and Control: Current Programs and Issues*, Congressional Research Service, RL33408, May 3, 2006, pp. 24-25.

[31] GAO lists these as: Situation monitoring: collection, assessment, and dissemination of information on friendly forces, adversary forces and possible targets, emerging nuclear powers, and worldwide events of interest; Planning: development and modification of plans for the employment of nuclear weapons; and other options; Decision making: assessment, review, and consultation on the decision to use nuclear weapons and for supporting operations; Force management: assignment, training, deployment, maintenance, and logistics support of nuclear forces before, during, and after a crisis; Force direction: implementation of decisions regarding the execution, termination, destruction, and disablement of nuclear weapons. See General Accounting Office, *Nuclear Command, Control, And Communications: Review of DOD's Current Modernization Efforts*, GAO-1--414R, March 18, 2014.

[32] Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat*, DSB Task Force on Resilient Military Systems and the Advanced Cyber Threat, January 2013, pp. 82-83.

[33] See Karen Marais, Nicolas Dulac, and Nancy Leveson, "Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems,"

Engineering Systems Division Symposium, MIT, Cambridge, MA, March 29-31, 2004. Leveson offers a whole framework for examining system hazard as against component level hazard, see N. Leveson, *Engineering a Safer World, Systems Thinking Applied to Safety*, The MIT Press, Cambridge, Massachusetts, 2011.

For analysis of multiple control systems analogous to linked national nuclear command-and-control systems, see T. Ishimatsu, N. Leveson, C.Fleming, M. Katahira, Y. Miyamoto, and H. Nakao, "Multiple Controller Contributions To Hazards," paper to *Conference of the International Association for the Advancement of Space Safety* , Versailles, France, October 2011.

[34] T. La Porte, "High Reliability Organizations: Unlikely, Demanding and At Risk," *Journal of Contingencies and Crisis Management*, 4:2, June 1996, p. 64.

[35] I am grateful to Nancy Leveson for these points.

[36] Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat*, DSB Task Force on Resilient Military Systems and the Advanced Cyber Threat, January 2013, pp. 82-83.

[37] C. Pascoe, I. Ali, "Network Centric Warfare and the New Command and Control: An Australian Perspective," Defence Science Technology Organization, presentation to 13th International Command and Control Research and Technology Symposium, 2008.

[38] See A. Wohlstetter *et al*, *Moving Toward Life in a Nuclear Armed Crowd?*, Pan Heuristics report to US Arms Control and Disarmament Agency, 1975.

VI. NAUTILUS INVITES YOUR RESPONSES

The Nautilus Peace and Security Network invites your responses to this report. Please leave a comment below or send your response to: nautilus@nautilus.org. Comments will only be posted if they include the author's name and affiliation.

View this online at: https://nautilus.org/napsnet/napsnet-special-reports/nuclear-command-and-control-in-the-millenials-era/

Nautilus Institute
608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org