TECHNOLOGY FOR GLOBAL SECURITY

NC3 IN A MULTIPOLAR NUCLEAR WORLD

BIG STRUCTURES AND LARGE PROCESSES

DR. PAUL, BRACKEN
YALE UNIVERSITY
May 14th, 2019

NC3 IN A MULTIPOLAR NUCLEAR WORLD: BIG STRUCTURES AND LARGE PROCESSES

PAUL BRACKEN
MAY 14, 2019

I. INTRODUCTION

In this essay, Paul Bracken analyzes the big structures and large processes of nuclear multipolarity. The structures include the national command and control of at least eighteen countries, to include nine nuclear weapon states, "shared" weapons in NATO, missile defense, and key intelligence nodes in select countries. Processes include the delegated flow of launch authority, innovation, and digitization in many forms. A framework for analyzing this global system is developed, one made up of national command and control plus the "system dynamics" of their interlinked behavior.

Paul Bracken is professor of management and political science at Yale University.

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

A podcast with Paul Bracken, Philip Reiner, and Peter Hayes on NC3 in a multipolar world is found here.

Banner image is by Lauren Hostetter of Heyhoss Design.

CITATION

Paul Bracken, "NC3 in a Multipolar Nuclear World: Big Structures and Large Processes," *Tech4GS Special Reports*, May 14, 2019, https://www.tech4gs.org/nc3-systems-and-strategic-stability-a-global-overview.html

II. TECH4GS SPECIAL REPORT BY PAUL BRACKEN
NC3 IN A MULTIPOLAR NUCLEAR WORLD: BIG STRUCTURES AND LARGE PROCESSES
MAY 14, 2019

Summary

This paper analyzes the big structures and large processes of nuclear multipolarity. The structures include the national command and control of at least eighteen countries, to include nine nuclear weapon states, "shared" weapons in NATO, missile defense, and key intelligence nodes in select countries. Processes include the delegated flow of launch authority, innovation, and digitization in many forms. A framework for analyzing this global system is developed, one made up of national command and control plus the "system dynamics" of their interlinked behavior. The paper underscores how advanced technologies — cyberwar, drones, and anti-satellite weapons (ASAT) —affects NC3.

The paper specifically assesses the two big structures that are forming in Europe and Asia. NATO is attempting to modernize its nuclear deterrent for the new realities of European security. In Asia, a pentapolar structure of major powers (United States, Russia, China, India, and Japan) has growing nuclear interactions: in missile defense, cyber, space, and in upsetting the U.S.–Russia strategic balance. The critical importance of information transfer for bolstering a coalition member's ability to target its nuclear forces is analyzed as an example of the "new" dynamics of multipolarity.

That a conference on nuclear command, control, and communications (NC3) is being held at all says a lot about the world we are in.[1] After the Cold War the overwhelming emphasis in the United States and Europe was on nuclear non-proliferation. Non-proliferation had wide support. I would argue that it had more bipartisan support than any other policy, whether in economics, health care, or protecting the environment. In these fields there were disagreements on goals as well as ways to reach them, but not in opposition to non-proliferation or the reduction of the role

[1] In preparing this paper, the author reviewed the 28 papers presented to the "NC3 SYSTEMS AND STRATEGIC STABILITY--A GLOBAL OVERVIEW WORKSHOP," Stanford University, January 28-29, 2019. This essay was prepared after the workshop. In some instances, the author refers to presentations at the workshop by mentioning an author in brackets rather than providing a formal citation. In such references, the full paper by this author will be published in the NC3 Systems and Strategic Stability Project papers that are forthcoming from Nautilus Institute and Technology for Global Security.

of nuclear weapons in American security policy. Hawk, dove, Republican, Democrat, liberal, conservative — it didn't matter. All were on board opposing nuclear weapons.

In the late 2000s the abolition of all nuclear weapons even seemed to be coming. President Barack Obama backed this goal. So did the foreign policy establishment. Henry Kissinger, George Schultz, Sam Nunn, and William Perry all supported "global zero" — that is, the elimination or sharp reduction of nuclear weapons for all countries, including the United States. Academics, think tanks, and intellectuals quickly jumped onto this bandwagon.

Yet here we are at a workshop on how to *operate* these forces — now for nine countries. The papers at this workshop analyze the command and control systems of major powers like the United States and of secondary powers like Israel and North Korea. They also explore new issues like the way that cyberwar could paralyze this command and control. And they examine new pathways to escalation in a world that is both nuclear and high tech.

The change in focus from non-proliferation and reduction to operations and command and control reflects an historical change. We are seeing a new security order take form, one that I've called a second nuclear age.[2] U.S. policy, along with others, is *responding* to this change. In this paper I describe a global perspective on the challenges of this new security order. My framework goes beyond the U.S.–Soviet stability paradigm of the Cold War. It offers a framework for how national command and control systems will interact with each other based upon interlinkages and connectivity created by new advanced technologies. This global system is made up of the national systems that have been so carefully analyzed at this workshop.

Big Structures and Large Processes

The world that we are in is *not* simply nuclear *and* multipolar. This description is fine as far as it goes. But it leaves out one critical element, namely, the system dynamics that this global structure produces. We do not know yet what these dynamics are. In order to get at these dynamics, I've chosen a framework consisting of two macro elements: big structures and large processes. By *structures* I mean the relatively enduring parts of a system, namely those that last over years and decades, and which bear on matters of defense and international order. Examples

[2] Paul Bracken, *The Second Nuclear Age, Strategy, Danger, and the New Power Politics* (New York: Times Books, 2012).

are the best way to illustrate the notion of big structures. As described in a masterful way by Henry Kissinger, the Congress of Vienna was the structure devised to keep European order following the defeat of Napoleon.[3] To make it work other big structures were developed: the Royal Navy, the Prussian Army, and later, the German General Staff. These big structures and their follow-on institutions were also important in the two world wars. On the American side I could add "Detroit" as a key structure in World War II. This was the huge U.S. industrial production system which was repositioned from commercial to war goods.

The big structures of the Cold War included NATO, the Strategic Air Command, the Soviet Army and Strategic Rocket Forces, etc. One could add arms control to this list, in that arms control as an institution endured over many decades to constrain nuclear weapon developments.

Processes are defined as flows of work or information. Important examples of processes relevant to nuclear multipolarity are the flow of launch authority for nuclear and cyber weapons, innovation, and digitization. The flow of authority in a command and control system for launching nuclear, cyber, or other weapons is now taking shape in several countries. Here, the "work" flow is the authorization to fire weapons. As this paper will argue, launch authority is an elementary institutional arrangement. Even established nuclear powers are revisiting this arrangement. New threats arising from cyber, hypersonic missiles, and disrupted communications, along with debate about the "stiffness" of nuclear triggers, are causing a rethink of this issue in many countries.

Innovation is also a very important process. The *institutionalization* of innovation was a distinctive invention of the Cold War. For the first time whole organizations were established by governments in peacetime to exploit science and technology for military purposes. Lawrence Livermore Laboratory, DARPA, and the Naval Research Laboratories are examples. Today, digitization is a major process in the armed forces of many countries. A raft of new organizations has been created (U.S. Cyber Command, Unit 61398 in the Chinese PLA) to do this.

[3] Henry Kissinger, *A World Restored: Metternich, Castlereagh, and the Problems of Peace, 1812-1822* (New York: Grosset and Dunlap, 1964).

Today big structures and large processes are transforming international security. They need to be identified. More, the multipolar nuclear order needs to be mapped out in terms of the complex relationships between these structures. This is similar to analyzing the European security order following Napoleon, which required a comparable identification and mapping exercise. The same could be said for mapping out World War II and the Cold War. Today, big security institutions need to be looked at in terms of their evolution and enduring character. We need to move away from overreliance on short-term thinking about them for the very good reason that they are not going away anytime soon.

These structures will be directed by governments for various purposes. Yet, like all complex organizations they have their own goals. Today, for example, a great concern in many countries is whether their intelligence services are up to the task of improving the performance of the legacy armed forces, the army, navy, and air force. Cyberwar is integrated into the operation of these forces. There are also national programs – "moonshots" – to advance a nation's innovation capability in cyber, artificial intelligence or AI, and quantum computing. Another example of a large process is the intelligence estimation of North Korea's two moonshots, in missiles and a hydrogen bomb. Both of these programs were badly underestimated by Western intelligence as to how long it would take to acquire them.

Nuclear command and control structures are new in many countries (North Korea, Pakistan) because their nuclear weapons are new. They are only taking shape now. For advanced countries one of their central concerns is how innovation and digitization will impact their own nuclear deterrents. How a new system dynamic will affect crisis management, early warning, escalation, and deterrence in a world where most major powers have the bomb, and where smaller nuclear countries also have it, is the central question of our age for everyone.

The Basic Structure of Nuclear Multipolarity

When we say that a nuclear multipolar world has developed what is meant, quite simply, is that nuclear weapons have spread to many countries whose leaders exercise control over their weapons. Since multipolarity is such a basic feature of the structure of the developing security order, it's worth specifying in more detail what is being said.

Three features of this multipolar structure stand out. First, the actors in this system are *sovereign* states the leaders of which can do pretty much what they want inside their own borders. They can choose to get the bomb or not. They can decide to MIRV (multiple independently targetable reentry vehicle) their missiles or develop tactical nuclear weapons. *Multipolarity* is an important concept precisely because different states will choose different answers to these choices.

Short of world government or global hegemony by one state over all the others, we are in a world of relatively independent national decision-making units. Restraints once sharply limited this independence, like technological backwardness or bloc membership. But today these are less powerful constraints than they were in the 20th century.

It might be added that this *multipolar* perspective rules out other possible structures for world order. For example, I see little prospect for a clash of civilizations because it is *countries*, not *civilizations*, the leaders of which control the "trigger" of using military force. This national trigger is what command and control is all about.

Second, multipolar systems are not new. As Henry Kissinger wrote, Europe after Napoleon and also in the first half of the 20th century were multipolar systems. Most of the time states in multipolar worlds behave in a conservative, risk avoiding, or at least risk managing way. Diplomacy in multipolar systems was usually about preserving stability, defined as not falling into a large war. But not always, as World Wars I and II showed.

What is new about *nuclear* multipolar systems is not only that they have atomic weapons, in the sense that most major powers in them have the bomb (the United States, China, Russia, and India). It's that advanced technologies introduce new system dynamics into the system that transcends diplomacy. This is a theme of many of the papers at this workshop: that technology has raced ahead of diplomacy. Another way of saying this is that *national leaders do not really understand their own forces*. Cyber, space, electromagnetic pulse, drones, AI, stealth, etc., so radically change operations that getting diplomacy in synchrony with them is extraordinarily difficult. As some papers argue, and as participants have pointed out to me, even senior military leaders may not understand their own forces because of the disruptive impact of advanced technology, and because legacy, archaic command and control systems are unable to manage the new dynamics of the technologies. Legacy command and control systems may be incapable of

dealing with the demands of advanced technology operations or the stress of complex interactions between so many nuclear command systems. The multipolar order, in effect, puts a nuclear context on poorly understood system dynamics. *It widens the gap between the military and diplomatic behavior.*

Third, and finally, in a world of multiple independent decision-making centers, coalitions take on renewed importance. This is the lesson from common sense, history, and game theory. In a dangerous world it won't be every country for itself, but rather a competition between coalitions. The Cold War had coalitions, it is true. But these (NATO, Warsaw Pact) were better seen as tautly disciplined blocs dominated by the two superpowers. This was overwhelmingly so when it came to nuclear weapons.

It's very different now. Holding coalitions together, extending deterrence to them, and driving wedges among states in rival coalitions is likely to be a significant strategy – and a source of crises. I would contend that this type of behavior is already seen in the way North Korea and Iran have been handled by the United States, and by China and Russia. That is, the major powers do not see these cases as instances of nuclear non-proliferation, but instead as "fronts" to disrupt American influence more generally.

A notable feature of these three multipolarity characteristics is how command and control imperatives permeate all of them. A state with nuclear weapons has to work out institutional arrangements for using this force, protecting it, and anticipating the possibility that the leadership itself will be a prime target of attack. The sovereignty of the state is itself a target. In addition, a country that is protected by another state's nuclear guarantee needs to judge whether this guarantee is believable, in peace and in war.

Most of the advanced technologies entering world arsenals now are information intensive. They exploit, leverage, distort, and conceal information. *Information is the "stuff" of command and control*. These technologies process vast amounts of information. And this vast scale and complexity makes the information processing structures opaque to political leaders. National leaders will be called on to assess the attribution of cyber strikes and conflicting intelligence and – at the same time – to see through deception efforts. The classic elements of surprise attack are all here: vigilance, warning, readiness, deception, assessment, and distribution of information to

those who can do something with it. But there are new elements as well. The speed of information, its variety, its fusion, and the fact that much of it is produced by algorithms and machine learning makes this a very complex problem.

Finally, command and control affects nuclear coalitions in critical ways. One is information sharing. Country A may have superior intelligence collection. It can share this with another state, Country B, as a way to rapidly bolster B's military preparations. Another new feature are *anonymous* attacks. A country can't really be certain who is behind the new domains of war like cyber. It may not be the enemy one thinks. It could be a "crazy state," one intent on upsetting stability between two other countries. A naïve belief has built up about attribution of cyber-attacks. We tend to believe what intelligence services claim is the origin of an attack. But the record of missed intelligence warnings, from Pearl Harbor to the Tet offensive, is pretty convincing evidence to the contrary. For cyber-attack against nuclear command and control and its supporting systems – electricity, transportation, etc., – attribution is a significant problem.

Two Themes: Globalization and Technology

Two themes animated the papers at this workshop: globalization and technology. By *globalization* I mean both geographic and network facets of command and control. Nine countries now possess nuclear weapons. Five more countries (Germany, the Netherlands, Belgium, Italy, and Turkey) have U.S. nuclear weapons positioned on their territory. Other nations are so critically involved with U.S. nuclear operations through warning, intelligence, and missile defense that for all practical purposes they are part of the U.S. NC3 system (Japan, the ROK, Australia, and Taiwan). At least eighteen countries are involved in nuclear or closely related NC3. Globally, no less than thirty-six states are directly or indirectly involved in the projection of nuclear threat against other states (namely, the U.S. and its NATO and Pacific allies, plus the other eight nuclear armed states, all dependent in one way or another on nuclear command and control systems).

Globalization in computer network terms has a slightly different connotation than in geography. In computer science, globalization refers to an information processing system that isn't local. Technologically speaking, the trend in sensors, communications, and information processing

over the last two decades has been to go from "local" to "global" networks in this sense. Examples include 5G networks, satellite communications, and the internet itself.

In terms of nuclear command and control this computer network definition of globalization has to be added to the geographic count of nuclear weapon states. Military geography is now made up of this network space just as much as it is of geography defined in terms of physical space.

For the United States especially, globalization defined in terms of who has nuclear weapons and in terms of the changing character of network space is important. Broadly speaking, most U.S. nuclear command and control in the Cold War focused on NATO and the strategic retaliation mission. Today it has to focus on Asia, from the western Pacific to NATO, to include the Middle East. The size of this geography is far larger than the NATO contingency of the Cold War. In addition, the nature of modern war is that space, cyber, undersea, and financial warfare via the banking system and clearing centers like SWIFT are now warfare domains with very rich targets spread over a global scale in both definitions of globalization.[4] Moreover, it must include space-based communication assets and ground nodes that are critical to the NC3 systems of most (but not all) nuclear armed states and their allies. It cannot be emphasized too strongly that command and control must be understood in this larger sense. There is a tendency to miss this point when nuclear weapons are analyzed only in terms of non-proliferation, where the narrow focus is on who has the bomb or not. This restricted view overlooks the important reality of what is now taking place in the world, namely, the appearance of completely new "big structures." It is akin to ignoring the Royal Navy, the German General Staff, and the Strategic Air Command in international security over the last two centuries.

What has developed is a world of nation states, which are the principal centers for decision making. There is a degree of cooperation among them, and many of the efforts to mitigate the problems of nuclear weapons have built, encouraged, and institutionalized these multinational efforts in, for example, arms control and other attempts at regulation.

But each state is pretty much in charge of what it does and how it does it. They're all different too, with varied goals, cultures, and histories. The papers at this workshop succinctly describe

[4] SWIFT is the Society for Worldwide Interbank Financial Telecommunications headquartered in Belgium.

these differences nicely. They underscore the point that the actors in this global system are highly differentiated.

Yet at the same time there are commonalities that arise from the nature of nuclear command and control. Such common problems also arose in the Cold War and are certain to appear again.

One example arises from behavior in complex organizations. Each nuclear weapon state today will solemnly declare that it wishes to emphasize above all else the "safety, security, and reliability" of its nuclear force. There will be top secret meetings about this with briefings to political leaders.

What these leaders will not know is that these briefings track with U.S. Cold War experience. The military in 1961 told Secretary of Defense Robert McNamara after he took office that "our nuclear forces are reliable, safe, and secure. Sir, there's really nothing to worry about." Today's leaders in nuclear states will likely hear this and they may be reassured.

But they will be wrong. Secretary McNamara responded to the briefing by sending a junior assistant, Adam Yarmolinsky, to visit the nuclear weapon sites. What he discovered was widespread violation of the two-man rule, grossly inadequate implementation of the locks on the warheads, unfettered movement of "live" tactical nuclear weapons close to the Warsaw Pact border, and, separately, an almost complete misunderstanding by civilians of the nuclear alerting system.[5] None of these things were captured in the top secret briefings given in Washington.

I would bet the same thing goes on today in the "new" and also in the modernized nuclear forces in the world.[6] The gap between what is briefed at headquarters and what actually takes place in the field can be enormous. Often it is. The fact that headquarters debates are top secret doesn't make them accurate. It may do the opposite, because security clearances can make it harder to discover what is actually taking place. Norbert Weiner was once asked about ways to undermine U.S. defense. He responded that if every classified piece of information was raised one level –

[5] This draws on my extensive discussions with Robert McNamara, Adam Yarmolinsky, and others. Yarmolinsky was a senior fellow at Hudson Institute where I worked.

[6] Indeed, in the United States in 2007 live nuclear cruise missiles were moved contrary to procedures, and even contrary to the knowledge that they were live by the people handling them. See Bracken, *Second Nuclear Age*, pp. 215-7.

"secret" information would be made "top secret" and "top secret" would be made "special access" – this would cause the collapse of the entire system.

If you want to understand how a complex organization behaves you cannot just look at its leaders. Their biases, fears, and rants are part of the problem, certainly. But we also have to look at *the information they rely upon to make their decisions*.[7] If headquarters thinks everything is fine – based on incorrect briefings – then leaders will act on what they think they know. The more complex the organization, the more the dependence on second-hand information provided to decision makers will shape their behavior. It isn't so much a question of psychology as it is of beliefs shaped by the information presented. In a complex organization with many parts, the decision maker becomes even more dependent than ever on the information reported to them. Virtually all of the experts at this workshop emphasized the greatly increased complexity of NC3. What I think needs to be understood is the next logical step that follows from this insight: that complexity makes the gap between headquarters and the real world larger.

This gap is what makes command and control so critical, because it raises fundamental questions about the feasibility of actually managing nuclear operations. It underscores the possibility that any strategy which overlooks this may be dangerously vulnerable to loss of control. We will know, roughly, how many nuclear weapons Russia has and how many North Korea has. But the dynamic behavior of their operations is something we will not know. And neither will their own leaders.

Many of the papers at this workshop focus on the risks of inadvertent escalation, accidents, and mistakes as the cause of a nuclear war (Acton, Leveson, Press). In one way or another these arise because command and control does not give a true picture of affairs – either of the enemy, or of one's own forces. This problem now is globalized due to the enlarged interactions from the number of nuclear states and the complexity of the information networks on which command and control is built.

Something else is at work as well. This is the learning curve. The Cold War saw multiple early crises, over Taiwan, Berlin, Cuba, etc. As Joseph Nye has underscored, these dangerous events

[7] This is the singular point of scholarly work in macro-organizational behavior theory. See, for example, Charles Perrow, *Complex Organizations: A Critical Essay* (McGraw Hill, 1993).

ultimately were turned into valuable learning experiences. The lessons learned from them were implemented by the two superpowers.[8]

This learning curve is now only at the earliest stage of formation. Suppose the United States and China, or India and Pakistan, got into intense nuclear crises – crises that are more serious than the Cuban missile crisis. By the third or fourth crisis, they undoubtedly will have discovered many problems and gaps. If the brain of a state's nuclear force is its command and control (Narang), then we're dealing with the undeveloped adolescent brain here. It is untested, unstressed. Adolescent brains do not process information the same way that adult brains do. They see different things. And they ignore warnings that would deter most adults.

This is why *nuclear operations* are so important. They are not some secondary detail that can be ignored in favor of a larger topic, like deterrence. In the United States, nuclear weapons are overwhelmingly seen in terms of *deterrence*. Everything else is looked at as the "details." This was also the case in the Cold War. I would agree that deterrence is the most important feature of nuclear weapons, then and now. But we're moving into a world where the "details" – operations, command and control, cyber, space – are going to matter a lot more. Nine states have nuclear weapons. Five more have them on their soil. How these states will interact in a nuclear prone conflict is poorly understood. The command and control of these forces is technically and organizationally dissimilar, with wide variation between countries.

The second prominent theme at the workshop was the importance of technology. The technologies have changed so drastically since the Cold War that entirely new issues arise that were not experienced in that era. "Technology" can cover many things. There are technologies of improved accuracy (Press) which create options for conventional counterforce attack of nuclear forces. There is technology to disrupt command and control (Lindsay). There are the technological opportunities from insider threats (Schouten). All of these reinforce the conclusion that new issues have arisen that need much more attention.

[8] Joseph S. Nye, "Nuclear Learning and US-Soviet Security Regimes," *International Organization* 41 (July 1987): 371-402.

A related theme here is that the information regime around nuclear weapons has fundamentally changed, and with it our understanding of deterrence, operations, and command and control. The technology of information processing has made command and control much more important – but also less understood than the regime of the Cold War. The deterrence models used in theorizing Cold War stability were what game theorists call games of perfect information. In a game of perfect information, each player is perfectly informed of the actual events that have already taken place, including the starting hand at the outset of the game, e.g., how many nuclear weapons each side has. In this framework, players make a sequence of choices, or moves, based on this knowledge.

In a multipolar nuclear world, attacks against information systems can provide a big strategic payoff. Blinding attack on warning satellites is a prime example. Stealth and hypersonic missiles reduce reaction time to zero. Cyber can deceive rivals about the state of affairs inside their organization. For all of these reasons the new information regime of nuclear war is radically different from that of the Cold War.

Signs of this changed information regime abound. The reported U.S. cyber-attack on Iran's uranium centrifuges was designed to fool the internal sensors running the operation. The cyber-attacks on North Korean missiles were also designed to conceal the insertion of faulty components to make the launches fail. Overall, much of the U.S. cyber program has been used to attack "nuclear" missile and enrichment facility targets. Most of this activity is below the surface, in that it isn't openly discussed or debated. It is concealed from public view, much like early nuclear strategy was hidden from public debate in the United States in the 1950s.

A Global Framework for Multipolarity and Command and Control

Global command and control in a multipolar nuclear world have to be understood in ways that go beyond the nation state, so to speak. It has to include the composite set of countries involved with nuclear arms. Today this larger global system involves at least eighteen different countries, with network extensions into new warfare domains like cyber, space, and finance, etc.

At the same time, we have to include overarching behaviors which arise as emergent properties of the national systems interacting with one another. National command systems are built for the purpose of operating these forces, such as ordering a launch and ensuring against accidental

firings. But, in addition, there is a "system dynamics" of interactions between the national commands. I will describe a framework for nuclear multipolarity that builds on these two concepts. The reason for taking this approach is that it describes the world we are in better than alternative descriptions. That is, we could focus on deterrence, or on nuclear non-proliferation construed as a set of treaties and associated norms. These approaches are useful in certain contexts. But they do not adequately describe the reality of what is now developing, or the dynamics of interaction that are the greatest worries of senior American military leaders, based on my discussions.

Levels of Analysis of National Command and Control

National command and control itself has to be considered in a more complicated way than simply declaring something called "the national command and control system." It needs to be decomposed into different layers of authority, technology, people, and processes.

For simplification, I will analyze a national system in terms of three separate levels. Complexity drives this need for different levels of analyses. Any complex arrangement of strategy, technology, people, and processes has to be decomposed into parts. Business schools, for example, make a basic distinction between *business* and *corporate* strategy. Business strategy deals with things like barriers to entry, customer bargaining power, and substitute products. Corporate strategy deals with strategy at a higher level. It includes government relations, political risk, and decisions about which businesses to be in and which to exit. GE and IBM, for example, are in many different businesses. To analyze these companies in terms of market share or deterrent to entry makes little sense outside of a specific business line, like health care or energy. Nonetheless, GE and IBM have corporate strategies in their approach to technology, regulation, innovation, and global investment.

The same is true for the military. We can describe a national NC3 as made up of three layers: the employment level, the operational, and the strategic. This may be thought of as a triangle with three levels of hierarchy. For nuclear command and control there is the "how to do it" level. This is the employment level, whether it is for deterrence or military operations. This level deals with the actual bombs, ways to prevent accidental launch, two-person rules, PALs (permissive action links, i.e., locks on weapons), targeting assignments, and collateral damage. It also deals with the ability to get the "go" message to the forces.

This employment level is treated in several workshop papers, either directly or indirectly. This is an important contribution of the workshop, to understand how other national command systems operate.

Next there are the operational and strategic levels of the command and control triangle. The operational level covers military plans, doctrine, and investment. In the United States it's what STRATCOM worries about. The strategic level of analysis considers things like political use of the forces, crisis management, "nuclear head games," and alerts for signaling. This level also covers NC3 in overall national policy, including nuclear stability, "appearances," and arms control. Most importantly, the lines separating conventional and nuclear plans and operations are decided at the strategic level. That is, the role for nuclear forces and its relationship to conventional forces has to be carefully thought through at this level.

Finally, there's the "system dynamics" of interactions between the national systems. This is a horizontal relationship that describes the coupling, intelligence, alerting, and probing of rival systems. It also includes linkage to allied nations, e.g., if they have U.S. nuclear weapons on their soil. NATO's nuclear deterrent is the example. But in addition to this, there are information processing centers for intelligence collection and missile defense which are so directly related to the nuclear mission that they must be included. Japan and Australia are leading examples of this involvement, although one could add the ROK and ROC with significant but lesser contributions to U.S. NC3.

This overall model recognizes that what is now developing is a global network of interacting nuclear national command systems. This system of national systems has received little attention. One reason is its complexity. Another reason is that in the Cold War, until the 1980s at least, attention was focused on nuclear weapons rather than the information regime they were embedded in. The "classic" nuclear strategy literature developed in the 1950s and 1960s before the significance of this information regime was appreciated.

An interesting feature of the global nuclear command and control system that is now developing is the recognition that the information regime around nuclear weapons is increasingly critical. It is critical for deterrence and for other aspects of nuclear governance. Protecting the force from

insider threats and ensuring against cascading failures that might stem from communications or electric power failures caused by an enemy are examples.

Still, there is a myopic tendency to look at national systems in isolation from the larger global system they are embedded in. The focus is on investments to bolster national command and control against direct threats. There is still as yet little attention given to how individual national systems together produce a new, emergent global nuclear command and control system of sensors, information, flows, and feedbacks. These elements interlink weapons, missile defense, satellites, and cyber war.

This framework, made up of many national systems, and system-wide linkages connecting them, is a model that can be used to understand today's multipolar nuclear order. I do not see how any alternative model, for example – one based on deterrence, public attitudes against nuclear weapons, or on diplomacy and treaties – can begin to grapple with the complexity of the global system we are now building. These other things are important – but they are frameworks which leave out pathways to war and to national security disasters.

Institutional Arrangements of National Systems

In the United States command and control at the operational and strategic levels arose at the dawn of the nuclear age in the form of what can be called the problem of "institutional arrangements." They are worth mentioning here because institutional arrangements are unavoidable issues in any command and control structure. The term describes the problem that once nuclear weapons are deployed the authority to fire them immediately arises. This was an institutional issue because it involved organizations and laws governing civilian control of the military.

In the United States, according to the Constitution, only the Congress can declare war. Firing nuclear weapons was clearly seen as an act of war. But this scenario could involve time urgent events that the Congress was not prepared to deal with. The institution that had declared war on Japan in 1941 was adjudged not to be reliable for this purpose in the nuclear age. This wasn't any usurpation of power by the executive branch. Rather it was a recognition of the brute fact that there was no way to stop a Soviet advance into Western Europe, the most stressing threat at the time.

More, a president could be killed by an enemy attack, along with all of the duly authorized successors, like the vice president, the speaker of the House of Representatives, president pro tempore of the Senate, and so on. The attack might be nuclear or it might be something else, like an assassination. This created a lacuna – a "gap" in command and control. An attack on the U.S. leadership offered a way to paralyze a response, or at least to delay it for a significant time. This potentiality might actually invite such an attack in the first place. Even if the president or vice president did survive it was uncertain that they could in the confusion get word to the forces to fire. This made the communications to connect political and military leaders absolutely critical.

My purpose here is not to detail the particular ways that the United States solved this problem. Rather, it's to make a more general point. *Institutional arrangements for going to war were radically transformed by the new technology of atomic weapons*. And these changes were deeply institutional, for they required new organizations and laws that radically differed from centuries of tradition. The organizational change led to the re-creation of the Air Force. The imperatives of a nuclear age drove the creation of a new "separate" air force, the Strategic Air Command, built for rapid reaction. Other changes included the creation of new organizations for warning, surveillance, and intelligence focusing on enemy nuclear forces.

The "law" part of the changes were special legal arrangements so that the nuclear force could be used even if the president was not available. This is where pre-delegation of nuclear launch authority comes in. Pre-delegation of this authority ensured that retaliation would follow an enemy strike on the United States. It would also define who was in charge and in control of the nuclear forces. This unity of command was important because no one knew how a nuclear war would end. Whatever form termination might take, it was inadvisable to allow for independent, separate islands of launch authority to be scattered over the military as an accidental consequence of which surviving units had communications. A chaotic situation like this would preclude centralized negotiations to end the war.

These organizational and legal changes were structural. They were not simple inter-agency decisions or private understandings among individuals. Nor were they the decisions of a single person like the president. Structural change meant an enduring change in the relationship of the military and civilian leadership.

The salience of institutional arrangements for today should be clear even as the details of the changes vary by country. Each of the nine nuclear weapon states has to face new institutional arrangements of civilian and military leadership. Many of these are described in the country-specific papers at this workshop both historically and in the present tense. It may be the case that some countries decide to do nothing on this front. They may even decline to address institutional concerns at all. Yet this too is a decision, one that could have far reaching consequences on command vulnerability and on nuclear war termination.

Moreover, today the challenge isn't driven only by the high speeds of the weapons, bombers, and missiles, as in the Cold War. At least not only that. Massive attack cyber options aimed at blinding and destroying electric power, communications, and transportation – the backbone of command and control – radically change the nature of the problem once again. Today, it is far different and far more complex than it was at the dawn of the Cold War.

We already see a creeping expansion of authorities over strategic cyber-attack, in the United States and elsewhere. Unfortunately, cyberwar is too often looked at in isolation from nuclear operations. It begs disbelief that the military in the operational levels of national command haven't noticed the effect that cyber-attacks could have on nuclear forces. This is an issue that, as yet, has received little attention. It lies below the surface of public and most think tank attention. This workshop has some excellent papers that touch on the problems raised.

It cannot be emphasized too strongly that each nuclear weapon state faces the challenge of "institutional arrangements." There are new ways to destroy a rival's nuclear forces, and these involve attack of command and control and include its supporting infrastructure of electricity, communications, and transportation.

I would expect different institutional arrangements for nuclear command and control to develop in China, Russia, North Korea, and Israel, etc. Again, our purpose is not to come up with particulars and specifics about these, many of which are covered in workshop papers. For our purposes it isn't hard to see how this issue of institutional arrangements could lead to dangerous scenarios. Many of the nuclear states are not democracies, and there is no unquestioned supremacy of civilian control over the military as there is in a democracy. The threat of internal subversion and insider attacks is especially important, and it was not really a major issue in the

Cold War. The capture of a nuclear weapon might come to symbolize successful control of the government by a dissident group.

Even a democracy can get into bizarre, unanticipated situations when it comes to institutional arrangements. This occurred in 1961. A coup by French generals in Algeria against the president of France, Charles de Gaulle, led to his ordering the hasty early detonation of a French nuclear weapon at a test site in the Sahara Desert (Pelopidas, p. 17). This destruction of the bomb prevented it from falling into the hands of the plotting generals. In addition, it demonstrated that the rebel officers did not control all of Algeria as they had claimed.[9] We can debate whether this particular case was dangerous or not. What we can say, however, is that in 1961 President de Gaulle thought it prudent to take this step. It illustrates the unanticipated pathways a crisis could take.

What this discussion suggests is the need to *"stress test" the institutional arrangements of nuclear weapon states to determine if they can withstand the pressures that might arise in various scenarios*, from both internal and external shocks. Banks are routinely stress tested today, especially following the unanticipated and unimaginable events of the 2008 financial crisis. It seems obvious that nuclear command systems should be as well. One approach to this modeling of command systems is suggested by Alex Wellerstein (Wellerstein). He develops a schema of authority flows for the launch of nuclear weapons, from the political leadership and through senior military channels down to the weapon operators. This is a useful way to comparatively map out the differences in national command and control.

A next logical step in the Wellerstein framework would be to include the interaction of command systems. Launch authority seems likely to depend on tensions and alert conditions; that is, launch authority flows are geared to enemy preparations. This agent-based modeling approach would be possible to stimulate. Indeed, this was the approach taken by Paul Davis at the RAND Corporation in the 1980s.[10]

[9] "France Explodes Nuclear Bomb at Sahara Test Site in Algeria," *New York Times*, April 25, 1961, p. 1.
[10] See Paul K. Davis, "Applying Artificial Intelligence Techniques to Strategic-Level Gaming and Simulation," Note N-2752, (Santa Monica, CA: Rand Corporation, 1988).

Another important takeaway here is that *if we confine our attention only to the "likely" cases in making nuclear assessments we are doing bad policy analysis*. We don't know what the likelihoods are. Experience shows that we are poor at predicting them. Our standard shouldn't be the likely cases, but also the most serious and damaging ones. The need to explore many different cases is also a key point in the work of Paul Davis and was emphasized in his paper for this workshop (Davis).

Some operational and strategic level issues are transitory rather than structural. These include decisions made in a time compressed environment which could be turning points in the way a situation develops. These often showed up in Cold War crises and in role playing crisis management games. In fact, they were one of the reasons for playing these games in the first place. The goal of the games wasn't *prediction* of what a country might do. It was *discovery* of the issues that other methodologies might have overlooked.

An interesting example of this was launch on warning. This policy was proposed by many experts, that is, setting the U.S. nuclear force to a launch on warning posture would be enormously deterring. It was included in highly classified options available to leaders as a way to rapidly bolster deterrence. Let me just say that in many games and politico-military crises that I played in either at Hudson Institute or in various projects for the Department of Defense, that launch on warning was one of the first options people got rid of. It was far too dangerous, and it veritably invited unintentional launch of nuclear missiles or war by accident. In the 1983 Proud Prophet war game of a U.S.–Soviet conflict in Europe launch on warning was immediately discarded as an option. The feeling in the game, which included play by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, was that no one would be crazy enough to institute a launch on warning.[11]

I think this reluctance is interesting and relevant for today because it bears on a new topic: autonomous weapons. The conclusion it leads to is that anyone crazy enough to turn "on" autonomous nuclear weapons – robot bombs – deserves what they're likely to get. This logic applies to long range conventional weapons and cyber as well. To my knowledge the

[11] Bracken, *Second Nuclear Age*, pp. 83-88.

autonomous weapons that the United States does have, like Aegis missile defense, have never been set to fully automatic firing mode in a combat environment.

But a real problem remains. Because what cannot be assumed is that other countries will follow this principle, that is to never allow autonomous weapons. Even in the United States there is a dangerous drift toward autonomous cyber response that could get out of hand or that could add to the intensity of a nuclear crisis. The problem with cyber especially is that it is so hidden and anonymous – and that it is available to so many countries. If national command and control systems move in this direction it's likely to be highly risky for them and others.

"System Dynamics" of the National Systems

System dynamics describe the interactions between the national command and control hierarchies of different countries. The issues of interest here are things like how changes in the state of one system affect changes in another. The "stiffness" of the nuclear trigger is a good example of a system dynamic issue. A country may decide to make its nuclear trigger very stiff or it can decide to put its nuclear forces on a hair trigger. This is a national decision that can be described in terms of the three levels of command and control. If another country detects a change in the stiffness of the trigger of its rival, then it may feel compelled to heighten its own readiness. Thus, the system is dynamic and interactive. Again, this is a phenomenon that should be susceptible to agent-based modeling.

System dynamics doesn't only affect the stiffness of the trigger. Other linkages include conventional and nuclear alerts, the degree of vigilance, and intelligence probes of rival systems. Arms race strategies and arms control are covered by system dynamics as well.

One of the key points to emphasize is that a big new structure of international security is taking shape. But it is a system made up of national systems. The national systems may be rationally designed, or not. But this global system is not rationally designed by any one actor at the macro level. It is better thought of as a "game" in the game theory sense of opposing actors linked by interdependent strategies for things like alert levels, stiffness of the launch trigger, and the degree of distributed launch delegation authority.

A remarkable development now taking place arises directly from the two themes emphasized at the workshop: globalization and technology. Because what is taking form is an increasingly automatic structure, one with a logic built into the software and organizational procedures which run it. This logic, quite literally, controls the changes of state of the national systems. The drivers of this are not nuclear weapons per se, but rather information, which in turn is driven by cyber penetrations, drone and satellite intelligence, and big data and analytic decision making. I would add that the ease of constructing the national automatic structures is greatly advanced by the innovation of cloud computing. Cloud computing allows all kinds of seamless integration of big data bases that otherwise would be very difficult to integrate in real time. This is exactly how cloud computing is used in commercial companies. The same now is happening in defense.

So far, we have not seen this global command system excited to a high level of vigilance and alert. There's a historical parallel for this possible future. Although there were repeated crises in the Cold War, only in the Cuban missile crisis did the U.S. system kick into high gear. This was the only time that Strategic Air Command (SAC) went to full airborne alert for a fraction of its bomber force. Also, it's the only time SAC bombers were dispersed to alternate civilian airfields.

So, there are two features of today's systems dynamics worth emphasizing. One is its increasingly automatic structure – driven by software and information technology – which responds to changes in enemy force state. The other is the intermingling of many conventional command and control systems with nuclear command and control. Many papers at the workshop emphasize this point as well.

The two places where these features show up most starkly are in Europe and Asia. This phenomenon by itself is worth noting. Because the key problem from a stability point of view is not the one that receives the vast amount of attention. It isn't the risk of a Russian surprise attack on U.S. Minuteman missiles, bombers, and submarines in port. Nor is it a U.S. surprise attack on Russian or Chinese nuclear forces. These cases get the overwhelming focus of official U.S. arms control policy yet they are among the least likely scenarios of instability. A START follow on treaty (Strategic Arms Reduction Treaty), which I do not oppose, is largely irrelevant to the serious nuclear risks which are growing in the world today. Rather, it's the regional structures in Europe and Asia that involve the United States where nuclear stability experts and the U.S.

government should focus their attention. "System dynamics" applied to these two regions suggest important behaviors and pathways to crises.

Nuclear Weapons and European Security

In Europe, the return of tensions with Russia and the seeming demise of the Intermediate-Range Nuclear Forces (INF) agreement have caused a reexamination of NATO's nuclear deterrent. The impetus for removing NATO's short-range nuclear weapons as was done after the Cold War has virtually disappeared. Indeed, the opposite tendency has now developed.

Widely overlooked is the fact that the F-35 is now becoming the front-line NATO aircraft. The F-35 is fitted to carry nuclear gravity bombs.[12] There will soon be two nuclear weapon carrying stealth aircraft, the B-2 and the F-35. The newly refurbished B-61 bomb was designed for this role.

In addition, there are the nuclear weapons shared among the United States with Germany, Italy, Belgium, the Netherlands, and possibly still with Turkey. On the Russian side there are many reports of nuclear missiles in Belarus and Kaliningrad, as well as in Russia itself.

The command and control problems arising from these developments are very interesting to examine. Yet they tend to be overlooked as attention focuses on modernizing the nuclear triad and an extension of the new START treaty, both of which have little to do with what is taking place in Europe. In a serious crisis NATO would need to "project" nuclear deterrence into Poland and the Baltic states, e.g., as a sign of support for these nations according to the NATO Treaty. Sweden, Finland, and Norway might be a part of this surge as well. The communications, transportation, and weapon protection aspects of such a movement are considerable, and would likely be prime targets for insider, cyber, and drone disruption and other kinds of interference by Moscow. How the various NATO members would respond is unclear.

The difference with the Cold War is stark. We are not returning to the old days of NATO versus the Warsaw Pact. Then, the problem was using NATO's nuclear weapons to respond to Russian aggression. *Now it is a multinational command system trying to project NATO nuclear deterrence into a region that is 500 miles east.* As this takes place, the "system dynamic"

[12] This is the F-35A version.

interactions with the Russian command system and its cyber, political warfare, space, and other domains would be unfolding.

There's a major political gap here as well, one that shows the way that nuclear weapons and foreign affairs are developing in this new world. It is entirely possible that a key country may decide not to participate in the NATO nuclear deterrent. Germany stands out here, perhaps prefigured by its recent announcement that it will not buy the F-35. At the same time the German air force is now phasing out its old Tornado aircraft, which were capable of carrying nuclear weapons under the NATO sharing arrangement, i.e., U.S. bombs on German aircraft. This move is widely seen as a political decision by Germany to exit participation in the NATO nuclear deterrence plan. If this departure occurs then a large political and military "gap" is created in NATO deterrence. Specifically, the rest of NATO will have no way to reach Poland or the Baltic states. Similar dynamics are evident in the very different case of Turkey, as explained in one of the papers at the workshop.

My purpose isn't to go through a full policy analysis of NATO and deterrence. Rather, it is to underscore two important points. First, that command and control in Europe interlinks many national systems, and that Russian cyber-attack, precision strikes, and insider attacks create preconditions for true disaster. Second, that it is not hard to write a scenario of these complex interconnected systems leading to unexpected events and misunderstandings. Like 1914 and the outbreak of World War I, no national leader is likely to understand this system before it is kicked into action.

A Pentapolar Security System in Asia

Turning to Asia, the profound geopolitical changes there take place along with a radical technology transformation that involves nuclear weapons. For the major powers of Asia – China, Russia, the United States, Japan, and India – a *pentapolar* security system is developing. I will exclude North Korea and Pakistan from this, not because they don't pose enormous dangers, which they do. Rather, dealing with them using the instruments of the Non-Proliferation Treaty does not look to be feasible, at least to me. The way to manage them, increasingly, is through the actions of the major powers.

A nuclear multipolar order has come to Asia – one that is increasingly accepted – unlike the European case the nuclear character of which is rarely acknowledged.

Each major power in Asia has a national command and control system for its nuclear forces, with the obvious exception of Japan. But Japan must be included in Asia's nuclear order. The reason is because of its tight integration with American defense. In particular the key role Japan plays in missile defense makes it necessary to include Tokyo. The role of missile defense is only going to grow in Asia. It may be the case, as many have argued, that U.S. missile defense in Japan is designed against North Korea, and not against China or Russia. Yet Beijing and Moscow are unlikely to accept this. They have every incentive to disrupt the space-based sensors, communications, and ships that go into missile defense. Also, most U.S. systems for conventional war in the Pacific are dual use, that is, they are used for nuclear and conventional operations. Japan is a key element in this structure as well.

Think of this Asian system as a network with five major nodes: China, Russia, India, Japan, and the United States. Asia's nuclear interactions "connect" the nodes. Among the many dimensions of this linkage are U.S.–Japan missile defense, India's nuclear modernization with respect to China, anti-submarine warfare (ASW), and the way China's nuclear modernization impacts U.S.–Russian nuclear stability.

U.S. missile defenses immediately impact China's strategic posture. This is because China's buildup in missiles is the backbone of its whole modernization program. By itself, it's a very impressive force. It is now much larger than the Soviet missile threat to Europe in the Cold War. Unlike that force, however, which was unguided and slow reacting, China's is equipped with precision-strike technology and an ability to track mobile targets like ships. This force is itself land mobile. The old Soviet force underwrote a "hostage Europe" strategy. In a crisis, it was something that was impossible to overlook, just as China's force is today. China, in effect, has a "hostage Japan" strategy that simply cannot be overlooked in any use of U.S. maritime power.

Interactions in another part of this Asian structure, between India and China, show another dimension of the pentapolar global structure in Asia. In ten years, India's MIRVed missiles could destroy ten to twenty-five of the largest Chinese cities. With an Indian hydrogen bomb this threat reaches a high degree of assurance. This surely adds to deterrence of China.

Whatever crisis develops in the western Pacific, Beijing cannot overlook the emerging nuclear threat from the South.

Another interaction in this pentapolar structure is the U.S.–India link. One issue that arises in any coalition is how a member can act to keep another in the group. So, we might ask how this could work with nuclear forces. Let's consider a historical example, one that interestingly occurred in the "tripolar world" of the 1970s. When Richard Nixon went to China in 1972, Henry Kissinger carried with him the nuclear order of battle for Soviet forces in the Far East.[13] Kissinger gave this information to the Chinese, to include the type of weapons, their yield, range – and exact locations. Photographs and maps were provided to the Chinese military. In short, Nixon gave Beijing targeting information about Soviet nuclear forces. There was no way Beijing could have assembled this data absent of the U.S. information.

This information transfer stabilized the tripolar nuclear world of the 1970s, which then meant the United States, the Soviet Union, and China. We may disagree about the wisdom of this move. Some would argue against it. But this does not affect the point I wish to make. *Information transfer will be much more important in the future – and it is very much a command and control issue*. This is because targeting information about mobile missiles has become so important. One of the uses of such information is to alter the nuclear balance by targeting these missiles. Information transfer goes directly to the topic of interest here, the system dynamics of command interactions. The United States found a way to rapidly improve China's military capacity against the Soviet Union, at the highest escalation levels of nuclear war.

In the 1970s, nearly all nuclear weapons on land were in in fixed sites. Some missiles were mobile, but these were mostly dug in and concealed with camouflage. They didn't move. Reliance on mobile missiles for carrying nuclear weapons is now widely practiced. These are much harder to locate. But they can be tracked with the new technologies, with drones, cyber, phone hacks, insider tips, AI, machine learning, etc. Countries which are good at tracking mobile targets will have valuable information to transfer to others aligned with them.

[13] Bracken, *Second Nuclear Age*, pp. 197-201.

Cyber technologies in particular are making the hunt for mobile missiles faster, cheaper, and better.[14] As a result, the hunt for mobile missiles will be the next great phase of the arms race. This also means that counterforce attacks can take out nuclear forces with conventional weapons, as several papers at the workshop argued. From a crisis stability point of view, this is extremely unfortunate. How the Asian pentapolar system handles this is likely to be one of the great challenges of the next ten years. Major powers need to think this through in a very different technological landscape than historical arms races.

Two other links in the Asian pentapolar system are ASAT and ASW. India has successfully tested an ASAT weapon in 2019, becoming only the fourth country to do so, after the United States, Russia, and China. In the ASW area, it is widely reported that in the event of war the United States plans to limit China's submarines to enter the South China Sea and the Pacific. The necessity of attacking communications and sensors, quite likely using ASAT weapons, to disrupt the ASW mission suggests that command and control will be an immediate target. India is directly impacted by this since it needs to monitor the status of Chinese and Pakistani forces and prevent China and Pakistan from knowing when it increases its readiness and alert levels. Specifically, all of these countries will be trying to locate land-based mobile missiles and submarines, which now carry nuclear weapons of these nations.

Finally, one other interaction in the pentapolar Asian system is between the United States and Russia. Henry Kissinger picked up on this idea, observing that at some point the nuclear forces of China and India will have to be considered in the calculations of nuclear stability between the United States and Russia.[15] Exactly when this tipping point occurs depends on the details, and this sensitivity is the key point. The details are starting to matter. So are the domestic politics of the major powers. By my estimate this threshold will start to seriously matter within the next ten years. The nuclear balance that has been thought of for seven decades as entirely a U.S.–Russia matter is going to radically change with Asia's military build-up.

This discussion of Europe and Asia can be used to make some key points about nuclear multipolarity and command and control. *The sources of instability do not arise only from*

[14] See Paul Bracken, "The Cyber Threat to Nuclear Stability," *Orbis*, Spring 2016.
[15] Henry Kissinger, *World Order* (New York: Penguin Press, 2014), p. 339.

bipolar counterforce improvement, i.e., from U.S. or Russian missile accuracy. They arise also from imbalances of power in nuclear coalitions.

Conclusions

In the 1980s a new focus on command and control changed the way we think about nuclear forces. Before then the basic model of deterrence was a stability paradigm based on the number of nuclear weapons each side possessed, and on three parameters (accuracy, yield, target hardness). After command and control frameworks were considered, this stability paradigm changed. Strong interactions were likely to overwhelm the best laid plans for "controlled" uses of nuclear weapons. The conclusion reached was that attention needed to focus less on the number of weapons and more on the command systems that managed nuclear operations.

We now live in a nuclear context far more complex than anything in the Cold War. Whole new kinds of emergent system behavior are developing, driven by the extension of nuclear arms to more countries and to new domains of conflict. This is readily apparent in Asia. It is less recognized in Europe, but is nonetheless taking place there as well.

We should expect that national leaders will not understand their own forces. I don't think we need to dwell on this by focusing on individual personalities. Today's leaders lack even the "dated" experience of Cold War crises. In their own way these crises "disciplined" the United States and the Soviet Union into more prudent, risk avoiding behavior. This knowledge has largely been forgotten outside of the experts of a kind at this workshop. New behaviors unseen in the Cold War are emerging, such as the behavior of nuclear coalitions and the cyber-nuclear intersection operations. This workshop began pulling together what some of these behaviors look like, as best they can be discerned. They are a first look – and a very sober one – of the challenges of nuclear multipolarity. They will start a necessary conversation about the road ahead.

III. ENDNOTES

IV. TECHNOLOGY FOR GLOBAL SECURITY INVITES YOUR RESPONSE

Technology for Global Security invites your responses to this report. Please send responses to: info@tech4gs.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent.