FOREIGN POLICY RESEARCH INSTITUTE

THE HUNT FOR MOBILE MISSILES

Nuclear Weapons, AI, and the New Arms Race

Paul Bracken

FOREIGN POLICY RESEARCH INSTITUTE

Published by the Foreign Policy Research Institute
1528 Walnut Street, Suite 610, Philadelphia, PA 19102
www.fpri.org

Library of Congress Cataloging-in-Publication Data
Names: Bracken, Paul
Title: The Hunt for Mobile Missiles: Nuclear Weapons, AI, and the New Arms Race by Paul Bracken
Identifiers: (electronic) ISBN: 978-0-910191-14-2 | (print) ISBN: 978-0-910191-15-9
Subjects: Technology, Political Science

Printed by Creative Print Group
Cover Design: Natalia Kopytnik
Cover Image: An army truck MZKT 79221 under missile Topol-M (RT-2PM2), Wikimedia Commons

FOREIGN POLICY RESEARCH INSTITUTE

THE HUNT FOR MOBILE MISSILES

Nuclear Weapons, AI, and the New Arms Race

Paul Bracken

Prepared for The Carnegie Corporation of New York

This page was left blank for printing purposes

Sometimes they [the Paris police] stand too near the problem. Often, if a person looks at something very closely, he can see a few things more clearly, but the shape of the whole thing escapes him.

Edgar Allan Poe, The Murders in the Rue Morgue

This page was left blank for printing purposes

Table of Contents

This page was left blank for printing purposes

EXECUTIVE SUMMARY

This report examines the increasing ability of major powers to destroy moving targets, in particular, land-based mobile missiles. Yet, at the same time, it analyzes something much broader and more fundamental. Technology has changed the use of force in peace and war. These changes stem from the growing importance of advanced technologies like AI, cyber, drones, cloud computing, data analytics, and hypersonic missiles.[1] These are increasingly becoming foundational technologies for new mission areas and strategies. One of these in particular is the focus of this report: locating and destroying mobile targets. The hunt for mobile missiles, seen in this broader way, is an exemplar of advanced technologies used in national security.

1 This report uses a number of technology and management concepts that are unfamiliar in most political science and history descriptions. A glossary defining these terms is included in the appendix.

An exemplar is an ideal model – an outstanding example of something which shows its feasibility. Other exemplars of advanced technology include the Manhattan Project, Sputnik, and the AI win over champions in the game of Go.[2] An exemplar is important because it shows that something can be done, even if it is only on a small scale or in a limited way. Exemplars are significant because they change how people decide what is feasible. Further, they point to its potential for the future, and its wider application.

There undoubtedly are other exemplars for advanced technologies in defense. Together, these will change how the use of force in peace and war is conceived. This is the reason for the subtitle of the report: Nuclear Weapons, AI, and the New Arms Race. This subtitle is meant to capture certain key ideas related to the focus of the report: the hunt for mobile missiles is spilling over into the nuclear arena. It provides a growing ability for the United States and others to attack the nuclear deterrent forces of other states -- even though they are mobile.

The principal findings of this report cover a wide range of national security topics. Advanced technologies will alter extant military power arrangements, and for this reason will have important political impact. Changes in international order, in turn, will shape national security. At the same time, the choice of national policies on how much to invest in technology innovation, where it's focused,

2 The idea of an exemplar as used here comes from Thomas Kuhn in *The Structure of Scientific Revolutions*, (University of Chicago Press, 2nd ed., 1970). Exemplars are an intellectually stripped-down version of Kuhn's more sweeping idea of a paradigm change, an all-encompassing transformation in how a field is conceived. Exemplars are more limited demonstrations of feasibility and potential. AI computer programs defeating human chess and *Go* players is a good example of an exemplar. We make no use in this report of the broader idea of a paradigm change.

and restraint on these activities will have an impact on a new arms race. This is the reason reference is made to a "new arms race" in the subtitle. It may not look like historical arms races – denoted by increases in the number of tanks, aircraft, or atomic warheads – because much of this new arms race will be hidden in algorithms, data centers, and computers. But it will still be an arms race.

Advanced technologies are reshaping national security and international order. Changes in one area changes the other. The causality doesn't go in only one direction, (e.g., technology driving change in the international system). Rather, both national security and international order coevolve in a dynamic way.[3] Advanced technology is an important element defining this coevolution. Technological innovation is shaping international order, just as it has disrupted the industrial order.

The key findings of our research are organized into three classes. First, there is a strategic and system level, which covers findings dealing with technology and the changing international order. This level includes major power competition and its nuclear context. This point – a nuclear context – arises because nine countries now have nuclear weapons, including most of the major powers.

Second, the report offers methodological suggestions for raising the level of debate about advanced technologies in national security. This was not anticipated at the outset of the project. But the significance

3 This idea of coevolution of two mutually evolving systems applies to many technological systems, for example, mobile missiles and the hunt to locate them. The two systems are mutually interacting. Coevolution describes these strategic interactions. This important insight is now increasingly appreciated in political science, see Nazli Choucri and David D. Clark, *International Relations in the Cyber Age, The Co-Evolution Dilemma*, (MIT Press, 2018).

of AI, cyber, drones, hypersonic missiles, and data analytics are so large that new, non-standard frameworks are needed. These new methods were developed from research about how businesses dealt with their technological challenges -- that is, how businesses analyzed investments in AI, cloud computing, and data analytics and how these technologies were aligned with corporate strategy. These new frameworks – value chains, touchpoints, information chains -- are taught in business schools, but are virtually unknown in academic strategic studies or in professional military education.

A third class of findings treats operational issues. These relate to execution, organization, and tactics. They are distinctive because they are "bottom up," so to speak, more than top down. They reflect the fact that countries use technology in different ways. A one size fits all approach won't work for understanding military uses of the technology. They also reflect the fact that there are so many new technologies at the present time that top down direction is extremely difficult. No one is able to manage all of the innovations that are possible with the new technologies.

Strategic and System Level Findings

Absent a broader, more sober view of the hunt for mobile missiles, one that goes beyond narrow measures of performance, the world is going to see more dangerous nuclear crises, and arm races that go beyond what is necessary for prudent national security. This arises because mobile missiles have unique crisis management implications, most of which have not been studied before. Arms races result because building up nuclear forces is one way to offset improvements in reconnaissance tracking of these systems.

The United States, China, and Russia are sharply increasing their

investment in the hunt for mobile missiles. The United States is doing this to find missiles in North Korea, Iran and other places. China's main thrust is to track maritime targets like ships and aircraft. Russia's emphasis is on disruption of NATO's ability to project military power into Poland, the Baltics, and Ukraine. The plans for these programs are highly secret in all countries.

Although the importance of technology is sometimes exaggerated and too much attention is placed on it, the reality is often the opposite: the significance of technology is systematically understated. The speed and scale of technological change in the security environment has been underestimated in the United States for over a decade. Examples include the North Korean nuclear missile program, its hydrogen bomb, the shrinkage of warheads to fit on mobile missiles; and China's manifold military technology advances. All of these developed faster than most groups in the United States anticipated. Until 2015, the enormous vulnerability of 5G technologies, electric power systems, satellites, and telecommunications had been discounted or ignored by most elements of the U.S. security establishment, including intelligence agencies, think tanks, and universities.

Major powers (U.S., China, Russia) are using the hunt for mobile missiles as an "exemplar" for integrating AI, cyber, data analytics, and other technologies into their kill chains. The hunt for mobile missiles serves as an innovation platform. The "hunt" mission, therefore, has a military purpose -- i.e., to destroy enemy missiles. It also has broader strategic purposes. It is a platform to organize additional advanced digital technologies around a clear mission.

There are two drivers behind the hunt for mobile missiles. One is

operational: to locate and destroy mobile missiles that could cause harm. The other is not to fall behind a rival in bringing digital technologies like AI into defense. This second dynamic is driving the arms race that is now taking shape among major powers. No great power wishes to fall behind in using advanced technologies for defense.

The mobile missiles of highest urgency are, clearly, those with nuclear warheads. Since the 1990s, mobile nuclear missiles have become the preferred nuclear weapon for nearly all countries, the United States excepted. The reason for this shift to mobile missiles is that fixed-site targets are vulnerable to precision conventional or nuclear attack, as has been demonstrated repeatedly in recent wars.

"High touch" reconnaissance strategies will become a focus of technology strategy. High touch is defined as frequent, stealthy, tailored contact between reconnaissance systems and a target. It is a recurrent, surreptitious monitoring -- the target is "touched" repeatedly by many types of sensors (drone video, cyber hacks, satellites, insider reports, etc.) that are continuous and unobtrusive. This high touch world of today contrasts with the Cold War, which had "low touch reconnaissance." Satellite passes occurred intermittently, aerial reconnaissance was cumbersome, and insider agent reports were infrequent.

The combination of multiple "touchpoints" of different sensors – drone video, cell phone tracking, security cameras, hacked computers, etc. – will lead to greatly improved tracking of mobile targets. AI will be necessary to "aim" this complex reconnaissance system, extract target information from it, and link it to hypersonic missiles and other weapons in an overall value chain. Any one reconnaissance

technology by itself (e.g., satellites or drones) will not deliver the required breakthrough.

An AI arms race among the major powers could upset the global nuclear balance for this reason. One way this could happen is from improvements in tracking the mobile missiles of another major power (e.g., the United States on China). Combined with massive cyber attack, follow-on nuclear and conventional strikes, a plausible first-strike threat is returning in a way not seen since the 1980s. This theoretical possibility could drive an AI-nuclear arms race. In the 1980s, the United States combined several "new" technologies (MIRVs, improved missile accuracy, SDI, ASW) to create a theoretical first-strike capability that created paranoia, and dangerous nuclear operating practices in Moscow.

An AI-nuclear arms race does not have to lead to actual war to impact international order in a significant way. Analogy with the 1980s shows this. It could produce heightened insecurity, loosening of the nuclear trigger, paranoia, hypervigilance, and nuclear groupthink. Another analogy with the 1980s stems from the synergy of several technologies, not just one.

A doubling of China's strategic nuclear forces over the next decade is forecast in a recent DIA estimate (May 2019).[4] This may reflect Beijing's understanding of just how effective new AI-directed search technologies are, with a recognition that Beijing's nuclear deterrent

4 Remarks of Lt. Gen. Robert P. Ashley, Jr., Director Defense Intelligence Agency, "Russian and Chinese Nuclear Modernization Trends," Remarks at the Hudson Institute, 29 May, 2019.

will become vulnerable as a result. China has been a leader in all of the advanced technologies discussed in this report. The issues in this project, then, are already having an impact on how the global nuclear balance develops. For another example, STRATCOM has been given overall authority to remodel the U.S. nuclear command, control, and communications system. Discussions with STRATCOM, CYBERCOM, and British nuclear planners indicate a very high level of concern about the vulnerabilities created by reconnaissance tracking and cyber attacks.

Some secondary nuclear powers (Pakistan, North Korea) are slow to appreciate the threat to their "small" nuclear forces posed by improved tracking of mobile missiles. They have also failed to understand how their actions in a crisis – like full dispersal of their mobile missiles – could tip a confrontation over the edge into nuclear war. At some point however, they will understand the danger they face from technologically advanced reconnaissance of the United States and China, and perhaps of South Korea.

None of the major or secondary powers, have seriously analyzed the long-term consequences of the hunt for mobile missiles beyond the operational level. The longer-term impact on nuclear stability, arms control, escalation, early warning, and accidental war have gone largely unexamined. The present focus is on "not falling behind." A similar pattern characterized Cold War nuclear dynamics. In the 1950s, the United States did everything it could to build up its nuclear forces. But, by the mid-1960s, restraint, arms control, and détente became new U.S. goals. Arms competitions have ups and down. The goals change. Today it would be a good idea to emphasize the long-term hazards of the arms race simply to bring this issue forward by several years, rather than waiting for this "turn"

to develop or be discovered on its own. This is the personal view of the author.

The arms control regime created during the Cold War can no longer guarantee strategic stability. Advanced technologies, such as cyber, AI, and hypersonic missiles, will alter the global nuclear balance from what it is today.

Methodological Issues

Progress in tracking mobile missiles is likely to be rapid because the underlying technologies are from commercial innovation. DoD innovation, so to speak, has "sped up," and the locus of innovation in U.S. defense is now in small and medium-sized enterprises (SMEs) rather than in big defense companies and in-house government laboratories.

There is a systematic bias in the "legacy" U.S. defense innovation system (the big defense companies, the intelligence community, DoD, in-house government laboratories) to understate the impact of technology on defense, especially of other countries. China's rapid increase in military ability, North Korea's nuclear missile program, were overlooked for years, in part, because of this behavioral bias.

Tracking mobile missiles is an example of "spin-on" innovation. The underlying technologies originated in the mass market (Apple, Facebook, Google, Uber, etc.). It is only in the last fifteen years that DoD financial backing has tried to systematically spin on this technology into the defense sector.

Some new aids to thought are badly needed to break out of what has become a stale academic treatment of deterrence and nuclear weapons. A useful set of tools for this comes from management,

and from the companies who've spent billions of dollars on advanced technologies like AVs (autonomous vehicles), 5G, AI, machine learning, vehicle tracking, and data analytics. These approaches are taught in business schools to analyze technology and corporate strategy. They have not been previously used in strategic studies or political science.

It is very important to think in terms of "technology packages," instead of individual technologies. This is how business develops technology. The packages integrate several technologies into a coherent system. Uber, for example, integrates three separate digital platforms into a single, seamless, integrated package: a communications system to connect customers with rides (the cell phone network), a map direction system (Google maps), and a payments system (PayPal, credit cards). The hunt for mobile missiles is likely to depend on such technology packages, too, rather than breakthroughs in any one technology, like super satellites that "see" everything.

There is often far too much focus on the specifics of a new technology, without sufficient attention given to its overall impact on a strategic posture or on its arms race consequences. Consideration of technology packages, rather than specific technologies, is one way to see these larger impacts.

Value chains, touchpoints, innovation platforms, and information chains (discussed later in the report) are four management frameworks used for analyzing technology packages in business.

All countries have value chains, in the same way that all have "organizations." It would be impossible to deploy a military of any

complexity without them. North Korea's or Israel's mobile missiles, for example, can be analyzed in terms of touchpoints and value chains – regardless of whether they conceptualize them in these terms or not.

Technological competition between countries is best thought of as a contest between value chains, rather than between technologies per se. The United States is building a value chain to hunt North Korean missiles. North Korea, in turn, builds a value chain to hide mobile missiles. The rivalry is between these two value chains. Moreover, there is a coevolution between these two systems. Simply counting North Korea's nuclear arsenal -- or American missiles -- misses the key dynamics shaping the evolving rivalry. This competition between value chains describes other technology intensive rivalries as well, such as the U.S.-China contest in the western Pacific, India vs. Pakistan, and Israel vs. Iran in missiles.

Operational Issues

In the Cold War and until quite recently, limitations of reconnaissance determined targeting, for both conventional and nuclear weapons. There was almost no way to kill moving targets short of massive barrage attacks.

Today, new reconnaissance technologies overcome many of these limits. New initiatives in cyber further offer ways to disrupt command and control.

The ability to track mobile missiles uses computer algorithms, vast data centers, cloud computing, and deep learning. The "work" of finding missiles is done by secretive organizations. A satellite picture of the physical plants tells one nothing about what is going on

inside. The situation was different in the Cold War. With difficulty, satellites could count enemy missiles. This "counting" of the threat is much more difficult today.

There are ways to penetrate this secretive world, however. Insiders, turncoats, and cyber espionage can to an extent assess capabilities. This is one reason that the "insider threat" receives emphasis in this report.

Insider attack of mobile missiles and command and control by agents, turncoats, special forces, saboteurs, and IT department staffers raise the insider threat to an altogether new level. The potential of "insiders with a flash drive" to wreak damage has been highlighted by reports that the Stuxnet virus, which infected Iran's centrifuge enrichment control system in the late 2000s, was implanted by an insider employee working for a foreign intelligence service. These and other attacks could cripple a mobile missile force (e.g., by disrupting its command and control or by interfering with locks on atomic weapons).

A full dispersal of mobile missiles from their peacetime locations is an extraordinary, dangerous threshold to cross. It has never taken place in any country. Full dispersal intensifies a crisis and leads to hypervigilance in the enemy and the region. It could provoke preemption, by a rival, or conceivably by major powers, like the United States or China.

But raising the danger of war is one reason for missile dispersal. It shows a willingness to risk war to bolster one's bargaining position. It signals resolve. It could also signal irrationality -- in a sense providing a rationality for irrationality. Missile dispersal is like the U.S. nuclear alerts of the Cold War. But the differences with the

Cold War alerts are important to underscore. The United States did not know where Soviet missiles were located in 1962, especially the Soviet IRBMs in Europe. Alerts in the future may increase crisis instability, as a major power may be able to locate enemy missiles precisely, and attack them with conventional counterforce strikes. It is not hard to write nuclear escalation scenarios from this situation.

Dispersal of mobile missiles as a signaling tactic has not had nearly the attention it deserves. Its salience as a "nuclear head game" does not stand out in military plans or academic studies. A decision to disperse missiles would fundamentally transform a crisis, making a confrontation far more dangerous. It will produce a political shock effect for the nations involved, and for most other countries. It could, for example, lead to ripple alerts that spill over to other countries outside of the region.

Dispersal of missiles is one example of a larger set of unrecognized nuclear dynamics. These are thresholds which, if crossed, change a crisis to make it far more dangerous – yet whose significance goes unrecognized or is overlooked in peacetime plans and studies. There were several of these in the Cold War. In the future, examples include massive counterforce cyber attack of electrical power systems and telecommunications, blinding of satellites, and others. The "mating" of atomic warheads to dispersed missiles is another such threshold. It will have extraordinary political impacts, and is increasingly likely to be detected by the advanced collection technologies.

One key problem in the future is the use of missile dispersal for political signaling. This could be the source of complex or complicated "nuclear head games." Partial dispersal might be limited, or might involve only a handful of missiles, or unarmed missiles. These tactics

need careful study. Otherwise they will suddenly "appear" in some future crisis. No president or White House staff (NSC, CIA) can be expected to make sense of them in the time pressured conditions of a nuclear crisis.

In the Cold War, such nuclear head games developed into a high art form. Crises in Berlin, Cuba, and elsewhere saw movement of U.S. nuclear weapons to signal rivals, (e.g., B-52 airborne alerts, dispersal of NATO tactical nuclear weapons form storage igloos). President Richard Nixon had the famous "Madman nuclear alert" to signal Beijing and Moscow to stand down against his bombing of Hanoi. Dispersal of mobile missiles by Pakistan, Israel, North Korea, or Iran are like this Cold War practice. They might well be intended to be detected by the enemy, and allies, as signals. They are more likely than actual strikes, yet receive far less attention.

Dispersal of mobile missiles for political signaling shows something else that is very important: a country does not require a sophisticated technological force in order to have a very sophisticated political strategy for nuclear weapons. The political strategy may be designed for spoofing, and keeping the pot boiling, rather than for deterrence. This is particularly true for secondary, smaller powers (Israel, Iran, North Korea, Pakistan), who need to manipulate major powers to come to their assistance when they get in trouble. Moving mobile missiles around, "noisy alerts," are an ideal way to do this.

The hunt for mobile missiles undermines the deterrents of the second-tier nuclear powers. New reconnaissance technologies make them vulnerable to conventional precision strike (conventional counterforce) from armed drones, hypersonic missiles, and stealth aircraft like the F-35. The mere perception that their relatively small

nuclear forces are not going to be survivable could have far reaching consequences.

Countermeasures to the hunt for mobile missiles could involve dangerous or highly undesirable developments. The most likely counter is to deploy more nuclear missiles. Other countermeasures include AI-generated "pictures" of different data sets (voice, images, text, intercepts) to create a deceptive picture of a missile force's position and readiness. Generative Adversarial Networks (GANs) are an AI method to tweak the probabilities of detection and movement to accept a falsified picture of a situation.

Arms control efforts to "cap" second-tier nuclear states' arsenals at levels of minimum deterrence will likely be an early victim of major power reconnaissance technology improvement.

Efforts to "fool" missile tracking systems will be a feature of the new arms race. Deception, AI-doctored images, decoy missiles, and virtual electronic missiles are a few of the many possibilities. GAN technologies will have especially important roles here.

Advanced technologies offer unprecedented ability to track individuals in key military units, including senior officers, their staffs, missile crews, atomic weapon protection guards, and political leaders. Their location and movement are an extraordinary way to gain intelligence and warning. Tracking people could provide insight into changes in alert levels and intentions.

Predictive analytics may be used to estimate the future state of a nuclear force. It could be used to predict the next location of a missile, and the location after next. Analytics could also distinguish routine from non-routine missile and warhead movements (e.g., by

whether key senior commanders were present, or whether atomic warhead units were close or distant from the missiles).

The main way to locate mobile missiles comes from the synergy of combining technologies: phone hacks, drone video, cyber penetration, spies, communication intercepts, facial recognition, hacked security cameras, and new kinds of radar. The vast amount of data generated from these collectors requires AI, cloud computing, edge computing, and data analytics to process and display it. It also requires real-time information chains linked to quick-reaction alert (QRA) weapons like hypersonic missiles, armed drones, F-35s, and other systems.

Part I

INTRODUCTION

The hunt for mobile missiles is becoming faster, cheaper, and better. By itself, this is an important statement with significant long-term consequences – because, over the last thirty years, countries with nuclear weapons have shifted much of their force to land-based mobile missiles. In particular, North Korea, India, and Pakistan rely on them. Iran, a country of great nuclear concern, does so as well. China and Russia also rely on mobile missiles. The hunt for mobile missiles threatens to undermine this enormous investment and to undermine the nuclear foundation of their security. It is something that they cannot – and will not -- ignore.

There are larger dimensions related to hunting mobile missiles than undermining nuclear deterrence. Because the way that the hunt for mobile missiles is improving is through the integration of advanced technologies like AI, cyber, drones, cloud computing, data analytics, and deep learning, with weapons that are tightly linked

into an overall kill chain. Quick-reaction alert weapons (QRA) are fast responding kinetic or cyber weapons directly integrated with the search technologies used to find mobile targets. They include hypersonic missiles, armed drones, F-35s, and cyber weapons. The hunt for mobile missiles, then, offers a foretaste of the dynamics of a rapidly developing arms race that pulls together old and new weapons.

With great power competition increasing, the hunt for mobile missiles has a larger meaning that goes beyond nuclear strategy. A significant part of this rivalry will involve technological innovation. This means doing old missions better, and using technology to create new missions. One of these new missions is tracking mobile targets. It looks certain to drive the arms race among the major powers, and countermeasures, to forestall the growing ability of major powers to threaten the nuclear forces of the smaller, secondary powers. The major powers themselves will feel threatened by each other's developments here as well.

Taking this larger perspective, there are three reasons for studying the growing ability to hit mobile targets. First, while there is an acceptance of the growing importance of technology, there is a strong tendency in the United States to focus on the details of individual technologies. Thus, books about "drone warfare" or "AI" are written from the perspective of who's ahead in these different technologies, and how the individual technologies will reshape the nature of war. Questions like "Is China or Russia ahead of the United States in hypersonic missile technology?" are advanced.

This report takes a different perspective. In our judgment, such a "Who's ahead?" focus overlooks the nature of the technological

revolution that is now taking place. As the opening quotation from Edgar Allan Poe underscores, focusing on the technical details often lets one see a few things more clearly. This is especially true because the details are so incredible. But like Poe's Paris police, a focus on the details leads to missing the larger whole that is taking shape. The use of these technologies, and the risk of war itself, are shaped by governments with strategies that operate at a level higher than technology. It is impossible to make rational investment decisions focusing only on the technology level. Only at a higher strategic level does the necessary perspective develop to see how the technologies influence questions of war, peace, and power. This is the reason for the methodological innovations used in this report. They have been found useful in guiding investments from a higher strategic level in technologically intensive businesses. Stated a bit differently, the methods force leaders and their staffs to take higher level strategic perspective than the details of technology.

A second "big picture" effect of an improving ability to track mobile missiles is that it focuses on long-term patterns and cycles of intensity of the rivalry. We should already know this from the Cold War. But it is too often forgotten. Most of the big systems of the Cold War (strategic bombers and missiles, command and control, super accurate missiles) took a decade or more to build. There were periods of building up the nuclear force of the two superpowers at all cost, with almost no thought whatever given to restraint. Then, there were periods with the opposite trend, when slowing the arms race became all important.

In short, the Cold War "arms race" wasn't a linear story of action and reaction as each side tried to top the other's moves. For some eras it was like this, but for others it wasn't. There's an extremely important

lesson here. Namely, great power rivalry looks very different over long periods of time measured in years and decades than it does over the days and weeks that are the focus of the news cycle. Not only is a higher-level perspective needed, it should also be one that is longer term if we are to understand the dynamics of technology and politics.

We should expect comparable dynamics in any future rivalry. Rhythms will develop. As just one example that is relevant to the topic of this report, one reason the United States nuclear arms race slowed down in the 1960s and 1970s was that it was pointless to acquire more nuclear weapons when all of the enemy's fixed targets could be destroyed many times over. Reconnaissance limitations – especially the inability to locate moving targets – and "overkill" of fixed targets convinced policy makers that it was futile to invest more money into strategic nuclear weapons.

A third reason for looking at the problem as a whole is that there may be dangerous thresholds that are missed when focusing only on the details of who has what technology. The hunt for mobile missiles shows this, and one of the key findings of this report is that they will likely lead to the creation of new thresholds of crisis intensity. The decision to disperse and arm mobile missiles with nuclear warheads has enormous consequences. As far as we can tell, it has never happened. Think of North Korea and the United States, or of India and Pakistan. The dispersal decision could provoke an immediate attack. Or it could bolster deterrence. Or it could raise the chance of accidental war. A country could disperse missiles from peacetime storage locations as a move in a nuclear "head game" with its rival, as Cold War alerts did back then. Dispersal could be used for political signaling, something especially important for smaller

nuclear states like North Korea or Pakistan. Although the crisis management aspects of a dispersal decision are critical, so far as I am aware this report offers the first serious analysis of them.

The hunt for mobile missiles tells us a great deal about the world of military technology we are now entering. This world can be thought of as made up of several "exemplars." As used in this report, an exemplar is a technological program or achievement that is an outstanding example of a strategic concept. The idea of an exemplar comes from Thomas Kuhn in studying scientific revolutions. In his original formulation Kuhn used the much broader idea of a paradigm shift, basically a complete change in world view, as in the shift to Newtonian physics from the classical model of Ptolemy. But overuse of the idea of "paradigm shift" led to many people questioning its usefulness. Instead of a paradigm, Kuhn later used the idea of an exemplar. This was an intellectually stripped-down version of a paradigm that applied only to particular examples of a concept. Military exemplars include the Manhattan Project, Sputnik, the U.S. moon landing, and the AI win over human players in Go. These were all major demonstrations of concept. They pointed to new potential applications of the technology.

The only claim for an exemplar is that it is an outstanding demonstration of a strategic concept. In the transition to a new military world from AI and other technologies it looks as if there will be several exemplars. Together these may or may not lead to some paradigm shift. What are the exemplars for today's world? One is the hunt for mobile missiles, the focus of this report. Another might be some sophisticated way to manipulate or shape public opinion using social media. Still another exemplar might come from quantum computing, with its potential to break any type

of encryption and for leading to exotic new weapons like quantum radar and quantum ASW. This report does not deal with these other, possible exemplars.

The report does deal with the hunt for mobile missiles as an exemplar in the sense of the term used here. Characteristic features of this particular example are that it creates a way to track mobile targets that are faster, cheaper, and better. Each term is important here. The search for mobile missiles is becoming faster because it is based on real-time reconnaissance: Drone video, satellite imagery, cell phone hacks, security and camera system penetrations. This information is collected in real time. By itself, this is radically different from the reconnaissance technology of the Cold War. Then, U-2 aircraft, satellites, spies, and analog radio signal intercepts had a two-to-four day delay built in. This was to collect and process the information. Photos had to be developed, and intercepts decoded and translated. Everything was done offline. In modern phrasing, the latency of Cold War information processing was about two orders of magnitude greater than it is today.

The search for mobile missiles is also getting cheaper. Like the information revolution more generally, the cost of information is going down. This is Moore's Law. The new, advanced technologies listed above are virtually all developed in the commercial sector. They were not developed in U.S. government research centers. This is especially the case for the key technologies needed to process the vast amounts of data flowing from the multiple collection systems described later in this report. AI, cloud computing, data analytics, and deep learning are dropping in price as they are used in commercial markets. This is one reason, for example, that China's autonomous vehicle (AV) program is so important. The scale of use of AI in the

auto sector drives its price down for use in other sectors.

Finally, the hunt for mobile missile is becoming better because it is built on multi-phenomenology, multi-sensor inputs. Different kinds of information can be used to estimate a missile's location (e.g., a cell phone intercept from a weapon's crew, a drone video, and a satellite image). These are three very different types of information. The result is a better estimate of a missile's location.

Comments on Methodology

This report offers some new methodologies for analyzing military technology and its impact. While the need for new methods has increased with the amount of technology, earlier historical periods had many of the problems that these methods are meant to handle. For this reason, it is believed that a summary of these methods should be placed at the beginning of the report rather than developed along the way.

These methods do not predict what is going to happen, nor are they scientific formulations in the sense of physics or chemistry. They are management frameworks. They have their origin in business. Companies like IBM, GE, Google, Apple, Facebook, and Ford try to grapple with the challenge of new technology. The methods are widely taught in business schools to students in courses with titles such as Technology and Global Strategy or The Global Corporation.[5]

In many respects the challenges facing a large, complex military organization like DoD or a private company like Google or Ford Motors are the same. They face the challenge of complexity. Indeed,

5 These courses are taught at the Yale School of Management by the author.

many business schools define management in terms of complexity for this reason. Deciding what to focus on, and getting a handle on the large number of details at the same time is what management is about.

In the cases of interest in this report the complexity is doubly difficult. It involves advanced technologies used in new applications that are themselves poorly understood. No one knows, for example, how China or Russia, or any other country will incorporate advanced technologies into their armed forces. Nor does anyone know how nuclear weapon programs will develop, and how these will be reshaped by this advanced technology.

The problem of complexity is not unique to defense, however. It arises for any large enterprise where there is technological and organizational complexity. There are many examples of enterprises who have confronted this. There are historical cases, like the United States in World War II and the Cold War. There are contemporary examples in the corporate world.

What may confidently be said is that technological complexity exists in all countries. It isn't something that is "removed" by reason of politics or national culture. China cannot use Sun Tzu to escape from the vast complexity it faces in its missile programs, just as the United States cannot do it using Clausewitz. Of course, this is no reason to avoid reading these great thinkers. Rather, it just makes an obvious point. Large enterprises, whether military or commercial, cannot escape the complexity problem. And one way to deal with it is to use frameworks that have been found useful to raise the level of analysis about these problems. Note again, that these methods are not used for prediction. The goal is more modest. Moreover, we

have no way to predict the future or to develop a reasonable theory of change.

A reason to borrow frameworks from management is that businesses confront the complexity of digital transformation on a daily basis. Digital transformation has disrupted one industry after another. It has fundamentally transformed retail, financial services, transportation, and even the fundamental character of work itself. The next wave of disruptive technologies is almost here in areas such as autonomous vehicles (AVs), and 5G communications, and the Internet of Things (IoT). These impending tsunamis will have even more impact than Amazon, Uber, and Apple have had.

So, the question becomes: how would large companies look at the way advanced technologies could be used? One of the answers is that regardless of industry or technology, there are useful frameworks for dealing so.

These questions will show how institutions with more experience in high tech disruption than any other frame the problem. At the same time, they show the need to get above the level of technology. It is very easy to get lost in the technical details of drone swarms, denial of service attacks, and GPS jamming. But the challenge isn't only about dealing with all of these details. It's also about providing leadership – that is, strategic direction -- to an organization on what technologies to develop, ways to combine them, and ways to align them with a corporate strategy.

This is done in the large technologically intensive corporation. Another place is the business school. Business schools have as a mission the capture of knowledge less about the technologies of AI and cyber, etc., than about managing these technologies and also

leading the technological reorganization of the firm around them. This is what I mean by arguing that a higher-level approach is required than what is usually found. It is "higher" in the sense of providing strategic direction from the apex level of the organization.

The methodology used in this report will draw on four key management concepts widely used in the business schools and in the corporate world. They have had little exposure or application in defense.

Each of the four concepts will be developed in more detail with examplar applications in the hunt for mobile missiles. But it useful to summarize the concepts here as they structure the ways any country can use technology.

"Touchpoints"

In business, a touchpoint is any interaction between a customer and the company. Someone visits a web site, or they enter a store. These are both touchpoints. A customer watches a TV advertisement for the company, or receives a pop-up ad on their phone, and has two more touchpoints. Customers who download apps that provide the company with continuous location information are providing a stream of touchpoints.

The basic idea of touchpoints is that there are almost always a lot more interactions taking place than people think. And that a company needs to look at their overall collection of touchpoints to shape the composite interaction with a customer. A great deal of business school research has found that unless companies are conscious of touchpoints, they will have a haphazard approach that is inconsistent for driving focused messages important for the firm's

success.

Touchpoints have long existed. What is new today is the skyrocketing number of touchpoints arising from the social media explosion, from the Internet, cable TV, and from media stories. Most large firms now consider it very dangerous to simply leave the process of reaching the customer to its natural tendencies, absent strategic direction. For one thing, a hands-off approach would lead to wasted spending on marketing, or worse, conflicting marketing messages in different touchpoint channels.

Another new feature of touchpoint analysis is technology that can increase the kinds and numbers of interactions between a company and its customers. The goal of many companies is to gather more information about customers. The National Basketball Association, for example, has downloadable phone apps that let fans look up players statistics, get discounts on team clothes, and discounted preferred seating at games. Another example is Saks Fifth Avenue's New York store, which recently redesigned its cosmetics department to allow customers to wander around various displays and be able to touch the cosmetics, try them out, and get advice from trained "style advisors." This is all done in an intensively designed environment of music, smells, and visuals that try to shape the customer experience in positive, relaxed ways.

There are many different touchpoint strategies. A "low touch" strategy involves only interacting with customers through a small number of channels. This might be due to budget limits, or purchase of commodities like wheat. The Cold War had low a low touch strategy between U.S. reconnaissance and Soviet missiles. "Contacts" in the 1950s and early 1960s were limited by the number

of satellite passes, which was low. Soviet counterintelligence made espionage difficult. And radio intercepts were random, and slow. Each intercept required someone with headphones, translators, and other handlers.

In contrast, a high touch strategy entails building continuous, frequent interactions. The new Disney Star Wars hotel is an example of a high touch strategy. In addition to themed rides and entertainment, the resort offers space costumes for children, special "space cocktails" with smoke coming from them, and Disney TV channels in the room and on customers' phones. Each of these is a touchpoint. Many of them are continuous while in the facility. Disney's touchpoints are integrated using AI-directed cameras deployed around the resort that measure the "delight factor" of its customers. That is, their posture, facial expression, gait, and movement are all monitored and categorized to estimate whether the guest is having a good time.

In our use of touchpoints, the "customer" is a mobile missile. Or it may be the atomic warhead for that missile. Or it could be the support crew or the trucks in the missile battery. The "company" is an intelligence service that wishes to know the location and readiness state of a missile. A satellite snapping a picture of a mobile missile; a track of a cell phone used by its maintenance crew; a drone passing over with a camera -- these are all touchpoints (or contact points) between the missile (or something closely associated with it) and a seeker who wishes to understand where it is and what it's up to. Note here that the seeker likely may choose a touchpoint strategy that is covert or at least stealthy. That is, the seeker may wish to avoid alerting the hider (the missile or its crew) that they are being tracked. This is not altogether different from the Disney example, where the AI "customer delight" measuring system is in a sense

covert, it is in the background in an unobtrusive way.

Alternatively, a "seeker" may wish to send a message to the "hider" that it knows what's going on. They might even choose to purposefully increase reconnaissance in a way that is noticed, to signal this fact. In the Cold War, both sides often launched multiple satellites in a crisis, or when there was suspicious activity as a way to signal the other side that it wasn't going to get away with anything. In short, touchpoints can get very complex and psychological. In business, there's a definite trend to drive touchpoints into the psychographics of customers.

One observation about touchpoints is that their number and frequency is today vastly greater than it was in the Cold War. By today's standards, Cold War touchpoints were few and far between. Satellite passes, U-2 overflights, signal intercepts, and spy reports were about all there was. In this report, we quickly found at least 25 touchpoints that could be collected to track mobile missiles. Since this report is an academic study, and not a military planning effort, other touchpoints were overlooked. A classified military study would find far more touchpoints.

Compared to the Cold War, the latency of touchpoint data is low for today's touchpoints. It is often in real time. Cell phone hacks and automated license plate readers are examples. But there are many more. This is important for the focus of this report because the whole point of using mobile missiles is to create fleeting targets.

Finally, like business use of touchpoints, there are strategies for leveraging them. Some countries may have low touch approaches, and others high touch. It is hard to imagine that North Korea could ever match China in reconnaissance in East Asia. (On the other

hand, it isn't hard to imagine China transferring some information to North Korea). Touchpoint strategies have reached a high level of sophistication in business. There are courses taught about it, and books written as well. We expect this to happen in the defense world as well.

One strategy might emphasize using touchpoints for political signaling or for "nuclear head games." This kind of thing has already developed in political rivalry. Russian efforts in the 2016 U.S. election are an example. Cambridge Analytica was a consulting company built around manipulating touchpoints in many areas, such as phony news stories, social media, and using trolls to mock a candidate. Another use of touchpoints was by corrupt businesses that used a hired-gun London consulting firm (Bell Pottinger) to sow racial tension in South Africa in the 2010s to distract attention from the corruption of political leadership in the government.[6]

Other touchpoint strategies could focus on aligning the seeker's information and communication channels to create a reconnaissance network that tracks mobile missiles. Here, touchpoints are a way to draw a line around the technologies that are otherwise impossibly complex to understand or manage. They answer the question: "How does one handle the vast complexity of so much information from so many different sources?" The answer it gives is to organize them around their performance in a specific mission – namely, hunting mobile missiles.

Information Chains

6 "State Capture: How the Gupta Brothers Hijacked South Africa Using Bribes Instead of Bullets," *Vanity Fair*, March 2019.

Information chains are communication lines that connect touchpoint data with the analytical process to build a composite picture of the situation. Today, in business and defense, touchpoint information flows to a center that does this. At the center, senior executives and staffs analyze the situation. They move things around, increase a budget here, and put more resources into one touchpoint or into some way to serve the customer better. This has been the historical pattern. The best example is a headquarters that draws in all relevant information about enemy forces, where they are, and what they're doing. In the old days this was the goal. Headquarters might be in the Pentagon or in the White House Situation Room.

One of the great concerns in recent years is that enemies could attack U.S. information chains that connected Washington with overseas forces. Fiber optic lines, satellite links, radio signals up to the satellites – these are the U.S. information chains. Without them, there is no command and control. There is no intelligence conveyed up and down the military command chain.

Recently, a new technological development has allowed a variation of this pattern. Information may be analyzed close to where it is collected. This is called "edge computing." It has very important applications for intelligence and military operations. The benefit of proximity to targets is to cut down on data sent to a central server or headquarters. These data flows can be detected by the enemy, and are a tip-off to the hider for this reason. Many of the new reconnaissance technologies are physically "small." They do not have a lot of space for on-board processing or computing. Drones built to be unobtrusive or designed to appear to look like birds flying overhead are like this. AI requires a lot of data processing and for this reason is hard to use in a drone, in a network box, or in a

cell phone. Edge computing allows AI to be used in these small spaces, like routers or security cameras in the field. An enormous investment is underway in China and the United States to deal with this problem using edge computing.

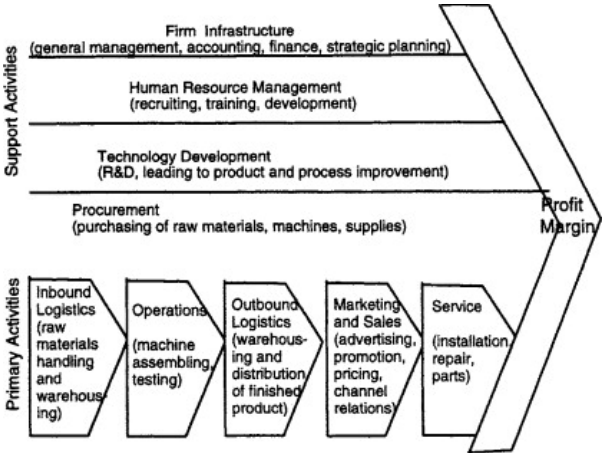
It is interesting to note that, historically, information chains aligned with organizational structure. For example, the corps and division forces from Napoleon through the Korean War had access only to the information they directly collected from scouts or air reconnaissance, whether this was from balloon or aircraft. This information would be sent up the chain of command to a higher level for analysis. What is happening today is that information is pulled out of organizational silos for storage and processing in the cloud. Information chains are the bedrock foundation of this process. All of the considerations of hardening, protection, concealment, and redundancy apply to their design. Likewise, attack of an enemy's information chains – cutting them, interfering with them, disrupting them – is easier because they are no longer inside the military structures they were originally built to serve. It was hard to attack an army division's communications without first attacking that division. Things are different today: the division's key data is now uploaded to the cloud over satellites and fiber lines. The only defenses are technological, not military.

The Value Chain

In business a value chain is a set of coordinated activities an organization performs in order to deliver a product or service. The activities describe the basic work of the organization. Core activities include sourcing, manufacturing, distribution, sales, etc. In addition, there are associated support activities like human resource management and R&D that are also included. All businesses,

indeed all organizations, may be looked at in terms of a value chain.

A general value chain is shown in the figure below. This diagram depicts a general characterization of an organization without regard to what it produces. It could be a soft drink manufacturer, or it could be a technology company.



For a manufacturing example, there are inbound logistics, manufacturing operations, outbound logistics (distribution), and service of the product. If the "business" was nuclear missiles, there would be two value chains, one for atomic weapons and one for missiles. The inbound nuclear logistics would include enriched uranium, reprocessed plutonium, special metals, test equipment, etc. Israel, to take as an example, got these items in the 1960s from France, and from scavenging all over Europe using front companies and secret buyers. North Korea has a similar collection of inbound logistics. Operations would be the construction of a functioning explosive device and its production of warheads of various kinds.

Outbound logistics would describe how the weapons were given to the military or to some special nuclear force. For example, Pakistan in recent years has decided to provide its navy, air force, and army with nuclear weapons. Each service has different needs, and this has to be coordinated with the operations part of the nuclear weapon value chain. "Marketing and sales" would cover things like doctrinal developments, rules for handling the weapons by the services, and training of a guard force to protect them. Service would describe making sure the weapons were in a useable condition.

A missile value chain would include missile components, heat shields, electronics, launch pads, overseas procurement "front" companies, and computers. It isn't hard to see how it can be described as a value chain.

Acquisition of nuclear missiles is one example of a value chain. Another is the hunt for mobile missiles -- i.e., a value chain built to counter nuclear missiles by tracking them and a means to destroy them. This value chain is examined later in this report. For now, it need only be pointed out that the "inbound logistics" for this chain would include information about their location – touchpoints -- and that the data links between the touchpoints to the finder. These links are information chains.

A value chain analysis describes rivalry less as a competition between countries, and more as competition between value chains. This competition is interactive. That is, one side bases its actions after looking at what the other has done. This is an example of the coevolution of the value chains. The two rival value chains – mobile nuclear missiles and touchpoints with information links back to the finder's weapons -- evolve in part, in reaction to each other.

This is a different way of looking at technology developments. For example, North Korea builds a nuclear missile force using two parallel value chains, one for nuclear weapons and one for missiles. The United States observes this decade-long development. It sees signs of North Korea buying special metals and parts from other countries or on commercial markets. It takes satellite pictures of missile engine tests in North Korea and nuclear tests. The United States builds its countering system after watching these things. This produces a value chain for hunting mobile missiles. In turn, North Korea likely will try to counter American actions in various ways.

Key issues raised by the value chain concept are how tightly the activities are coordinated with each other. One of the key conclusions of this report is that the major powers are using AI and other digital technologies to tighten the coupling between the activities in value chains to track mobile targets. Here, new technologies aren't used to do things like improve accuracy, as was the case in the Cold War, but to closely track movements and readiness conditions of the target. This requires large-scale, real-time data integration from the touchpoints.

Value chains are especially useful to analyze technology-driven industries. One example of this is how much to invest in each activity of the chain. They offer a way to take a higher-level perspective above the individual technologies. In addition to allocating resources, the value chain also raises the question of how tightly its activities are coordinated. This is especially important nowadays because many of the advanced technologies like AI, machine learning, and data analytics have their greatest impact in just this way. They can be used to tighten the value chain to make it responsive. Indeed, that is one of their main uses in industry today.

Finally, it should be mentioned that value chains are different from another term that is increasingly used in military circles -- kill chains. Kill chains narrowly focus on the kinetic military aspects of a problem. Value chains, on the other hand, incorporate strategic and crisis management assessments that transcend operational considerations. Political signaling and nuclear head games would likely be excluded from a kill chain, but would be extremely important considerations for a higher level assessment. Likewise, value chains describe the future enterprise, as they analyze where investments in the future organization should be made.

Innovation Platforms

A digital platform is a computer term describing the software and hardware of a site to connect its customers with markets, or to coordinate their interactions with an organization. Examples are Airbnb, Uber, Amazon for shopping, and eBay.

Broadly speaking, there are two kinds of platforms. Transaction platforms bring buyers and sellers together. Examples are ecommerce sites like eBay and Amazon. Likewise, Uber's ride-hailing platform brings drivers and riders together.

A second kind of platform are innovation platforms. These are the technology foundations on which other applications are built. Examples include Microsoft Windows, Google's Android, and Amazon Web Services. Innovation platforms have become the fundamental building blocks of innovation in the modern world economy. These are the building blocks of nearly all of the disruptions that have changed economics and business.

The U.S. military has lagged behind the commercial sector in

innovation platforms by some 5-8 years. But the military is now playing catch up. In a relative sense, innovation has shifted from government research laboratories to commercial innovation platforms. The DoD is now building special versions of "hardened" platforms resistant to hacking or disruption for use by the intelligence community and the military.

One especially important innovation platform is cloud computing. Cloud computing refers to "always on," on-demand computer resources – data storage and computing power – without the need for direct active management by the user. In other words, introduction of a new reconnaissance technology would seamlessly use cloud resources and would not require separate distinct IT contracting and acquisition to use the technology.

Cloud computing opens up whole new landscapes of innovation in national security. Consider the ride hailing example. Uber uses Cloud computing to integrate three separate digital platforms: a GPS system locating where a customer is and routes to a destination; a cell phone communications system linking driver with passenger; and a payments system that links to a customer's credit card. The result is a seamless ride hailing network, and an extraordinary innovation in transportation.

The Uber case is a 21st century example of a critical innovation development for many decades. This is technology synergy. It refers to the larger payoff from combining technologies than from using them individually. A classic example comes from the Cold War. In the 1950s there were separate, distinct technology advances in inertial guidance for missiles, nuclear propulsion, solid fuel rocket motors, and navigation so that an underwater submarine could tell

where it was. The combination of technologies led to synergies, and the result was the Polaris SSBN force of nuclear firing submarines. Polaris dramatically altered the nuclear deterrence landscape because it offered a secure second-strike force. This had enormous implications for capping the nuclear buildup, for arms control, and for driving down the probability of accidental nuclear war.

The point to underscore is the strong likelihood that there will be future synergies, and that they will come from software rather than hardware, as in the Polaris example. This is why cloud computing is so important. It isn't because it's cheaper, and more flexible, although it is both of these things. Rather, it's because it creates an innovation platform for software, and all of the associated tools like AI, data analytics, machine learning, etc. The very structure of innovation has changed because of cloud computing.

To give one sense of the scale of this change, a modern intelligence service today can easily process 500 million data records made up of phone calls, emails, and texts to target some 50 people who are suspected terrorists.[7] For the focus of this report, suppose the 50 people in question are not terrorists. They are crew members on a mobile missile force, or guards of atomic weapons that are mobile to keep up with the missiles. Soon, hundreds of billions of records will be swept by intelligence services because of the scalability of the cloud. One country could swallow the whole communications system of another, for the purpose of tracking a few hundred targeted

7 These are actual numbers taken from NSA reports to Congress in 2017. See Office of the Director of the Office of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities*, Office of Civil Liberties, Privacy, and Transparency, April 2018, and summarized in "NSA Triples Collection from US Phone Companies," *New York Times*, May 4, 2018.

individuals.

Nuclear Postures

The immediate focus of this report is land-based mobile missiles. However, these missiles are one element in a larger framework of nuclear strategy and they must be looked at in these terms. Fixed site missiles, bombers, and SLBMs are other weapon elements. Short-range nuclear weapons could be added to this picture. So could command and control, doctrine, people, and organizational structure.

But my purpose is not to once again describe how nuclear postures have developed. There are many excellent histories that do this. Nor is it to warn of dangers from new technologies or from the spread of nuclear weapons. Again, there are many reports and journalistic treatments that do this. Rather it is to make a different point, one that's important to state clearly up front: the evolution of nuclear forces has been a competition between the weapons themselves and the reconnaissance technology available to find them. In simplest terms, limitations of reconnaissance technology determined targeting strategy. This meant in the Cold War that there was no utility in fielding more nuclear weapons because there was no useful target they could be fired at as none could be found using the reconnaissance technology of the era.

For example, in the Cold War long-range nuclear missiles and bombers were aimed against the enemy's fixed site forces. This includes their ICBMs, airfields, and command and control.

Although missile sites and airfields could be struck, there was no guarantee that the missiles or bombers would still be there. If they had been launched, the incoming missiles would be destroying empty holes and vacant airfields. This weakness was one source of nuclear instability, that the first to launch would have a better chance of catching enemy forces before they had been fired. It was dubbed quite fittingly by Thomas Schelling "the reciprocal fear of surprise attack."

The United States undertook efforts to build reconnaissance to determine whether enemy missiles had been fired or if the bombers had been launched. Infrared sensors on satellites could detect missile launches from the heat of the engine exhaust. In theory, a computer could be fed this information and the enemy missile could be associated with a particular silo. Then the U.S. nuclear war plan could be recalculated so as not to waste missiles against empty silos. This was called "reoptimizing the SIOP" (the single integrated operational plan, the U.S. nuclear war plan in the Cold War).

But all of this is nuclear strategy theory. It was never really possible because the sensors were not accurate enough, and because the information processing system with its latency and vulnerability was just not up to the task.

One area where reconnaissance technology was up to the task was with tactical nuclear weapons. These short-range weapons could accurately be fired against moving targets. But this was because the reconnaissance system was the same one used by Napoleon and by Eisenhower at D-Day -- human forward spotters. The spotters might be in airplanes over the battlefield. Or, conceivably, they might be listening in to radio enemy messages that revealed locations of

particular units. This is what was taking place in the Battle of the Atlantic in World War II. The British cracked the German codes for messages sent to their submarines in the North Atlantic. These messages were intercepted, decodes, translated, and analyzed quite successfully. It turned the tide in the war of submarines against shipping.

While something akin to a system of eyeball (or ear) spotting could be conceived for the tactical nuclear battle in Europe, there were many other problems with tactical nuclear weapons, that such a comparable system was never built. But the difference between the tactic and the strategic battles shows the differences in how reconnaissance impacted targeted strategy.

The reason this history is described is because the current revolution in technologies radically changes reconnaissance. Missiles haven't changed that much since the Cold War. But the advent of new, advanced technologies like cyberwar, AI, drones, for reconnaissance has changed. The term reconnaissance technology as used in this report includes aircraft, satellites, signals intelligence (SIGINT), and other kinds of data (human and telemetry intelligence, HUMINT, TELINT, etc.). This includes both collection, analysis, and distribution of the information. In the Cold War, this meant U-2 aircraft, satellites, spies, SIGINT, ELINT, etc.

The coevolution of missiles versus reconnaissance changes, and with it, the very notions of stability that grew up in the Cold War and which are widely used still. It is, so to speak, a model that has aged out.

One big conclusion from this is that reconnaissance improvements mean that a nuclear force – or a conventional one – could be aimed

at moving targets. There are qualifications to this statement. First, the reconnaissance has to be built, and it has to be built as a system. Both of these are important. A major power like the United States, China, or Russia cannot simply leverage the new technologies to better advantage and get a capacity to track mobile targets. Buying more drones, cyber, and satellite pictures will not simply come together and be capable of locating moving targets. This approach may find a missile here or there. But these will be lucky cases. An actual system in the sense of a constructed value chain of interlinked activities will need to be built for it to perform. This statement applies to all countries. At present, there are strong indications that this system is being built, with national variations to be sure. But it is being built. Whether it should be built is a different question still, one discussed later in this report.

The second qualification to the above statement is not so much a limitation as it is an additional insight. There's a very good chance that an arms race will develop around the effort to find mobile targets. This is a safe statement to assert because such an arm race has already begun in East Asia in the 2000s. China has invested enormous resources in it and indeed built its military posture around the tracking of U.S. maritime targets. Ships, submarines, aircraft, bases, command and control – Beijing's posture is designed to track and potentially destroy these forces. Here, the United States is the "hider." It uses deception, jamming, and elaborate countermeasures so as not to be found. The hunt for mobile missiles is the land-based version of this competition.

It is interesting to look at the hunt for mobile missiles this way. This competition raises the possibility that it could spill over into the nuclear arena more generally. In other words, there may be an

accelerated nuclear modernization not only because old systems are wearing out but because the "old" system cannot survive in the advanced technology world of the 21st century. It may be worth noting here that this too seems to be taking place. That is, the United States nuclear modernization now underway is presented as a kind of replacement system meant to put new missiles in place of old ones, thereby maintaining the nuclear balance of many decades. A different interpretation, however, is equally valid. It's that the new realities of vulnerability are understood by the military in Washington, Beijing, and Moscow. They know that command and control can't simply be a redo of the Cold War in a world of massive cyber disruption. Where this will lead isn't clear; the only conclusion offered here is that it leads to an arms race in these technologies and systems.

Nuclear postures do change over the decades and so this shouldn't be all that surprising. It is important to see this change in a coevolutionary perspective in order to understand not only how we've reached the current position, but where this evolution could be heading. There is a tendency in much of the historical nuclear literature to overlook these powerful technological dynamics, and to lock in on measures of stability that are not universals, but rather are specific to a particular technological era.

As technology evolved, the ability to find fixed site nuclear weapons improved. Just as there was a mix of nuclear weapon basing modes, like land based, sea basing, and bombers, so too was there a mix of reconnaissance.

An operations research framework developed in the 1960s pulls these ideas together. It describes explicitly a nuclear posture as a

contest between reconnaissance technology and the basing modes of nuclear weapons. The specific conditions of the model need to be updated, but this isn't difficult. The model, called "max-min theory," has another distinctive feature:[8] It offers an alternative to the aged stability paradigm of the Soviet-American nuclear balance. This alternative is especially useful for analyzing long-term rivalry with advanced technologies, rather than focusing exclusively on short-term crisis stability.

Max-min theory describes a nuclear posture in terms of two general variables: accuracy and search. Accuracy measures how close to the target a force can deliver a warhead. Search measures whether the target can be found in the first place. The philosophy behind the model is relatively simple. A precision weapon is of no use if you don't know where the target is located. Likewise, a weapon does nothing against a target if it can't land near it.

Accuracy in this formulation is measured in terms of CEP (circular error probable). It is the radius of a circle centered on a target within which 50 percent of the warheads are expected to land. A smaller CEP indicates great accuracy. CEP has come to be associated with nuclear ICBMs, but it is actually a purely statistical measure that can be used for conventional warheads as well. Conventional warheads are capable of destroying hardened targets if they get close enough, and this is a very important issue today. Laser or GPS guidance, for example, may bring the CEP down to 1-5 meters and this means that a conventional warhead can destroy a mobile missile -- if it can find it.

8 See John M. Danskin, *The Theory of Max-Min and Its Application to Weapons Allocation Problems* (New York: Springer-Verlag, 1967).

Search is measured by the time it takes to find a target. This is in minutes, hours or days. For some targets, it could be an infinite amount of time -- that is, the target would never be found. An oft-used surrogate variable for search is the amount of money put into reconnaissance technology. In the Cold War era, dollars invested in the U-2 program, ASW, and spy satellites would be counted as "search" investments. The idea is to see what the return on investment in search looks like (i.e., the shape of the curve). For example, in the Cold War, doubling the amount of "search" investments would likely produce small returns measured by how long it took to locate a particular target. This was because of inherent limits on the reconnaissance technology of that era. Such a decreasing marginal returns payoff curve would be a poor use of resources.

For nuclear weapons analysts have long understood the significance of accuracy improvements. Killing power goes up as the square of accuracy. In other words, a doubling of accuracy produces a fourfold increase in lethality. Accuracy, then, was the most important driver behind the missile arms race of the Cold War.

The term "max-min" comes from game theory. But it is very different from game theory in one important respect – namely, that its "moves" are dollar investments in a nuclear posture over a much longer period of time, usually many years. The contest is between two antagonists. One must act, knowing that the second will learn about what he has done, and will act to his best advantage on this information. The question then becomes what should the two antagonists do.

A simple example shows the interaction. North Korea decides to get a nuclear weapon. The decision may be hidden for some time from the United States. Some tests can be conducted in secret, and some

components can be acquired without detection. But the scale of an atomic effort means that at some point in time it will be found out. Plutonium reprocessing involves large reactors. Missiles have to be tested. And a bomb must be detonated to see if the whole design actually fires.

So North Korea builds a force knowing that the U.S. has good reconnaissance to find out it has done so. Moreover, Pyongyang knows that the United States can find some of its nuclear missiles using satellites, drones, and other search technologies. Missiles in fixed locations are an example. If buried underground they stand a good chance of being found, as it may takes months or longer to dig the whole, install the launcher, and remove the spoil.

Once the United States sees what North Korea has done, then a new reconnaissance (search) system is in order to locate North Korea's nuclear targets. It also could invest in better weapons (with more accuracy). Or it could invest in better search technologies. Most likely, the answer is to invest in both. That is, a program of accuracy and search will be the best answer to the new problem of dealing with a nuclear armed North Korea.

I would argue that something close to this describes the last two decades of U.S.- North Korean strategic interactions. Of course, there are bureaucratic issues not accounted for in the model. But the more important point is that max-min describes dynamics far more usefully than the two-strike stability models that seem to be the only way nuclear interactions are analyzed.

In the 1960s, when this theory was originally developed, U.S. policy makers assumed that the Soviet Union would strike first, and that the United States would retaliate. But this assumption is easily

changed to fit different conditions. This is one of the features of max-min. Moreover, today an attacker can invest in very accurate conventional weapons – hypersonic missiles, F-35s, armed drones, cruise missiles – to threaten nuclear targets. This made no sense in the Cold War because conventional weapons then were ineffective against hardened or moving targets.

There are other aspects of the max-min model that are worth highlighting. As constructed, this model does not mono focus on the number of nuclear weapons as a measure of strategic interactions. Instead, it focuses on investments in "search" as a way to counter the adversary. In other words, it explicitly models coevolution of an arms race between a nuclear posture and the reconnaissance effort applied against it.

Even "sophisticated" accounts of nuclear proliferation focus on how many weapons the different countries possess. But this says very little about the interaction dynamics of an arms race that are taking place below the surface of public attention. In many respects, these are more important.

For example, Pakistan and India are engaged in a buildup in nuclear arms. While this is unfortunate from many perspectives it misses another danger that could be much more serious. If India could locate Pakistan's mobile missiles, the stability problem in South Asia will become a lot worse than anything measured by counting bombs. In max-min theory, the focus is on the number of weapons after an enemy strikes first with an undamaged force. This is likely to be quite different than the absolute number of weapons. The second striker has to retaliate with a damaged force, one that is likely to be badly impaired. Max-min frameworks give substantially different

answers about the "value" of a deterrent force compared to simply counting the number of weapons.

A second point to highlight is to underscore that the moves in max-min do not occur at the same time. They take place in sequence. The order of the moves -- who goes first and who goes second -- matters a lot. If the sequence changes, so do the results. Therefore, max min ≠ min max as in game theory.[9] Therefore, this is not game theory. For this reason, there is no notion of bluffing or "threats that leaves some to chance." What is described are long-term investment decisions -- in weapons and reconnaissance -- not short-term crisis moves. This approach offers a usefully different look at the long-term consequences of the arms race rather on focusing on short-term crisis stability. The focus is on multi-year efforts of building or countering a nuclear posture after looking at what a rival has already deployed. The "moves" are not decisions whether to fire missiles or to hold them back; rather, they are how much investment to make in different kinds of weapons (e.g., bombers, missiles, SLBMs) so as to deter attack by preserving a large enough retaliatory force. More, the theory calls for investments in search technologies (like ASW, satellites, reconnaissance aircraft, drones, cyber penetrations, etc.) to locate enemy missiles.

It is in this respect that max-min theory differs from the classic nuclear stability assessment. In the classic Cold War stability formulation, there are no search technologies whatever. Since AI and other technologies (drones, cyber, phone hacks) can be applied to the search mission, this is a major gap. Much of what this

9 This refers to the minimax theorem of two person games, using mixed (random) strategies.

monograph is about is this key issue: search technologies are getting a lot better. The United States, China, and Russia have multi-billion dollar investments to improve them.

Since the start of the atomic age it has been clear that different nuclear postures have different kinds of vulnerabilities. In the Cold War, some weapons were easy to find, but difficult to destroy. Other weapons were hard to find, but easy to kill if they were found. As an example of the first kind consider fixed-base ICBMs. Once both superpowers had spy satellites in the early 1960s, they could locate the missiles of the other side. Actually, it was the absence of this search technology in the 1950s that led to the famous "missile gap" that figured in the 1960 election campaign between John F. Kennedy and Richard Nixon. Contrary to Kennedy's assertion, there was no missile gap. But the United States didn't know this until the surveillance satellites informed the CIA of this fact. Before satellites, the Soviet Union denied overhead air space to U.S. spy airplanes like the U-2, and Washington couldn't know how many missiles the Russians actually had. The change in search technology, spy satellites, greatly informed U.S. intelligence.

But in addition to spy satellites there were other sources of information about U.S. ICBMs. Soviet analysts could comb through Congressional testimony to see where construction budgets were being spent. If a large construction project for the Air Force was authorized for the middle of nowhere – like remote parts of Montana and Wyoming -- it was a tip-off that an ICBM base was getting built. Moscow sent spies to these communities to get more data about the amount of construction and the size of the missile base. The Soviets could read local newspaper in these states, and talk to local contractors. There were intercepts of U.S. communications.

The Soviets always put a great deal of effort into this field, with their embassy in Washington D.C. serving as an antenna farm to monitor the Pentagon, State Department, and the White House. These intercepts might provide a tip-off that an Air Force general was coming out to Wyoming from the Pentagon to inspect progress of the construction.

This diverse information was pulled together by Soviet intelligence to assess where ICBMs were being based, how many, and with what types of weapons. The Soviet Union could do this for the United States. And the United States did it for the Soviet Union.

It is useful to emphasize the very diverse information that went into this effort. Satellite photographs, agent reports from the local area, intercepts, and data drawn from newspaper and Congressional reports. There are two features of this search system that stand out because they underscore just how different the search technology process is today. First, these big ICBM complexes didn't move once they were built. Most U.S. silos are where they were in the 1960s.

Second, the process was very, very slow. It required years, not minutes. It relied on manual processes that took months of careful research, like compiling estimates from Congressional testimony and agents dispatched to monitor construction. So, both ICBM forces and the collection of intelligence about them was slow, expensive, and cumbersome.

But even as ICBMs could be located precisely, they were hard to destroy with the nuclear weapons of the 1960s and 1970s. This was because ICBMs of both sides were placed in hardened underground silos built of reinforced concrete. This protected them from the ground shock of a nuclear burst unless it landed very near the silo.

With the accuracy of ICBMs in this era it was unlikely that many missiles could get very close. The silos also were placed far enough apart from each other so that one warhead could kill, at most, one silo.

ICBMs were easy to find, but hard to destroy. On the other hand, SLBMs were hard to find, but easy to destroy. This was because there was no way to locate them once they left port. ASW was restricted to short ranges, so putting a number of submarines to sea meant that most would survive. The Soviet Navy simply didn't have the ships, communications, and sensors to cover much of the ocean where U.S. SLBMs patrolled. In a war they might luck out and get one or two. But this wouldn't be nearly enough to limit retaliatory damage to their country. If, somehow, submarines could be found they could easily be destroyed. This could be done with depth charges, torpedo attacks, or with nuclear blasts set to detonate below the ocean surface.

It was theoretically possible to destroy many submarines with area attacks. If one knew that submarines were in some relatively confined area, say the Barents Sea or the Sea of Okhotsk, then firing scores or hundreds of hydrogen bombs at the area might destroy them. For obvious reasons this was called a barrage attack. But the mathematics of search and physics worked against this tactic, given the technology of the era. Later in the Cold War, under the terms of the maritime strategy, it became an important tactic in some American plans.

Bombers fit into this framework as well. Bombers parked on known military airfields and armed with nuclear weapons were easy to locate, and easy to kill. A single air burst of a nuclear weapon would

destroy all of them. But if they moved to different airfields they were very hard to find. This was because the surveillance of the era couldn't re-locate quickly to search all possible airfields. In the Cuban missile crisis, for example, the United States shifted its B-47 and B-52 bombers to alternate airfields, including Logan Airport in Boston, so the Soviets couldn't locate them.

Also, bombers could be launched to airborne holding positions. These were called fail-safe positions. The idea was that these were the staging areas to get bombers away from vulnerable airfields. They were called "fail safe" because the U.S. Air Force distinguished between a launch order to get off the ground, and a "go" order to attack the enemy. It was part of an elaborate response to changing tactical conditions.

Both dispersal to alternate airfields and airborne alert were extremely expensive to maintain over any period of time. It also placed enormous stress on the crews, and the guard force of the air bases. There were strict rules for loading the bombers with nuclear weapons, and this required a very large group of specialists and technicians, and guards. Even with the highly professional force that SAC had, and the large Cold War budgets of the 1950s-1970s, this was a very important factor and is useful to remember when we analyze mobile nuclear missiles today. Throughout the Cold War SAC executed a dispersal and airborne alert only a single time. This was the Cuban missile crisis. At other times, SAC practiced elements or pieces of the operation. They might disperse a few bombers. Or they might put a few planes into airborne alert. But only in the Cuban crisis did they exercise the full dispersal and airborne alert plans they had developed.

Another reason that a full dispersal and airborne alert was not executed in a full-out exercise was because it was extremely dangerous. Many B-52s crashed while carrying live nuclear weapons. It was tremendously provocative as well, as the Soviets could detect a big military exercise with their satellites and intelligence. The rarity of SAC bomber dispersals and alerts underscores the practical problems and dangers associated with mobile systems. It is very useful to keep this in mind as we go into a second nuclear age.

The next step for understanding nuclear postures is to combine the different basing modes. With the three types of nuclear weapons, ICBMs, SLBMs, and bombers and accounting for search technology performance, it becomes possible to define composite posture types.

The following table summarizes the combination as it existed in the Cold War:

Easy to Find, Hard to Kill	**Hard to Find, Easy to Kill**
Silo-based ICBMs	SLBMs at sea
	Dispersed and airborne alert bombers

It must be understood that this table describes a particular technological era, the Cold War. In other words, changes can occur, both to weapons and basing, and also to the classification of vulnerability.

Note also how this nuclear posture is slow to change. Nuclear postures are complex institutions that take decades to build. Their cost and complexity mean that they change slowly and only over many years. These changes also are of a scale that they will be observed. Construction of new missile fields, submarines, bombers, etc. will be detected in today's world, as they were in the Cold War.

The other necessary addition to the above table is search technology, and improvements in the technical characteristics and speed of weapons. This is not as easy to capture in the neat form of a table. But it is a critical part of a nuclear posture. In the Cold War the improvements in accuracy especially looked to upset the strategic balance of the 1980s. Accuracy improved from advances in missile guidance to a degree where it became possible to destroy a missile silo with a single warhead. With the advent of MIRV missiles in the 1970s this meant that a single ICBM could carry 8-12 warheads. It could destroy 8-12 silos, in theory. This was destabilizing for military and political reasons. And this instability drove the arms race, and a great deal of politics as well.

This isn't the place to again argue the debate of the late 1970s over Minuteman missile vulnerability. But it is useful to underscore two significant points about that debate because it shows how technology entangles with politics. There was sharp disagreement among experts on these matters. The outcome of this debate was a major arms race -- the Reagan nuclear buildup and modernization of the 1980s. In other words, even if improved Soviet missile accuracy was a fiction, or purely a theoretical possibility, it drove U.S. decisions to build up the force. This is something that could easily occur again, with different technologies, as will be discussed later in this report.

Only U.S. ICBMs and peacetime bombers were vulnerable to improved Soviet missile accuracy. It never threatened U.S. SLBMs or dispersed bombers. Two legs of the nuclear triad, then, were unaffected. This is one reason the debate over how to respond to improving Soviet missile accuracy was so controversial. Many experts argued that since the SLBMs and dispersed bombers were not impacted, there was little reason for the United States to respond. But their arguments were ignored.

So, the United States explored variations of ICBM deployment to offset Soviet improvement in missile accuracy. Mobile missiles were seriously considered. This entailed putting ICBMs on rail cars, barges on the Great Lakes, or on trucks. It was determined that the best choice was a moving system of mobile missiles deployed as a shell game of deception in Utah. This was the MX missile system (for Missile Experimental).

The MX mobile missile, however, was never deployed for reasons of cost and domestic political resistance. Utah did not wish to turn half of the state into a giant missile farm. With the end of the Cold War, all of these efforts to redesign the ICBM force came to an end.

The second noteworthy point about America's flirtation with mobile nuclear missiles is that as ICBM vulnerability was increasing, the United States used new, advanced "search technologies" to make Soviet submarines more vulnerable. This was known as the maritime strategy. The technologies involved were highly classified communications systems that allowed the U.S. Navy and NSA to

penetrate Soviet communications to their SSBN force.[10] In addition, new sensors were developed that could help locate these submarines in certain waters.

The maritime strategy has received far less attention than it deserves. The complex politics and technological interactions are a prime example of major power competition. This is where max-min theory is especially insightful. Because a country watches what its rival builds, and it then comes up with a counter program.

Below the surface of day to day rivalries in the Cold War in the 1970s there was a technological revolution that was driving changes in the nuclear balance, changes that colored the worldviews of the Pentagon and the Soviet military. Politicians in both countries were largely ignorant of these technology dynamics. The defense bureaucracies in each country drove their nation's policies to build bigger and better military systems. This wasn't a case of bureaucracies grabbing more budget for themselves in an expansion of power and authority. There was a definite strategic purpose to the restructured nuclear postures. It would be very surprising if this complex of issues didn't develop again. Whether in the United States, China, or Russia, the potential for big advances new technology programs is quite high. The current relationships among these major powers, not to mention their domestic politics, makes this a plausible development.

10 The maritime strategy is described in Christopher Ford and David Rosenberg, *The Admirals' Advantage: U.S. Navy Operational Intelligence in World War II and the Cold War* (Annapolis, MD: Naval Institute Press, 2014.

PART II

MOBILE MISSILES

The Shift to Mobile Missiles

In the first Gulf War of 1991 Iraq fired 42 Scud missiles into Israel. These unguided missiles did little damage. But they marked a turning point in the world military situation. Iraq had never directly participated in war against Israel with its ground army. It was too far away. What changed in 1991 was that Iraq could get at Israel with missiles, something it couldn't do with air forces or infantry. Neither the United States nor Israel could locate the Iraqi missiles to destroy them before they were fired. This is because they were mobile, mounted on trucks.

The attacks shocked Tel Aviv and Washington because people asked what might happen if atomic or chemical warheads had been used instead of conventional high explosives. It turned out that Iraq in

1991 didn't possess the technical ability for using atomic warheads on the Scuds. But they did have a chemical warhead. With 1950s technology and simple tactics, Iraq was able to evade U.S. strikes, and advance a strategy against Israel -- namely, to bring a distant Middle Eastern state into the battle.

The 1991 attacks also marked a systematic move to mobile missiles around the world. The reason was simple. Iraq's mobile missiles could never be located, but virtually all of its fixed targets could be. They were promptly destroyed by precision U.S. airpower of laser-guided bombs and cruise missiles.

It is easy to get lost in the bewildering array of missiles used by Iraq, Iran, Pakistan, North Korea, Israel, Saudi Arabia, and the other countries. The missile ranges, fuel, and types of mobile launchers present to the average person a seemingly incomprehensible complex picture. But it is more important to see the big picture of what happened in 1990-1. Missiles were shifting from fixed site basing to mobile deployment.

Mobile missiles had been used in the Cold War, especially in Europe. There were short-range missiles like Corporal, Honest John, and Pershing II. There were cruise missiles, like Matador and Mace in the 1950s, and later in the 1980s the ground-launched cruise missile (GLCM). All carried nuclear warheads. But there were many problems with all of these, as will be discussed. The problems have not disappeared.

Some terminology needs to be defined. Mobile missiles are any missiles carried on a truck, tractor, or other such vehicle. Usually, the vehicle is used to set up and launch the missile. But not always, as some small missiles can be fired from very simple launchers

away from their carrier. For this reason, flatbed trailers that merely transport a missile from point A to point B are not considered to be mobile missiles. Mobile missiles may use a jerry-rigged truck, or as recent trends indicate, a special purpose one. Some vehicles have air-filled tires, others are tracked in order to travel on rougher off-road terrain.

Mobile missiles are transported parallel to the ground. That is, when moving around, they are horizontal and cannot be launched. Vehicles stop and there is a set-up period wherein the missile is put upright at some angle. Usually this erector part of the operation is done with fluid dynamics driving the elevator launcher.

A common term to describe self-contained transporter-launcher vehicles is the TEL, or transporter erector launcher. TELs come in a very wide variety of shapes and sizes. Some are developed to a high technical level. The TEL driver can deploy spades that dig into the earth to stabilize the transporter so as to be able to handle the shock of a launch. They may have special stabilizing systems to ensure launch from a flat surface by adjusting the tire pressures in each wheel. Since TELs are meant to be reusable they often have fire-resistant glass windows. They also may have fireproof blankets that are used to cover the vehicle to prevent burn damage.

The parade picture below shows the North Korean Musudan missile on its TEL. It is worth mentioning that this photo shows another benefit of mobile missiles. They are wonderful for parade showings. As we shall see, this psychological element is a not an inconsiderable feature of these weapons. They are key elements of perception manipulation – and have been used many times by many countries in this way.

Source: KCNA

This North Korean missile (above) is an intermediate range ballistic missile (IRBM) with a range of 1500 - 2400 miles. It could carry a high explosive or nuclear warhead to cover all of Japan and it could reach Guam, the site of a major American base. Note the complicated mechanical lifter braces of the TEL. Also, note the many cabinets on the side of the vehicle for carrying various supplies (e.g., the fireproof blankets and window covers to drape the truck).

The 1991 Gulf War marked a milestone in mobile missiles for the reason described earlier. But the development process behind the shift to mobile missiles had a longer history. Through the 1970s the success in the United States of laser guidance for precision strike was joined by terrain contour matching radar, which guided a

cruise missile to follow complex routes to a target, avoiding enemy radars. With these technologies cruise missiles, which, earlier in the Cold War, were useful only for nuclear missions, could now deliver accurate conventional warheads.

Later, GPS marked a big advance over terrain matching radar. With GPS guidance the time-consuming task of preparing contour maps was disposed of. This allowed cruise missile attacks and fighters to be much more agile. It also highlighted the importance of mobile missiles for every country in the world as a way to beat this U.S. capability. India, Pakistan, Israel, Russia, China, North Korea and others shifted their effort to these mobile missiles.

Another factor behind their spread in the 1990s and 2000s was the collapse of the Soviet Union. Russian engineers were looking to sell their know-how abroad. Moreover, Russia itself was so desperate for hard currency in the 1990s that it sold outright the special-purpose mobile launchers. China bought old Soviet SS-20 missile TELs to use for their rapidly growing missile buildup against Taiwan. These TELs had advanced features, including operator controls to automatically inflate/deflate tire pressure depending on what type of surface it was on.

The diffusion of TEL engineering knowledge allowed even technologically backward countries like North Korea to field mobile missiles. There were private agreements between Washington and Moscow not to sell these technologies. But the agreements were either ignored, bypassed, or violated outright in the turbulent conditions of Russia in the 1990s.

Some broad conclusions about how we got to the present condition of widely proliferated mobile missiles can be offered. First, looking

back over many decades, the process was dynamic. It illustrates a coevolution of reconnaissance improvement – like the ability to deliver very accurate strikes using GPS – against the desire of the adversary to hide its missiles in order to avoid getting struck. The clear answer was to go mobile.

Another conclusion was that the United States was late to recognize the larger significance of the shift to mobile missiles. The CIA focused on counting Chinese missiles deployed against Taiwan, and this they did very accurately. But when it came to the tactics of tracking China's missiles, little was done. Even less was done about the crisis management implications of mobile missiles, anywhere. The political shock of a country moving alert nuclear missiles around was completely ignored. This is still the case, broadly speaking, and this report may be one of the first to delve into these crisis management issues.

Another conclusion deals with command and control. Armies, navies, and air forces are expensive, difficult to build, and hard to operate. The only reliable way most countries could deliver a nuclear bomb to another country was with manned aircraft. Yet an air force is an especially complicated enterprise. They require training, support, maintenance, and complicated knowledge of logistics, electronics, and command and control.

Missile forces are much simpler than air forces. The missile itself is less complicated than a jet aircraft. But even more, once one knows how to build a missile, production can be scaled up quickly. This in a way is a "business school" concept too. What it means is that there are significant economies of scale. The 101st missile is a lot cheaper to get than the 100th. This scaling made missiles attractive especially

to the developing states of the second nuclear age because, compared to aircraft, there is relatively little maintenance needed for a missile. It is unlikely to be tested, and if it is, one doesn't expect to reuse the missile. With aircraft, one needs computerized maintenance manuals, trained people in everything from the engines to servicing the bomb carriages. Not so with missiles.

From a command and control perspective, things are a lot easier as well. A national leader has a much simpler problem than with an air force. There are clear channels of communication to deliver the "go" order for launch. With an air force, the comparable order needs to pass through layers of commanders -- the top general, the base commander, the wing commanders, etc. Fuel has to be at the ready. Spare parts are needed because otherwise the missions will abort. Finally, there are the pilots. They require a high level of training and are almost always in short supply.

The experience of Gamal Nasser in the 1967 Arab-Israeli war was an object lesson in how the complexity of an air force could overwhelm the leadership's ability to control it. The Israeli surprise strike on Nasser's air force destroyed the Egyptian air force on the ground in just a few hours. Yet Nasser was completely unaware of this. He had given orders to it to attack Israel and thought the order was carried out. He knew nothing about just how vulnerable this force was. And not until two days after it had been destroyed, did he learn of this.

The shift to mobile missiles in the 1990s and 2000s took place by those who acted on the information they had available to them at the time, and with the technology known to them. There was little appreciation of technological advances in cyber, drones, or hacking.

The belief was that mobile missiles were the survivable way to base a nuclear force, and that this would last for the indefinite future.

Problems of Mobile Missiles

The problems of mobile systems are issues related to their vulnerability to enemy tracking and attack.

Before going into the details of these problems in an individual case by case manner, it's useful to describe the key overall argument. We are not advancing the argument that mobile systems have many problems. This is true, as will be detailed, but it is obvious. It would describe any nuclear force at any time. Nor am I are arguing in this report that a technological breakthrough will somehow make mobile missiles vulnerable. Breakthroughs may well take place in radars that can see inside tunnels, or that penetrate forest cover, or that drone swarms can track these missiles. These advances may happen, but they are not the essential argument of this project either.

Rather, the argument made here is that mobile missiles have <u>always</u> had major problems, going back to the Cold War, and that they have not been solved. Indeed, these problems led the United States not to rely on mobile missiles for strategic deterrence. Mobile missiles now and in the future, then, face two substantial challenges:

the long- standing problems of mobile systems inherent in this basing mode and new, advanced reconnaissance technologies that exploit just these problems, and more, that these new search technologies can be pulled together – integrated -- using AI, deep learning, big data analytics and other tools.

It may be said that the first item on the list is historical. It goes back to the first nuclear age of the Cold War. The second item is a new

feature of the second nuclear age we are now in. Namely, technological advances have radically improved search capabilities. These include both reconnaissance technologies, and integrating software and data bases to fuse diverse sources of location information.

The synergy of the two factors leads to increased vulnerability of mobile missiles.[11] This development has long-term consequences for the arms race and crisis stability that need to be recognized and carefully analyzed.

Technological advances (factor b. above) are analyzed in the next section of this report. For present purposes, it is useful to underscore that a large number of countries have chosen land-based mobile missiles for their bedrock deterrence. Consequently, they will either have to change their nuclear force in some way to restore a level of deterrence they seek, or they will have to accept a lower level of deterrence. Both alternatives have significant tactical and strategic implications that are discussed in Chapters 10 and 11, respectively. The tactical implications of the alternatives necessitate a more thorough study of crisis management with mobile missiles. The strategic implications suggest possibilities for restraint and arms control, especially for major powers in dealing with secondary nuclear states.

The inherent problems of mobile systems are listed in the following table for convenience.

11 Synergy is the interaction of technologies or systems to produce a combined impact greater than the sum of their individual effects. A Cold War example of synergy was the reduction of atomic warhead size, improved inertial navigation, and nuclear propulsion. These independent technological developments led to the Polaris submarine and a sea-based SLBM deterrent force. New synergies in today's world will surely occur, and many will be software related.

Problems Associated with Mobile Systems

- Definitions of Mobility and Portability
- Geographic Restrictions and Constraints
- Command and Control
- High Cost of Operation and Maintenance
- Vulnerability to Area (Barrage) Attacks
- Soft Targets
- Security, Protection, and Guarding of Missiles and Warheads
- Insider Attacks
- Peacetime Attacks to Degrade Capability
- Outsized Alert Signature
- Accident and Safety Issues

Definitions of Mobility and Portability

The first problem with mobile missiles is the definition of mobility itself. In many circles and in the public mind, people think of mobile missiles in terms of the parade videos that are broadcast by Pakistan, North Korea, and China. These videos show trucks with missiles driving smoothly down broad highways at a steady rate of speed. Not shown are the trucks coming to a halt, deploying spades into the ground for stabilization of the vehicle, and elevation of their missiles into a vertical launch position.

Also not shown is the fitting of a nuclear warhead onto the missile. While this can be done before the missile is deployed from its peacetime storage site, this runs the risk of loss of control over the warhead if something goes wrong. Loss of communication, for example, with a "loaded" missile in the field could lead to catastrophe, such as accidental launch, theft of the warhead and missile, or the seizure of the missile and its warhead by terrorists or dissidents or by military factions who suddenly see an opportunity. For these reasons, nearly all countries who possess mobile missiles separate the warhead from the missile in peacetime.

In addition, many of the larger mobile missiles are difficult to move because of the complexity and road clearances they need. TELs must be as proportionately large as the missiles they carry. Some highways may be unable to bear the weight of the combined load. This is especially the case in third world countries. The idea that these missiles can freely drive over the highway system overlooks the fact that overpasses and highway width may not clear the missile trucks. All of this applies with greater emphasis for off-highway operation. Unless routes are scouted beforehand a TEL may get bogged down and stuck. In this case, it might be in the clear and easily spotted by a satellite or drone.

In many cases, a mobile missile force will require an associated force of construction engineers and demolition teams. The engineers are needed to pull mobile missiles out of a ditch or from being wedged into an overpass whose clearance wasn't checked. The demolition teams are needed to demolish overpasses and obstacles using explosives so the missile caravan can advance to its launch spot. What is missed in the parade pictures of mobile missiles is that that these missiles are being used under extremely controlled conditions.

Parade roads are thick, there's no atomic weapon on the missiles, and there's no flotilla of support trucks because the purpose of the exercise is to take nice photographs.

For many of the long-range missiles of greatest concern, it is not clear that "mobile" is the even best adjective to describe them. It would be better to say that they are "portable" or "relocatable." These behemoth missiles are large because they carry the fuel necessary to hit long-range targets. They have to move very slowly, and may be easily spotted for this reason.

Geographic Restrictions and Constraints

These requirements and reality constraints radically cut down on the operating geography of mobile missiles. So, to give the area of a country like North Korea or Pakistan is very misleading. Most of the national area would not be suitable. Unless advanced testing had taken place to test compressibility of the concrete for highways and off-road surfaces, large risks would be taken with mobile operations.

This background only begins to touch on the mobility environment for these missiles. The long-range mobile missiles of North Korea, India, Pakistan, China and other countries have to travel on highways to reach firing positions. This geographically constrains them to a much smaller land area. Physical obstacles like rivers, lakes, and coastal highways limit their maneuver space. So do mountains and overpasses.

A missile launcher may be able to climb a 40-degree road grade in theory, but not in practice. This could be for several reasons. It may never have been tested on a steep grade. Or key parts like the transmission in the truck may be worn from use or from poor

maintenance and no longer able to handle the grade.

Likewise, missiles might have to avoid some highway overpasses for reasons of clearance. This is both because the truck and launcher may get stuck -- and unable to fire. But it is also for operational reasons. While the missile force of a country and the atomic weapon guards may constitute an elite force, many of the truck drivers who operate the vehicles will not be. They are more likely to be low-end draftees. One often overlooked problem is that when a new, inexperienced crew is on duty they may simply be unfamiliar with local terrain and highways. There are manuals that specify clearance rates on bridges and overpasses but there are often mistakes in these data.

In the Cold War in Europe, the United States ran into this problem repeatedly with its mobile missiles. Moving them about was a big deal requiring extensive preparation, advanced scouting, and rigid plans that told drivers exactly where to go and when to turn. This is obvious with a moment's thought. A missile crew can't be told to follow highway direction signs because these may be out of date. Or they may be changed by vandals or enemy agents to sow confusion. In NATO, crews were given no discretion on route selection and turns. Even with this, there were unexpected developments. For example, a traffic accident could block a highway requiring the rerouting of the convoy. Headquarters worked out alternate routes as the missile crew waited for orders.

In today's world, GPS receivers and radios can be given to missile crews. But this still requires giving discretion to drivers and crew, and this is a big decision. It opens up another vulnerability. Jamming GPS or its counterpart systems in other countries could produce chaos inside of a mobile missile crew. Interfering with GPS signal

accuracy in local areas is a highly developed art form. Moreover, local force commanders may not be familiar with the area. They might get lost, and then might be required to travel on unplanned routes.

These considerations bind the force to headquarters for orders about where and when to move. As we will shortly argue, this drives up the intensity of two-way communications between the mobile force and headquarters.

An experienced crew should in advance go on field rides in order to check the local area and to measure load-bearing capacity of highways and clearances. But an inexperienced crew, or a new one that is ordered into action at the last minute may not have the opportunity to do this. Training standards for U.S. Army crews in Europe in the 1960s were very high compared to many of the forces manning third world missiles today. It is particularly risky in this situation because most missile forces today are small. The United States had over 7,000 nuclear weapons in Europe and if a few of these were incapacitated, it wouldn't matter. But if a country only has 20-100 missiles to begin with, there could be serious consequences.

One commonly sees on highways how outsized cargo is trucked to a location only along carefully prescribed routes at non-rush hour times. This planning helps. But it too is a source of intelligence. Certain routes may stand out because they are tested to suitability.

Off-road operation is even trickier to undertake. This is worth mentioning because some TELs are tracked rather than wheeled. In theory, this increases their off-road capability. But it also adds to the weight for on-road operation, and this can tear up a highway for other traffic. To go off road is to enter areas with high variance in

their load-bearing capacity (i.e., whether the dirt will turn to mud if it rains). This is likely to be a risky thing to delegate to junior officers.

Another characteristic of many of these constraints is that they present problems that cannot be solved in a short period of time. It's impossible to quickly reinforce the load-bearing capacity of an off-road surface (e.g., in a forest). It is also impossible to quickly change the grade of most roads. With time, new routes could be selected, and engineers could blast overpasses to remove them. But all of these actions would take a great deal of time, measured in days and weeks and perhaps months.

Yet another mobility constraint arises from visibility and exposure to enemy surveillance. It is probably not a good idea to select routes over long stretches of open highway easily monitored by satellites. Movement may be restricted to night time for reasons of operational security. This in itself makes movement difficult. Most stealthy nighttime military convoys require that headlights and other illumination be tuned off to minimize the chances of detection. But these lights may be needed to prevent collisions, especially if something goes wrong. More, routes would have to be selected by experts who understood the periods of satellite orbits and the resolution and features of their cameras. In an era of drones this becomes more difficult. At least satellite orbits are predictable; drone overflights are not. This further reduces the time and space that mobile missiles may use. It also makes centralized control more necessary. Junior officers in the field are unlikely to know of or understand enemy satellite or drone capabilities. Therefore, route selection must come from a headquarters that grasps these movements. This reliance on a headquarters for route selection also

is communication between a missile unit and the center. These communications may be a tip-off that dispersal is about to begin or that certain routes are more likely to be used than others.

One interesting development associated with this particular mobility constraint is worth mentioning here as it is likely to be quite evident in the future. Route selection may be used to intentionally signal another country that one is moving up the level of nuclear preparedness. This is especially relevant for the United States. Another country could select a route it knows would be detected by American satellites in order to send Washington a message that the risk of nuclear war is increasing. This was the strategy of South Africa in the 1980s. The idea was to "move" their six atomic bombs in such a way that the United States would be alerted to the existence of Pretoria's weapons. A case can be made that this esoteric signaling – moving nuclear weapons in a purposeful way to ensure detection by U.S. intelligence – is a central tactic in Israel's nuclear strategy.

The image of missile TELs driving freely around the countryside in Pakistan, North Korea, India, or Israel at 50 mph, hiding beneath underpasses to avoid satellite passes, and ducking into a forest for daytime cover against drones significantly mischaracterizes the realities of mobile missiles. By reducing the physical geography of where these missiles travel, it becomes easier to focus reconnaissance on this smaller space.

Command and Control

Mobile missiles require far more communications than fixed-base missiles. This is obvious, and it is one reason the United States didn't build mobile missiles in the Cold War for strategic missions. It

opens up potentially lethal vulnerabilities. Communications can be monitored. They can be analyzed for content and for subtle patterns even if the country in question may have little awareness that they are revealing.

Most basically, the "go" order, that is, the command to fire the missile needs to be sent to the crew. For a fixed missile like an ICBM, this is easy. Reliable, protected buried cables can be used to send these orders. Radios can offer backup. Most importantly, the sender of the "go" command knows where the missile is.

None of this applies to mobile missiles. First, it is much more likely that radio rather than cable has to be used for communications. And radio is much easier to listen in to than cable. It is true that advanced locations can be prepared where the missile might be sent, and they can have cable links set down ahead of time. But these could also be the very spots monitored by enemy intelligence. Watching the cable being laid would be a tip-off about wartime firing positions. Burying cable is easily monitored by intelligence services.

Radio links today are much improved over those in the Cold War. It has been suggested, for example, that dense cell phone or 5G networks could be used for command and control. They have a great deal of redundancy. However, it may also be necessary to turn some or all of these cellular systems "off" in a crisis or in a war. Otherwise, they may be tapped for insights into operations. Or they could be used for espionage. In recent crises in Kashmir and other places, these networks have been shut down.

Turning off part of the cell phone system would necessitate advance coordination between military and civilians to work out the details of what exactly gets turned off and what stays on. This would be difficult

to work out in the short period of an emergency if preplanned actions hadn't been undertaken beforehand. Turning off the total cell phone 5G system could paralyze the political command and control of the nation. While turning social media "off" may take place, turning everything off risks chaos and disorganization. It would also place an enormous demand on the plain old telephone system, landlines, which in most countries have been underbuilt.

The communications target of intelligence includes not only the missile itself, but the associated support crews and logistics needed for its operation. A fuel truck or a communications van, rather than the missile TEL itself, may offer the clue to a mobile missile's location.

In today's world, cell phones could be an especially important source of data about a mobile missile's location. There are 5 million cell phones in North Korea in 2019. Samsung, iPhone, and Nokia phones are widely used in North Korea. A government can order that its military not carry or use cell phones while on duty. And it can shut off the cell phone network in a region or in the entire country. But this is unlikely to happen. With young people in their teens and twenties the most likely demographic to work in missile support, there is a very good prospect that not everyone will heed the message to turn off their phones.

Another feature that has to be considered in command and control is that not everything will go according to plan. Deviations from plan generate a surge of communications as people consult back and forth to handle the problem. For illustration, a critical support truck may go off the road and require a wrecker to tow it out of a ditch. The hydraulic lift gears on the TEL elevation mechanism

may fail and require the attention of a technician. A location where support is supposed to be available may not have stocked the right parts. All of these will lead to sharp increases in communications with headquarters to sort out the problem. The situation in the field first has to be described to higher commanders. Requests for spare parts have to be sent. Technicians with the right skills need to be dispatched.

Such mundane tasks are how intelligence services exploit communications for insights. One of the great features of the fixed site ICBM was that most of support tasks could be undertaken in the familiar, protected environment of the missile base. Communications were over shielded underground cables. Most importantly, the number of deviations from normal procedure were low because these missiles didn't move. Its environment was fixed. There were no moving parts, so to speak, meaning no broken TELs, blown transmissions, broken axles, bad hydraulic lifters, or surprise road conditions.

One final consideration related to command and control needs to be recognized. It is unlikely that missile and TEL support crews will have physical control of the nuclear warheads. For the "new" nuclear weapon states, every country we know about separates the warhead from the missile. This is to prevent loss of control of the warheads or accidental use. The guardians of the warheads are usually made up of loyal, elite units who report through a separate command chain than the missile support crews. This was the case for the United States and the Soviet Union in the very early part of the Cold War. National leaders are fearful that they will lose control over these weapons. As a result, we should recognize that we are dealing with two command and control systems. One is for the missiles and their

support; the other is for the atomic warheads themselves.

This raises the issue of integration of the two systems. The warhead control crews have to be mobile, obviously. They have their own command channels that need to be synced with the missile's command and control if there is to be a launch. This whole process -- from warhead to missile launch -- increases communication levels. There are national variations, certainly, but there also are common problems of organization and communications affecting all nuclear weapon states.

High Cost of Operations and Maintenance

Mobile systems have far greater operating and maintenance costs than fixed systems. This is because moving parts wear out, and because the costs of a guard force, repair technicians, and communications are much greater. In the Cold War, such costs were burdens for the superpowers, and was one reason they chose not to go down this road.

What should be distinguished are costs in the narrow economic sense, and costs in terms of their impact on organizational performance. Call the first of these "direct" costs. They include payroll, fuel, spare parts, and vehicle wear and tear. Call the second "transaction costs." These would cover exercises, practice drills, and specialized crew training. Again, the direct and transaction costs apply to both missile systems, and to the atomic warhead crews.

The two kinds of costs have different implications. Other parts of the armed forces have to be underfunded in order to support the mobile missile force. The result is underinvestment in conventional forces, like the army and navy. One already sees this in many countries, like

North Korea, India, and Pakistan. The giant infantry forces of the post-colonial era are now used as cash cows for investment in new kinds of forces, the nuclear missiles.

It is the second type of costs that receives little attention in most descriptions of nuclear strategy. The result of higher transaction costs of mobile compared to fixed site missiles is to minimize them. This means cutting back on training and exercises that work out the bugs. If there are cutbacks, then the likelihood of glitches developing during a real crisis go up. The standard learning curve that is used in engineering, the S-shaped logistic curve, suggests that there is a very steep improvement in learning in the early practice exercises. If there are few such exercises, this learning never happens. When something goes wrong in a real crisis, there is a greater chance of paralysis or panic, and also, sharply increased levels of communications. This is because the missile units in the field do not know how to handle a problem. So, they send messages to headquarters to find out what they should do. What takes place is frequent back and forth communications as headquarters tries to understand the exact nature of the problem.

The other consequence of running into problems in the field is that it creates delays in the movement to "safe" positions, safe in the sense that there are resources there to handle crew and repair needs. This is the care and feeding of support troops, repair of damage to the TELs (flat tires, oil leaks). With such delays, and increased communications, a missile dispersal could turn into a disorganized mishmash. This possibility is decreased if the dispersal is rehearsed many times. But if this isn't done, a full-out dispersal of missiles and warheads may have many surprises. This is what took place in virtually every crisis of the Cold War, as later studies revealed -- and

this was with a largely fixed force of ICBMs, SLBMs, and bombers.

So, the real problem of high operating and maintenance costs is that realistic exercises will be cut back for budgetary reasons. The consequence is lowered performance. Delays, confusion, redo's and recalls to base -- all lead to a noisy dispersal. It is noisy in the sense that it has a large communications signature, with delays at locations extended beyond what plans call for.

Lowered performance occurs in all organizations when they attempt something new, when they don't practice. Imagine putting untrained sailors on an Aegis cruiser with a written rulebook manual describing what they should do. Accidents, confusion, and increased vulnerability to attack are the result. A nuclear crisis with mobile missiles might even become so disorganized that it leads to a judgment that war may be coming even if it isn't wanted by either side. One side decides that it had better get in the first blow to limit damage to itself.

Vulnerability to Area (Barrage) Attacks

Mobile missiles do not have to be precisely located in order to destroy them. They can be attacked with conventional weapons that are especially designed to destroy them if their location is only known imprecisely. Or they can be attacked with nuclear weapons with their greater lethal area.

Mobile systems, the missiles and the warheads, mounted in vehicles are not designed for combat like a tank or armored troop carrier. A cluster bomb is an air-dropped or ground-launched explosive weapon that ejects a smaller submunition called a bomblet. The purpose of a cluster bomb is to destroy people or vehicles over a wide area.

Cluster bombs today are widely available. They may contain 200 - 500 bomblets. Each of these is fused to explode above ground at an optimum height for damaging a particular target. Some of these cluster weapons have a large lethal radius for use against electrical power lines or airplanes distributed over an airfield. The blast from a single bomblet in a cluster weapon can spread lethal shrapnel over a circle of 350-foot radius.

A new development in this field is delivery of submunition bomblets and flechette warheads by placing them on hypersonic missiles. Hypersonic missiles will be discussed later as an activity in the value chain for hunting mobile missiles. Here it need only be noted that this is a new development with significant implications for destroying dispersed targets. A flechette is a pointed steel blade about one to two inches long with a finned tail. The idea behind this is to give the blades -- the flechettes – flight stability in order to increase the size of the kill zone.

When a missile's speed is above Mach 3-5, it imparts tremendous kinetic energy to the flechettes. This kinetic energy turns the flechettes into a super deadly weapon for destroying area targets. The tungsten blades can disintegrate an aircraft, vehicles, or buildings.

Finally, nuclear weapons may be used to attack mobile targets spread over an area where the location is not precisely known. Studies of nuclear blasts in the Cold War indicate that even very heavy trucks will turn over at 4-5 pounds per square inches of overpressure.[12] This is not a particularly large overpressure to generate with nuclear weapons. Strike plans may involve both conventional and nuclear

12 W.R. Elswick, "The Response of Hypothetical Missile Transport Equipment to Nuclear Blast," RAND Corporation, RM-2270, October 16, 1958.

attacks sequenced in various ways. Or they may include staged attacks, such as a conventional first strike to be followed up with bomb damage assessments for deciding on what to do next. If the locations of the surviving weapons were unknown, and there was a chance that they would be fired in retaliation, then nuclear barrage attacks could be employed.

Soft Targets

As indicated above mobile missiles are soft targets. If located, they are easy to kill. Missile containers on a TEL are designed only against rain and dust. The mobility requirement requires that any protective covers be light in order to minimize the size of the truck and the strength of shock absorbers needed.

Anti-personnel weapons of all kinds can make them inoperable. Rifle fire by snipers is a significant danger. A rifle bullet can easily penetrate the thin shield of a missile container as well as the missile itself. Firing a damaged missile could pose a very high risk to the crew because leaks may detonate the missile fuel. Word that a missile exploded at a launch point will get around to other missile crews very quickly.

Security, Protection, and Guarding of Missiles and Warheads

In the Cold War the United States discovered that it had to spend far more resources for protection of nuclear warheads and weapons than anyone had ever imagined. This was especially the case for U.S. nuclear weapons in Europe. The threat from protesters, enemy agents, and terrorists was so great, and the consequences if a nuclear warhead were seized so enormous, that extraordinary efforts were undertaken to make sure this never happened. Many experts who

studied the problem concluded that such an assault stood a good chance of success.[13]

Strict rules were imposed as to how and when nuclear weapons could be moved from one place to another, both inside the United States and overseas. Before the 1970s, nuclear missile and warhead movements were generally done using guarded truck convoys. In the 1970s, helicopter movement of warheads was mandated. One reason for this was that historical data suggested that road accidents would halt the convoy movements, often in remote unprotected areas. These were prime areas to stage an ambush attack on the convoy. Moreover, the time on the road was far greater than with helicopter movements.

The weakest link in the safety and protection of U.S. nuclear weapons wasn't the vehicle selected to move the device, however. It was the quality and training of the guard force. Nearly all studies showed that guarding nuclear warheads was a low status job, one with little possibility for career advancement. It was a boring, mind-numbing task because nothing ever happened, and the daily routine was monotonous. As a result, the quality of the guard force was extremely difficult to maintain. There was high turnover. Drug and alcohol abuse and lowered standards were constant problems. This problem was resolved by requiring a large number of officers to monitor the guard force and to assure that the rules were closely followed. This added to costs, however, and, more important, it required a large number of communications among the officers

13 Frank E. Armbruster, John Thomas, Herman Kahn, and Paul Bracken, *The Physical Security of Nuclear Weapons, 1945-1977*, Hudson Institute, September 1977.

monitoring the guard force.

This is an endemic problem, one that crosses national borders. No country is unique, and the problem hasn't disappeared by any means. Reports that U.S. short-range nuclear weapons are still deployed in five European countries (Belgium, Germany, Italy, The Netherlands, and Turkey) have raised a great deal of concern about security for the reasons described. There are many specific examples of problems in this area. Only two will be mentioned here, but these two are interesting because they took place in democratic countries. Both were adjudged "unlikely" before they occurred.

Even democracies can get into bizarre, unanticipated situations when it comes to institutional arrangements for protecting and moving nuclear weapons. In 1961, for example, a coup by French generals in Algeria against the French president, Charles de Gaulle, led to his ordering the hasty early detonation of a French nuclear weapon at a test site in the field in the Sahara Desert. This firing of the bomb was ordered by de Gaulle to prevent it from falling into the hands of the plotting generals. In addition, it showed that the rebel officers did not control all of Algeria as they had claimed.[14] 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 developments with nuclear weapons in the field.

Another example comes from Turkey at the present time. According to media reports the U.S. air base at Incirlik, Turkey is authorized to store nuclear weapons as part of its NATO mission. The attempted

14 "France Explodes Nuclear Bomb At Sahara Test Site in Algeria," *New York Times*, April 25, 1961, p. 1.

coup in Turkey in 2016, and the proximity of Incirlik, located near the border with Syria, has raised many alarms about the security of nuclear weapons there. There are many ISIS-related groups in the area. One detailed study of the problem adds that the general confusion of command and control within Turkey as it goes through political changes, and the arrest of thousands of Turkish officers for supporting the coup attempt, should increase concern about the safety of these weapons.[15]

In both of these cases the concern is with emergency exfiltration of one or a small number of bombs. But with mobile missiles, we are talking about frequent movement around the country, something that could involve scores of warheads for a small nuclear power, and hundreds or more for a major one. Most of the cases of interest now are about non-democracies where there looks to be a serious risk of military factionalism and coups.

Another consequence of guard force management difficulties is that, historically speaking, when accidents did occur they tended not to be reported up the chain of command to higher authorities. The study conducted by the Hudson Institute in 1977 found that the more serious the accident, the less likely it was to be reported to headquarters. The reason was simple: it would constitute a black mark on the record of the officers responsible for managing the force. It's Organization Theory 101. This is one reason most companies make quality control managers report directly to senior executives. If they reported to someone who directly controlled their salary

15 See Can Kasapoğlu, "Turkey and Nuclear Command, Control, and Communications," NAPSNet Special Reports, June 27, 2019; https://nautilus.org/napsnet/napsnet-specia--reports/turkey-and-nuclear-command-control-and-communications

and promotion, there would be systematic underreporting. Every business school teaches this lesson in introductory courses.

New nuclear states will likely have much lower standards for safety and protection (i.e., quality control) than the United States had in the 1970s. Tolerance of risky behavior, accidents, and personal reliability issues are endemic in the new nuclear weapon states.

To add to the difficulties today, social media and cell phone use are likely to be major problems for a guard force. Indeed, there have been many proposals to use social media for arms control verification purposes for just this reason. This means calling on elements of a population to report over social media suspect activities related to nuclear weapons.[16] However useful this may or may not be, it shows that social media could be used for spying as well. It could, for example, offer a way for political groups opposed to war to oppose military preparations of the state. Something close to this happened in 2003 in the revelations by groups inside Iran, and opposed to its current regime, revealing nuclear activity at Fordow. This revelation tipped off the world media about Iran's activities, and drew intense scrutiny of western intelligence.

Again, it may be simple to declare that no social media or cell phones may be used by missile crews while on duty. Or that social media would be shut down in a war or crisis. But it is altogether a different matter to enforce this order. It should be remembered that a cell phone, for these purposes, is in essence a radio beacon. If the individual with the phone is assigned as the driver of a missile

16 This discussion draws upon *Social Media Storms and Nuclear Early Warning Systems, A Deep Dive and Speed Scenarios Workshop,* Nautilus Institute Preventive Defense Project, Stanford University, January 8, 2019.

convoy or carrying technicians to repair a dispersed missile, it could be a dead giveaway as to where that missile is.

Social media can be closed down by government. Indeed, this seems to be an growing response in a national crisis. Social media was closed down after bombings in Sri Lanka in April 2019, for example, and by India in Kashmir in August 2019. But there are many ways around this. Intelligence services, NGOs, and journalists have perfected ways to circumvent most of the obstacles.

Insider Attacks

That mobile missiles are soft military targets and require large amounts of communications to operate makes them especially vulnerable to insider attack by spies, saboteurs, and commandos. Agents may be deployed in sleeper cells, and activated in a crisis. Another insider attack threat arises from agents infiltrated into the lower levels of the transport and guard units. These are not likely to be elite units because they are really glorified motor pools. Guards for convoys are likely to have even lower status and rank.

It is, frankly speaking, difficult to imagine that mobile missiles will not be tracked in a nuclear weapon state by enemy agents. It happened in the Cold War, both for nuclear weapons in Europe and it happened in the United States. Soviets agents watched the Strategic Air Command. This arises for many reasons. Early warning, unusual military activity, new weapons, communication and staffing patterns -- all give tip-offs of what the enemy is up to. Small things, like gate closures, canceled leaves, officers converging on a particular area, and parking lots filling up are useful intelligence indicators.

They can reveal missile locations, increased readiness, and preparation for unit moves. Today, agents could also be supplied with flash drives to inject disruptive malware into a system. The shortage of trained personnel in many nuclear weapon states means that if someone shows up with needed skills, they're likely to be assigned straightaway to a unit.

In the Cold War there were instances of spies emplaced close to the enemy command and control apparatus. The names Oleg Penkovsky and Oleg Gordievsky have become part of Cold War legend. Both were involved in extremely sensitive nuclear operations. Penkovsky described Soviet military preparations during the 1962 Cuban missile crisis.[17] His reports went directly to the Pentagon and the White House. Gordievsky reported to the British MI6 on Soviet reactions to the 1983 Able Archer NATO nuclear missile exercise.[18]

Neither Penkovsky or Gordievsky worked directly in operational units. They could not disrupt or sabotage military preparations. Nor could they interfere with military alerts. But something akin to this did occur in the Cold War. In 1975 Christopher Boyce and Andrew Lee, two people in their early twenties working for TRW Space Systems Group in Redondo Beach, California decided to approach the Soviet Union. They worked in a very sensitive operation dealing with U.S. reconnaissance satellites. The CIA and Air Force had earlier outsourced this task to TRW in a cost-saving move. Boyce

17 Len Scott, "Espionage and the Cold War: Oleg Penkovsky and the Cuban Missile Crisis," *Intelligence and National Security* 14:3 (1999), pp. 23-47.

18 For an assessment of the 1983 nuclear war scare, see Benjamin B. Fisher, *A Cold War Conundrum: The 1983 Soviet War Scare*, CIA Report; also Marc Ambinder, *The Brink: President Reagan and the Nuclear War Scare of 1983* (New York: Simon and Schuster, 2018).

and Lee's assignment was espionage, to tell the KGB exactly what U.S. satellites could do, and how they were managed.[19] Later, Ronald Pelton, an NSA employee revealed key operational aspects of a top secret Navy/NSA tapping of undersea Soviet military cables in the early 1980s.[20] In both of these cases had the technology of flash drives existed, it isn't hard to imagine that the individuals could have caused massive upset to operations from the inside.

It is useful to summarize the lessons of these cases, and to go beyond the details of particularities of the Cold War. There are four useful insights that emerge:

All of the cases involved nuclear reconnaissance -- i.e., military observation of enemy nuclear operations;

Some involved (Boyce and Lee) penetration of commercial enterprises with sensitive responsibilities;

All of the above cases involved only a single "information chain," using the term as it was defined earlier. Penkovsky focused on Soviet alerting and readiness, Pelton on undersea cable collection, Boyce and Lee on intelligence satellites;

The cases showed a range of common motivations on the part of the insiders: ideology, financial gain, thrill seeking.

Today, the potential damage from insider attack is on an far greater scale than anything possible in the Cold War. Compare the revelations of Edward Snowden to those of the above cases.

19 Their story is the basis for the 1979 book by Robert Lindsey, *The Falcon and the Snowman, A True Story of Friendship and Espionage*, and a movie of the same title.
20 See W. Craig Reed, *Red November: Inside the Secret U.S.–Soviet Submarine War* (New York: William Morrow & Company, 2010).

For one thing, Snowden's revelations covered many information chains: penetration of commercial support organizations, intercepts, communications systems, social media, undersea fiber optic lines, and computer hacking, to name just some. The breadth of the take is staggering, and it is likely a precursor of where the intelligence services of many countries are going. It is also worth noting that some of the Cold War lessons still apply, however. Snowden was employed by a contractor support organization, SAIC. It had far fewer security controls that the organizations it supported. And like earlier insiders, Snowden himself seemed to be motivated by ideology, more than financial gain or thrill seeking.

Digital systems widen the scope of intelligence operations to go far beyond the espionage of Cold War cases. Like the corporate world, the sheer size of IT staffs in military organizations is growing exponentially in size. There are huge shortages of IT personnel. This offers an open door to foreign penetration because the military needs people desperately. Turncoat citizens lured by a range of motivation create substantial opportunity for penetration, not only in the United States, but in every nuclear weapon state. Indeed, the controls against insider threats would be far lower in other countries than in the United States.

The sophistication and scale of insider attacks will increase. Insider access makes it easier to implant new disruptive technologies using AI and deep learning inside the enemy nuclear command and control system. It defies belief that intelligence services around the world would not take advantage of these new opportunities to position themselves inside the enemy system. Quite unlike the Cold War, where espionage was the main use of insiders like Penkovsky and Gordievsky, disruption of missile operations, misdirected orders, and

viral cyber attacks could paralyze a force.

Peacetime Attacks to Degrade Capabilities

Given the soft character of the targets, uneven guard protection, and insiders, partial attacks on an enemy missile force in peacetime could be used to reduce the striking power of a nuclear force. Attacks could be disguised to look like terrorist strikes unrelated to any foreign power's plan. Attacks could be against missiles, warheads, unloaded TELs, spare parts for the missile vehicles, or against computer systems that store routes and plans. These attacks could be quite sophisticated. For example, they could be a slow motion, stealthy, disruption of individual parts of the system to conceal the larger purpose of the campaign.

Moreover, for ease of protection, countries may concentrate missiles and warheads into a very small number of peacetime bases. This is what the United States did at the outset of World War II. In December 1941, at Pearl Harbor U.S. commanders economized on their limited protection and guard forces by having as few sites as possible. That way the guard force would not be distributed over large disconnected areas. Japanese intelligence in Hawaii carefully noted this tactic in the months beforehand. When war came, it had the effect of "bunching" allied aircraft into lucrative, easy to kill targets.

Terrorists attacks in Pakistan are almost routine today. If an attack destroyed only 10 - 20 percent of the warheads, it would greatly facilitate a first strike on Pakistan. The attack might only involve 1-2 targets, such as storage bases for nuclear missiles and warheads. A peacetime attack might be dismissed as a "terrorist action" -- yet it could mask a more serious impending preparation for war.

Outsized Alert Signature

A feature in the Cold War that dampened crises was the introduction of ICBMs and SLBMs in the 1960s. Fixed-base ICBMs and SLBMs at sea were "always on," so to speak. They did not have to be dispersed or otherwise alerted and they could be fired on short notice. The time to launch was in minutes, not hours. Bombers did not have this feature. They required topping off the fuel, arming, and crewing because most of the time the bombers were sitting empty on a runway.

As a result of this difference between missiles and bombers, there were distinct changes in the alerting signatures of the two big nuclear powers. It is useful to note that all of the serious crises of the Cold War occurred before the early 1960s, when strategic and tactical bombers had to be prepared for nuclear launch. Most fictional books and movies on accidental war were based on bomber alerts that had gone awry.

The reason for pointing this out is that there are beneficial features to a deterrent which is "always on." A deterrent which does not have to be thrown into high gear avoids the possibility of provoking an overreaction by an opponent. This dynamic precipitated the spiraling escalation of August 1914 that led to World War I. In fact, the summer of 1914 became an archetype of the nuclear age. It was specifically mentioned by President Kennedy prior to the Cuban missile crisis, a president who actually read a key book on the subject.[21] Academics have attempted to debunk Tuchman's description, and to argue that it doesn't apply to the nuclear age. I think this misses the point.

21 Namely, Barbara Tuchman, *The Guns of August, the Outbreak of World War I* (New York: Macmillan, 1962).

"1914" is an archetype of nuclear catastrophe, a universal pattern that originates in the collective unconscious fears of humanity. It will surely remain so into the foreseeable future.

This is the reason nuclear alerts are so interesting. Nuclear war as something that could actually happen is dismissed from our consciousness on a day to day basis. There are times when it comes to the surface, however. The Cuban missile crisis. The early 1980s when President Reagan was calling for a more assertive U.S. nuclear posture. But it's not right to interpret these times as strategic efforts. Because people also understood that things can go wrong with big complex technical systems. It is one reason that the focus of research in the early 1980s shifted from nuclear strategy – the calculated policy of targeting and alerting – to the complexities of nuclear management.[22] Alerts raised the readiness of a force for actual use. But more, they brought the terror of nuclear devastation from the unconscious to something real and present for the world.

Most countries would like to keep this terror buried below the surface. This is especially true in the West. In the 2000s, when Britain was planning the future of its nuclear deterrent, this "always on" feature was a goal of the review. The idea was that the deterrent should be kept in the background as much as possible. There should be no necessity for decisions to raise the alert level by dispersing or launching aircraft or fitting warheads on missiles.[23] It led the British

22 Including the present author, *The Command and Control of Nuclear Forces* (New Haven: Yale University Press, 1983).

23 This conclusion is based on discussions I had with British nuclear planners in London while serving on a U.S. Navy advisory panel at the time. It is also included in the official White Paper put out in 2006, *The Future of the United Kingdom's Nuclear Deterrent*, U.K. Ministry of Defence and Foreign and Commonwealth Office, December 2006.

to rely exclusively on the Vanguard submarine force for deterrence, and to abandon other kinds of nuclear weapons. There were strong memories at this time of large crowds blocking U.S. nuclear missiles deployed in Britain in the 1980s by anti-nuclear groups. Moreover, and privately, British planners wanted to avoid the panic and dread associated with high profile nuclear alerts of the 1950s and 1960s when the British force was based on Canberra bombers and other systems that needed to be placed on alert before they could be used.

Mobile missiles have to be dispersed to be effective, and this creates an outsized alert signature. In this respect they are like nuclear bombers in the Cold War because, if they are not dispersed, they are sitting ducks offering a high value target -- a bunched set of nuclear missiles easily destroyed with conventional or nuclear weapons. But, if they are dispersed, they might provoke war fears in the enemy, and lead to preemptive attack. In other words, switching "on" these weapons could trigger the attack they were built to deter.

The danger of alerts arises because of the large signature of mobile weapons. Moving them will generate multiple signals in the enemy radar, communications intelligence, imagery, and spy network. Today, there is another dimension that must be added to this list. Were a country to alert its nuclear forces by dispersing its mobile missiles, a social media storm is likely to follow, as discussed earlier. The dispersal will be reported by news outlets around the world. it will also be reported by millions of people with cell phones. We would see pictures of support vehicles rushing to support the dispersal, phone reports that someone's son was called up for service, road closures that block traffic arteries, closure of military bases, or increased guard forces deployed to key locations.

There are several issues associated with the outsized alert signature of mobile missiles that should be distinguished. First, it is a source for intelligence for the enemy. The information may be pieced together and combined with other data to locate the missiles. Second, the outsized alert signature enlarges the drama of the crisis, and, politically speaking, this becomes part of the political strategy for "using" nuclear weapons. Because one of the key lessons is that you don't have to fire a nuclear weapon to use it.

There is a third element to all of this which needs to be included. A country may choose to go on alert, or partial alert, for signaling purposes. Such "noisy alerts" using mobile missiles is akin to the United States launching nuclear bombers to their airborne holding positions in the Cold War. One part of the bomber force was put into the air. The other part of the bomber force was dispersed to alternate civilian airfields and stood on ready alert, prepared to go on short notice. This is what created the drama and feeling of danger that was used during the Cuban missile crisis between Washington and Moscow. It was used again in 1973 during the Yom Kippur war by the United States to signal the Soviet Union that it would not tolerate Moscow's intervention into that conflict. One could add here that it was used by Israel as well, when their nuclear weapon movements were staged to be seen by U.S. satellites.

Accidents and Safety

Nuclear weapons greatly increase the peacetime safety problem. Today, this is further intensified by the shift from atomic to hydrogen weapons in several countries. An accident of a low yield atomic bomb at a test site in North Korea is one thing. But an accidental detonation of a hydrogen bomb is on an altogether different scale.

The debris tossed into the atmosphere would be vastly greater than with the atomic weapons. It would poison South Korea, Japan, and the United States.

The other reason for concern here is the shift to mobility for nuclear weapons. The earliest nuclear weapons of the superpowers in the Cold War were designed by scientists. The 1950s and 1960s saw the transfer of this scientific device to the military. Bombs had to be hardened against the shocks of movement, acceleration, and fire. These weapons further had to be made to work in harsh conditions of cold and heat, humidity, and lightning storms.

Frequent handling of nuclear weapons raises the possibility of accidental detonation. When the handling is done by untrained personnel, the problems will be all that much greater. These weapons all contain high explosives that are needed to trigger nuclear ignition. U.S. and Russian weapons have been designed to minimize the chance of nuclear detonations using precision engineering, and safety checks. For example, all U.S. nuclear weapons need to go through a prescribed acceleration profile before they can be armed.

It is unlikely that North Korean or Pakistani weapons have anything like these safeguards built into them. If they contain some of them, it is unlikely that they have anything approaching the degree of protection that have come to be standard in the United States. In short, the margin of safety of many new nuclear weapon state weapons is likely to be considerably lower than what was developed by both superpowers in the Cold War.

The added problem here is that the basing posture for these weapons is mobile. This means frequent handling by crews and repeated shocks. Forklifts, dollies, and wooden pallets are commonly used.

This frequent handling exposes the bombs to accidents, strains, and deformations. Temperature and humidity conditions may affect the weapon by seeping into the fusing and "safe-ing" mechanisms of the bombs. This is all quite different from the nearly sealed off mechanical and environmental conditions of Cold War deterrents.

For all of these reasons the United States chose not to rely on mobile missiles on land for nuclear deterrence in the Cold War.[24] One could even go further than this. In the 1960s there were expectations that the United would build a mobile medium-range ballistic missiles (MMRBMs) for deployment in NATO, and possibly in Asia against China. At this time Moscow had over 500 MRBMs aimed at NATO, and China had gone nuclear in 1964. However, for the reasons discussed above, the Pentagon decided not to go ahead with a planned MMRBM. It was not just that the problems were severe enough to move away from mobile missiles in the United States, but even in Europe.[25]

24 Stephen A. Pomeroy, *An Untaken Road: Strategy, Technology, and the Hidden History of America's Mobile ICBMs* (Annapolis, MD: Naval Institute Press, 2016).

25 Twenty years later in the 1980s the United States did field mobile missiles in NATO Europe. These were the ground launched cruise missile (GLCM) and the Pershing II missile.

In the 1990s, when the global shift to mobile missiles began, technology had changed. "Accuracy," in the sense defined earlier had greatly improved. But "search" had not. Search for fixed targets had certainly improved, but not for mobile targets. Few people in the 1990s saw where reconnaissance technology was going in this respect.[26]

26 An interesting assessment of the contest between mobile missiles and reconnaissance technology to locate them in the late 1990s, given reasonable technology projections of that time is found in *Aerospace Operations Against Elusive Ground Targets*, (Santa Monica, CA: RAND Corporation, 2000), Report MR-1398.

PART III

ADVANCED TECHNOLOGIES

Advanced Technology and the Hunt for Mobile Missiles

Digital technology has remade the American economy and transformed the world of business. Going digital will have the same impact on national security and international order. In particular, technology will play a central role in finding mobile missiles, and it will do so in ways that are very different than merely improving the reconnaissance technologies of the Cold War. In other words, it won't be all about better satellites and faster computers.

It is easy to get lost in the details of the many new advanced technologies: drones, cyber, AI, space and ASAT, deep learning. These will be important, but focusing on individual technologies keeps our attention down in the weeds. It misses the remake of war and business that is taking place. The fundamental argument of this report is that our focus should be on packages of technologies. There is no claim made here that some advanced technology, like Super AI or satellites with radar that can "see" into tunnels and below ground, can find enemy missile locations. These developments are possible, however unlikely.

To apply this thinking to locating mobile missiles, advanced technologies exploit the vulnerabilities of these systems. The combination of these two factors -- inherent vulnerability and advanced technologies to exploit them -- makes the hunt for mobile missiles faster, cheaper, and better.

The advanced technologies relevant here are of many kinds. Importantly, they use different phenomenology. Therefore, it is not just one technology that delivers the benefit. Drones, satellites, cell phone and security camera hacks, etc. -- in combination -- have a synergistic effect. They are better operated together than used separately.

This is actually a fairly deep point. The import of this last point -- that "operated together" makes the difference -- is a key dimension of what is going to be a stepped-up arms race. It is here that AI and related technologies like data analytics and deep learning are so critical. Broadly speaking, there are two different classes of technology at play in the hunt for mobile missiles. One collects information about missile location: think here of drone video, satellite pictures, cell phone and security camera hacks. In this report, these are called "touchpoints." The second kind of technology integrates the data streams of these touchpoints into a common operational picture. Here, think AI, deep learning, and data analytics.

In looking at the future, there can be a tendency to claim too much for technology. But I believe the opposite tendency is more likely. Analyses of national security in academia and think tanks tends to underestimate the far-reaching effects and speed of technological change.

Two examples show this bias. No one in any U.S. government agency

or think tank imagined how quickly North Korea could field long-range missiles that could reach the United States with hydrogen bombs. North Korea proceeded much faster in both missiles and atomic weapons than anyone thought possible. There were all kinds of reasons offered as to why this could never happen.[27] But it did, and with far-reaching consequences. North Korea today is a nuclear weapon state, and shows little interest in disarmament. More, the fact of its nuclear capability has altered the political security system of East Asia, with wide-ranging implications for other major powers.[28]

The second example is the United States underestimating China's rise in 5G telecommunications. The implications of relying on Chinese companies, Huawei and ZTE, for most of the world's 5G roll-out were unforeseen and not taken seriously as recently as 2016. In the academic field of security studies, it was completely missed. In the Pentagon it was seen by a handful of experts, but their concerns were ignored while attention focused on buying F-35s and ships. Before 2016, 5G was not seen as a national security issue at all. Hence, it was overlooked by most defense and intelligence agencies, think tanks, and academic centers dealing with security.

Another broad aspect of digital transformation that is an especially important factor is the rate of progress in advanced technologies. The locus of defense innovation has changed from government research, centered on DoD and its affiliates, to commercial businesses. Commercial innovation cycles are much shorter

27 An interesting historical parallel exists with the Soviet and French bomb programs, and with China's hydrogen bomb program in the 1960s. In these cases, the rate of progress was seriously underestimated by the U.S. Government.

28 See Paul Bracken, "Asia's 'Pentapolar' Nuclear System," *Global Asia*, Vol. 11, no. 3, Fall 2016.

than government-backed innovations. Every few years there is a large shift of technologies. The clearest example of this is in telecommunications, something of direct relevance to the topics of interest here since these networks are the fundamental carriers of nuclear command and control. The shift from 3G to 4G took only five years. The innovation cycle of DoD, on the other hand, runs from ten to twenty years. The government's longer innovation cycle has colored how think tanks and the academy view technology in defense because they rely on data from government. These security studies centers have little contact with modern business, or even with business schools. More, virtually all of them have moved inside the Washington beltway to get closer to their customers.[29]

In academia it is striking, especially, how grand strategy programs at major universities are isolated from industry. Nor have any of them had any intellectual contact with business schools, even on their own campus. Such contacts would have made academic security studies realize that technology has remade the major institution of world society, the corporation. Given this, it would be surprising if it didn't have a large impact on national security institutions as well.

For these reasons there has been a tendency in the United States to underestimate the impact and pace of technological change. It has led to underestimating how quickly North Korea could produce H-bomb ICBMs, and how serious the threat is from backdoor "tunnels" built into telecommunications that in many cases directly support America's high tech arsenal, conventional and nuclear.

29 An exception is the Foreign Policy Research Institute in Philadelphia.

It should be noted that the large number of new technologies has made it difficult to grasp the impact that they are having. Should an agency focus on drones? Or should it focus on cyberwar? Perhaps AI should be the major concern. But specialization on any one of these obscures what is taking place in the others.

There are a number of books about each of these technologies, about cyber and drone warfare. Yet the challenge facing a senior decision maker and their staffs in defense is to understand the combined impact of both of these. This is similar to problem facing senior executives in business. They face the challenge of deciding which products to develop, how fast, and how to align the new systems with overall corporate strategy.

Blockbuster advances in business combine several technologies. Apple, Google, Facebook, Uber, and Amazon demonstrate this. Uber is a good example of this. It offers a ride-sharing service built on close integration of three technologies: 1) cell phones for communications; 2) a payment system (credit card, PayPal); and 3) a GPS direction-finding program. The three systems are integrated into a seamless package. The result is synergy – and a disruptive new business model.

The lesson to be drawn is the need to look at packages of technologies, to include their organization, integration, and synergy. In the following section, value chains and other business frameworks are used to describe these packages. First, the individual component technologies to the packages need to be identified. To do this, we will use a management concept widely used in business: touchpoints.

"Touchpoints"

Touchpoints are any interaction between a customer and a product. They are widely used in business in marketing and strategy. Touchpoint frameworks are taught in every business school. Touchpoint strategies can get quite complicated. But the basics are really quite simple.

While touchpoints have long existed – Pepsi advertising on TV or on a store sign in order to sell soda – new technologies like social media, streaming video, iPhones, and video games have revolutionized touchpoints.

A touchpoint is any way a customer interacts with a product, service, or company.[30] It may be a person-to-person contact in a store, as when a clerk approaches someone to ask if they need help. Or it could be a customer visit to a company's web site. A downloaded app is another touchpoint. It gives the customer information about an upcoming sale, or offer details about the product. An advertising display is another touchpoint. The display may be activated by the customer's mobile phone to deliver a targeted, personal message as she walks by a particular display.

The idea behind touchpoint strategy is to identify all the touchpoints a customer has with the company, and to create a strategy that

30 For good introductions, see Aparna Sundar, *Brand Touchpoints* (Nova Science Publications, 2018); Chris Risdon and Patrick Quattlebaum, et al., *Orchestrating Experiences: Collaborative Design for Complexity* (Rosenfield Media, 2018); and Jerry Wind and Catharine Findiesen Hays, *Beyond Advertising: Creating Value Through All Customer Touchpoints* (Wiley, 2016).

shapes this interaction in different ways aligned with the goals of the company. What comes out of this assessment is that there are a lot more touchpoints than anyone imagines. Many of them are unexploited or overlooked. Another interesting finding is that companies often fell into the trap of specialized marketing expertise, absent the recognition that there were interactions between the contact points in shaping customer attitudes. For example, a consumer product company might divide its marketing department by channel: TV ads, radio, billboards, product placement, print, etc. The specialists didn't talk to each other, and the customer was hit with uncoordinated messages from many sides. This was the pattern for decades. Touchpoint frameworks were developed as a way for a more integrated approach, one that focused the entire resources of the firm.

In business, highly defined touchpoint strategies have become central to the way a corporation interacts with its customers. In the process it led the way to one of the most important changes in business in the last twenty years. It shifted the firm's focus from a "product" focus to a "customer" focus. This was a fundamental change. It is now taking place in everything from retail and finance to health care and consumer products.

One reason behind this change is that companies now have large data sets because of the new digital technologies. In the past, it wasn't possible to "connect" with customers as deeply or as broadly because data about them was costly, slow, and difficult to collect. High touch strategies weren't possible in the pre-digital era. The parallels in national security should be obvious.

In practical, applied terms, touchpoints can be organized to

orchestrate customer behavior over time. Pepsi, for example, uses the many touchpoints it has with its customers (TV advertising, store displays, social media, event sponsorship, vending machines, contests) to shape customer receptivity to its Aquafina water in a can. The reason behind this is Pepsi's desire to reduce the number of plastic bottles that overload the environment with non-degradable containers. Cans are more recyclable, and environmentally acceptable. This notion of orchestrating customer behavior over time will be an important strategy in tracking mobile missiles, specifically to shape the behavior of the targeted force in various ways.

Studies show that there are definite patterns in the touchpoints. For example, offering a coupon for a discount to a customer to buy a product is a widely used technique to drive sales. This can be done by mailing coupons to the customer. This is the old fashioned way. Now, the customer can download electronic coupons from a web site. Another new way is to provide the customer with a phone app. When she enters a store and walks down an aisle that sells, for example, toothpaste her phone is pinged by a Bluetooth beacon. This triggers the phone to send an ID to the vendor who looks it up in a database in the cloud. From past sales history of this customer a tailored discount coupon is automatically sent to the phone. The customer doesn't have to do anything. They don't have to remember to bring a coupon, and more, they may not even be looking to buy toothpaste.

Studies show this to be a better touchpoint, better in the sense of the probability of generating a sale. When a customer is in the store, and walking past the toothpaste aisle, seeing a coupon for 30 percent off has a higher hit rate than receiving a coupon with other junk mail on a weekday afternoon. This is the sort of finding that is transforming

retail around the world.

For our purposes the mobile missile is "the customer." There are many interactions this "customer" can have with a foreign intelligence service (i.e., the "company"). The company can take photographs from a satellite of the missile. This touchpoint has a certain latency, that is, it may be hours or days out of date, depending on the details of the satellite system and the processing time. The missile may no longer be in the same location.

Another touchpoint could be a spy snapping a picture of the missile with GPS coordinates, and automatically uploading it to a Cloud data base. Still another touchpoint could be between an enlistee on the missile crew and a cell phone hack of his phone. The enlistee might be unaware that a covert app was installed on his phone. It might have been downloaded under the guise of some other purpose. Or the enlistee could be working for the foreign intelligence service itself.

With a touchpoint framework one begins to see just how many contacts there are between the customer (a missile) and the finder (an intelligence service). If we imagine a mobile missile moving about a country on military exercises, we can see how a very large number of touchpoints could be exploited. The figure below offers an example of advanced technologies and touchpoints.

Mobile Missile Touchpoints Using Advanced Technology

Each touchpoint circle in the figure is an information source. However, there are actually many more touchpoints coming from closely associated activities. There are support crews, supply trucks, warhead teams with their own crew and supplies, and headquarters command and control units in contact with all of these. In other words, it is not necessarily the mobile missile itself that is the source of detection. It could be some other element that is highly correlated with the missile in terms of geographic proximity, or in terms of some other tip-off as to its location.

Before discussing the technologies used to collect information from the various touchpoints it is worth making some additional general points about this approach. There are twenty touchpoints in the diagram. Only four of these existed in the Cold War. These are the unshaded circles in the graphic on the next page.

Missile Touchpoints in the Cold War (Unshaded Circles)

Satellite pictures and intercepts were the principal touchpoints relied on in the Cold War to track missiles. In the Cuban missile crisis, the United States tracked Soviet communications, took overhead pictures with the U-2 aircraft, had spy information (Penkovsky), and tailed Soviet ships as they approached Cuba. This produced a data flow, but it was episodic, random, and not really institutionalized into systematic intelligence products. It was also frequently out of date. That is, the latency between events in the field, and reports to headquarters was considerable. Even the overhead photographs were 24-48 hours out of date during the Cuban crisis.

A revolution in technology has brought new and entirely different kinds of data into use, data that simply did not exist in the Cold War. The institutions to collect, process, and distribute this information are starting to be built. Each major power tailors this to their

national needs. The process is still early, as it takes many years to build these processes and organizations.

The major powers are in a position like the early Cold War when high altitude aircraft like the U-2 became available, or as satellites were first used. These "collectors" required the creation of new institutions, organizational structures and processes, to take full advantage of their capability. This was not only to build the information collectors, but also to process the information that was collected. In the United States it led to the creation of the National Security Agency (1953), and the National Reconnaissance Office (1960). There were also cross-silo organizations like the National Overhead Reconnaissance Program (NORP), and the National Underwater Reconnaissance Program (NURP). The availability of this data, properly organized and put into the right context was critical to new missions.[31]

Some of the information in these systems was critically important for national decisions, like early warning, surprise attack, the decision to launch and disperse SAC bombers and submarines in port, and the decision to evacuate the president and vice president from Washington. The design and construction of this complex apparatus took over ten years.

This is all worth recalling because the world is now witnessing a comparable development by the major powers. They are building new institutions to collect, process, and use the information available. What is surely true, is that the amount of information in

31 China's defense and intelligence system is now going through this transformation. The macro-organizational changes and their strategic implications are discussed in Paul Bracken, "How New Technologies Are Shaping China's Military Strategy," in David Denoon, ed., *China's Current Grand Strategy* (New York: New York University Press, forthcoming 2020).

this endeavor dwarfs anything undertaken in the Cold War.

Some countries are at the beginning of this process, whole others are further along. Some will do an excellent job, and others will do it in a half-baked way.

Another general trend is that each touchpoint in the figure has received significant investment from business purposes for the commercial market. The upfront work on these technologies has either been done, or is now being done. Most of these technologies are in the field already. They are in operational use now. They are not simply a deck of PowerPoint slides. This is very different from the development of the U-2 and spy satellites of the Cold War. The work needed to bring them into operational use was made harder because there was no real commercial markets for these technologies, at the time.

Moreover, the existence of large markets for 5G telecommunications, AI-driven autonomous vehicles (AVs), drone delivery, mobile systems in general has another implication. It could be used as a mask for military purposes. This is the fear behind the Huawei case, that commercial systems will serve a military purpose.

Another general point is that the data streams from these touchpoints are correlated with each other. Traffic cameras that monitor congestion are correlated with cell phone use. People who are delayed make more phone calls to explain that they will be late. These correlations can be monitored and studied to orchestrate driver behavior. A purposefully staged accident at a key intersection could tie up a mobile missile force, and its effects could be monitored by listening to the resulting phone traffic. The delay would cause calls to headquarters to tell them of the delay, and to seek changes in

orders.

There's also a natural ordering in many of the data flows. To use the previous example, congestion detected on traffic cameras precedes a spike in cell phone usage. Likewise, congestion may cause traffic police to dispatch drones to video the congestion. Or, highway patrols may be sent to the tie up. These can be monitored over police radio channels.

In sum, there is a large data-intensive fingerprint that develops over time, something that can be studied for clues about behavior. This information could be left on the table, so to speak. That is, it could be ignored by focusing on traditional information collectors – the unshaded touchpoints in the above figure.

But this seems unlikely. It would be like arguing against a reconnaissance satellite program in 1958 because that wasn't how things were done in World War II. At one time it also was argued in the 1950s that satellites can be fooled by deception, camouflage, and other tricks. The conclusion was that it might be better to not rely on satellites for this reason. This argument, of course, got nowhere.

Such arguments were not persuasive in the 1950s. And they are not persuasive now. A new surveillance regime is being built by major powers. Only they can afford it. And it's capability and performance will vary by country.

There is one other big reason behind the technological momentum described here. Success in this technological area has enormous commercial spin-off implications, and big "spin on" ones as well. The cost of the information collection systems in the touchpoint figure are falling because mass production and commercial use drives it down.

China is said to have 300 million cameras for facial recognition, for example. This is spin-on. China also uses defense applications to perfect the technologies. This is spin-off. Unless there is some surprise development, the momentum path of technologies is likely to be used in the hunt for mobile missiles.

New Reconaissance Technologies

The framework for finding mobile missiles used in this report treats new reconnaissance technologies for search and data collection as touchpoints. The term reconnaissance is used to describe military observations of a region to locate an enemy or to determine strategic characteristics of its forces. This would include readiness and alert levels, whether a missile is nuclear armed, and whether a pre-delegated launch order has been given to subordinate commanders.

Reconnaissance corresponds to the "search" concept used in max-min theory discussed earlier. There are "hiders" with mobile missiles. And there are "finders" who search for them.

The reconnaissance technologies described in this section all qualify for attention because they could "touch" mobile missiles. There is no assertion or claim that the particular technology will always "find the mobile missile." Rather, our intent here is to identify touchpoints between hiders (missiles) and seekers (an intelligence service trying to locate the missiles).

Advanced technologies for search have created new possibilities for finding mobile missiles and other fleeting targets. The technologies themselves allow for collection of new kinds of data much more broadly than in the Cold War. The use of this data for search represents an application of the collection technologies. It should

be noted that the search for mobile missiles is one application area. There are others, such as in cyberwar where one tries to locate the computers causing problems. Another is to locate warships and submarines. All of these are exemplars in a revolutionary change in the information regime of war.

The touchpoints are treated in the order shown in the graphic on page 106.

Hacked Security Cameras

It is estimated that there are 300 million security cameras currently operating in China. Moreover, the rapid urbanization taking place around the world has led to a sharp increase in surveillance cameras everywhere. These are used in everything from traffic control, beach safety, emergency response, environmental monitoring, crime prevention, and crowd control. The output of the cameras goes to a processing center.[32] What is different from old-style security cameras is that the cameras now are organized into a network.[33] The camera output doesn't simply go to a room where a sleepy guard watches 25 TV screens. The network is "smart" in that it can be triggered automatically by various events. A car with a particular license plate drives by; more than 5 staff cars leave a building in a 15-minute time span; a nuclear engineer walks across the street and his photo is snapped by a facial recognition camera -- these are "events." This network can be pointed at different targets, it can zoom in to take

32 For an overview of camera networks, see Amit K. Roy-Chowdhury, *Camera Networks: the Acquisition and Analysis of Videos Over Wide Areas* (Morgan & Claypool, 2012); and Andrea Aghajan and Hamid Cavallaro, *Multi-Camera Networks: Principles and Applications* (Elsevier, 2009).

33 See Christophe Bobda, *Distributed Embedded Smart Cameras*, (New York: Springer, 2014).

a closer look, and it can be programmed to trigger an alert message when a certain vehicle or individual is detected.

The output from the cameras may be analyzed by AI software. This could be some combination of automated license plate readers, facial recognition, and tracking of suspects in criminal and other matters. The key point to underscore is that surveillance cameras today operate as dynamic networks. The analysis goes beyond mere detection. Millions of hours have traffic can be used to feed neural nets and deep learning algorithms so that the camera network itself builds up knowledge of, for example, the nuclear alert behavior of a particular country.[34]

Over the past decade, unsurprisingly, there has been an enormous increase in the orchestration of camera networks to process the vast amount of data that comes out of them. This involves automation of the assessment process. This is closely connected to the optimization of camera networks. If a target was detected driving down a street from an automated license plate reader (see below) or from facial recognition camera, it might trigger a message to a regional camera network to re-point the cameras at certain other streets where the target might be headed. The re-aiming of cameras in sync with mobile targets is meant to optimize the search process. This is important because some "hits" from a security camera may be partial or uncertain, or they may be altogether wrong. Lighting conditions, rain, and shadows can all reduce the performance of the cameras. The angle of the picture may not be good enough to get a perfect identification of the target.

34 For examples, see Vajaiyan K. Asari, (ed.), *Wide Area Surveillance: Real Time Motion Detection Systems* (New York: Springer, 2014).

Another feature about security camera networks is that they are notorious for being easy to hack into. One reason is that the vast number of cameras now in use present an enormous network surface open to penetration. It would be comparatively easy for an intelligence service that understood camera networks to understand the collection and data bases used. This could be done simply by penetrating through one single camera, which would give access to the network. It would be a simple matter for a team to access a camera on one telephone pole under the guise of servicing the camera. Indeed, this has occurred in several known incidents. Penetration could also be through some opening on the management system at a headquarters (i.e., from an insider with a flash drive). Security companies tend to have very low personnel standards, and few internal checks and controls on employees.

Most camera networks transmit their data over radio links, and this too offers another opening for penetration. For example, in India, Pakistan, and Britain the network boxes that do this are nearly all built and serviced by Huawei, the Chinese company. Some of these have had recently discovered "tunnels" – administrative channels to allow remote updating of the camera firmware. This is a legitimate servicing technique. At the same time, it opens the network to penetration on a much wider front.

Camera networks will likely be connected to other reconnaissance technologies. These include automated license plate readers, computer vision, and facial recognition. If the names of soldiers working on a missile crew were known, it would not be difficult to find their personal information, such as the license plates of their personal vehicles or motor scooters. These individuals could then be tracked through movement by hacking into the camera network.

Their home addresses could easily be found. In the event of a crisis or mobilization, the sudden movement of such key individuals to a new location might be a tip-off that preparations for heightened readiness were underway. In other words, the camera network would reveal alerts, crisis management moves, and provide insight into the situation. They could aid in distinguishing between token, small movements of a nuclear force and a full-out mobilization.

By counting the number of trucks or staff cars in motion over a small number of roads a good estimate could be had of the scale of an alert. It might also be possible to determine if there was movement of the nuclear warheads themselves. The cameras for this job could use special purpose lenses discreetly mounted on buildings or poles. Or the task could be done with off-the-shelf iPads running AI programs that count different kinds of vehicles (e.g., trucks known to be used for carrying or guarding atomic warheads, TELs, or support trucks). A recent study of crowd size in Hong Kong political demonstrations was able to use just seven iPads with their standard built-in cameras to accurately count people traveling over known routes.[35]

Camera networks are less dense away from urban areas. But they also have a longer range of vision because they are not blocked by buildings or other obstacles. Indeed, one of the latest advances is to extend the range of camera vision. Small cameras or cameras disguised to appear like cable or electric insulators on power lines would likely evade detection by local authorities.

Hacked Cell Phones

35 "How A.I. Helped Improve Crowd Counting in Hong Kong Protests," *New York Times*, July 3, 2019.

Cell phones offer an entirely different phenomenology than camera video. Technologies for tracking cell phones have veritably exploded in recent years.[36] It is used to track individuals as they travel through a shopping mall. It is used in law enforcement to track suspects by following the GPS "pings" from their phones. And it is used create individual and group profiles of different groups of people. In a recent business case, a department store studied the origins of their customers and found that a large number of them lived in the city's Asian neighborhoods. This led the store to offer more Asian products, like noodle and sushi bars. In another example, a restaurant tracked the cell phones and traffic flows in their neighborhood. They found a large number of women driving at rush hour through the area. They created a "girls' night out product" of discounted drinks to attract new, female customers. Note that this process involved not only tracking of mobile phones, but matching the phone owner to other data bases to determine gender, age, and income levels. All of this was integrated into a common operational picture of a "market in motion" of the traffic patterns around the restaurant.

Phone tracking in business, therefore, is linked to other data bases using something called location analytics (see below). Virtually all of this data is inside the company, not in hardened military IT sites. Generally speaking, companies offer a lower set of protections against hacking. And while government may regulate cell phone

36 An overview of technical developments in mobile networks is Simone Fratassi and Francis Cantonio, *Mobile Positioning and Tracking, From Conventional to Cooperative Techniques*, (Wiley IEEE Press, 2017); for emerging 5G mobile networks, see Mojtaba Vaezi, *Cloud Mobile Networks from RAN to EPC* (New York: Springer, 2017). RAN refers to radio access networks, and EPC refers to evolved packet cores.

networks, in almost no countries do governments actually operate these systems. This means that personnel data are protected by lower standards of cyber hardening.

The mobility patterns of soldiers attached to missile or warhead units could be tracked in a variety of ways. It could be accomplished without their consent. Doing this would show patterns of movement and other behaviors under different conditions. There might be one pattern displayed in normal peacetime conditions, and a different pattern at times of heightened tensions or during an exercise or alert. Since virtually all phones have GPS or some other location system, and links to cell towers, tracking a crew member could be the same as tracking a missile. Such a reconnaissance system would require careful planning, investment, and observations perhaps over years to fit the data collected with actual movements. But this is probably no more difficult than the tracking of customers driving by a restaurant, the business example described above. The amount of data collected to do this is large, by the standard of World War II and the Cold War. But it is quite small by the standards of today's databases using cloud storage.

There are segments of people that could be pursued. In many ways this is a akin to segmentation of customers in market research.[37] One "customer segment" is to track the phones of senior officers associated with nuclear command and control systems. Another customer segment is officers and enlistees in the field as they go on missile dispersal exercises. Still another is to track the atomic

37 See Sara Dolnicar, Bettina Grun, and Friedrich Leisch, *Market Segmentation Analysis, Understanding It, Doing It, and Making It Useful* (New York: Springer, 2018).

warhead guard force. It isn't difficult to extend this segmentation list to key individuals associated with various nuclear activities.

Another type of segmentation is geographic. Here, individuals entering a particular region are tracked as to the times they enter or leave a particular location. The location could be a military base, headquarters building, or an area that was suspected to be a site for a missile. This process is called "geofencing," and it has been highly developed to track customer cell phones in shopping malls and big box stores.[38] It is also used to enforce congestion tolls in some cities. Anytime a person's phone enters an electronically fenced off area, a notice is sent to the monitor. The area could be, for example, the housewares section of a retailer.

Geofencing goes far beyond merely tracking individual phones, however. Complex deceptive strategies have been developed based on geofencing. To take one prominent example, Uber developed ways to fool regulators trying to crack down on their unregulated ride services. The idea was to create "phantom" cars that suddenly disappeared if they were hailed by a regulator posing as a normal customer. Uber did this as far back as 2014, using a tactic called data poisoning.[39] The point of this example is not only to offer a specific way that phones may be tracked and used. Rather, it is to assert that very complicated strategies and counter strategies of geofencing will develop, just as they have in commercial enterprise. A similar development will develop in digital tracking of targets for security.

38 For an overview of geofencing, see Gerardus Blokdyk, *Geofencing: A Clear and Concise Reference* (5STARSCooks, 2018).

39 See Mike Isaac, *Super Pumped, the Battle for Uber* (New York: W. W. Norton & Company, 2019); and "How Uber Deceives Authorities Worldwide," *New York Times*, March 3, 2017.

For phone hacking, it is necessary to get inside the cell phone system of a country. There are many technologies to do this. StingRays are boxes placed on telephone poles that are made to appear like standard telephone equipment. These boxes trick the network into behaving as if the box were a true part of the network. StingRay receives all phone calls, text messages, social media, etc. that are tagged to a particular phone number. In short, StingRay simulates a cellular phone element, and resends messages and ping locations to an outside source. Recently, several unauthorized StingRay boxes have been discovered in Washington, D.C.[40] No one knows who put them on the poles, but it was not the local cell phone companies. The boxes were unauthorized by the cell phone company.

StingRay boxes are also used on small aircraft to track individual subjects. They would be easy to put on a drone. They are only one collection technology associated with cell phone hacking. There are many others, to include systems on satellites that continuously cover a geographic area.

Drone Video

Drones are an ideal reconnaissance technology because they get close to their targets without endangering human operators.[41] They are getting smaller, cheaper, and stealthier as well. This allows for unobtrusive surveillance.

40 Lily Hay Newman, "DC's StingRay Mess Won't Get Cleaned Up," *Wired*, April 6, 2018.

41 There are many journalistic accounts of drones in war. A good technical overview of current drone technology is in Jung-Sup Un, *Drones as Cyber-Physical Systems, Concepts and Applications for the Fourth Industrial Revolution* (New York: Springer, 2019).

In searching for mobile missiles, drones are especially useful when they are operated with other touchpoints. They can be assigned to cover a certain region that had delivered "hits" from the reconnaissance channels. Used this way, the drones could double check to corroborate these sources. This is likely to be quite important in tracking nuclear targets.

Some drones are especially difficult to detect and these are likely to be a new fashion in this field. Most high-speed cameras fail to find drone swarms as they look on earth like a flock of birds. They can swoop down on a target individually or in groups and are hardly noticed. Other kinds of sensors can be put on the drones. For example, some may have machine vision sensors aboard programmed to detect the long narrow shape of a TEL. According to press reports, this is what Project Maven, the contract between DoD and Google, was designed for, to put machine vision aboard a small carrier like a drone so it could pick out objects of a certain size and shape.

Other drones might carry different types of sensors, like video cameras or StingRay boxes. The technology thrust is to build in autonomous flight capability. This is so the drones do not collide with each other, or with other objects. And it is also drone swarms are too difficult to control by a human operator.

Small drones, it should be mentioned, could be hidden inside of a country and launched when ordered. This is a another way that the reach of an insider threat mentioned previously could be enlarged to cover and track targets over a bigger geographic area. The insider need not get physically close to the target. Rather, he could locate it, then signal where it was. Next, drones from outside a country's

border could be sent to the area in question.

Satellites

While reconnaissance satellites have been around since the late 1950s, advanced sensor packages for them have not. Many of the sensors discussed in this report could be placed on satellites (e.g., cell phone detection systems, video, communications intelligence). The big change in this area is to place multiple packages on a satellite. This is made possible by advances in shrinking the size of the sensors and their electronics. It also fits in with the trend to small easy-to-launch cube satellites.

This "packaging of multiple sensors" on a satellite has another consequence. It makes it difficult to determine exactly what is up there because military sensors may be on commercial satellites. Some may be activated only periodically. In the Cold War most satellite sensors required special purpose satellites, and this allowed the enemy to estimate its purpose from orbital data.

A satellite with multiple sensor packages could switch over collection systems as the strategic environment changes, or as the intensity of a crisis increased. In other words, it would be integrated into the alerting system of nuclear command and control. One of the tips offs of an impending crisis in the Cold War was the launch by a superpower of reconnaissance satellites. But this told the other side that something was up. Now at least some reconnaissance can be disguised as a commercial launches or conducted with drones in order to conceal national intensions or actions.

Ground Penetrating Radar (GPR)

Ground penetrating radar (GPR) is useful to locate mobile missiles hidden in caves or underground facilities of various kinds. It is based on polarized radio waves that detect variations in the soil makeup. Other technologies rely on sensing small changes in gravitational fields. For example, a tunnel or mountain chamber would have a different gravity signature than if there were no cavity.[42] The United States has had a DARPA project on this for several years. And there is good reason to believe that China has invested in this technology as well, given their extensive use of tunnels for their long-range nuclear forces

Advanced GPR could be deployed on stealthy aircraft or drones. Again, it would make sense to link the output of this data collection with other sensors. The whole reason behind putting a missile underground or inside a cave is to have it come out to fire. In other words, it is a fleeting target. GPR is more likely going to be used to find missile bases in peacetime rather than to be employed for real-time tracking.

Spy Reports

Spies have been used since the beginning of time. Some spies have had enormous impact, but most have had very little. Spy networks take on a new potential when armed with turbocharged smart phones for taking videos, burst transmission of information to headquarters, and micro drones for wide area surveillance.

Especially as technology becomes a larger element in intelligence, spies will be used to gather information about enemy technology.

42 "Secret Tunnels Can't Hide from Gravity, *National Defense,"* September 1, 2009.

This includes how it operates, and information about vendors who build and maintain it. Getting spies inside a telecommunications or a power company, or inside a supplier of equipment for TELs could provide far more useful information than the classic spy movie dramas fed to the public. It is useful to recall that Edward Snowden was an NSA contractor. His revelations to the public uncovered the existence of a world that few people knew existed before his revelations.

It is, frankly speaking, hard to imagine that spies won't try to penetrate the technology companies that build the advanced technologies of modern war. This brings up a closely related topic. The supply chains that provide the technologies are often global. Protecting the information in them is extremely difficult because they were not designed for this. China in particular has made many large advances by penetrating the supply chains of Western multinationals. Indeed, it is the commercial technology companies that understand best of all the opportunities for penetration of telecommunications and power grids.

Spies who can get information about communications and data storage may offer especially useful ways to track mobile missiles. The spies themselves may not directly track the missiles. But spies can now direct reconnaissance systems – drones, satellites, StingRay boxes -- to greatly widen the scope and reach of their surveillance.

Facial Recognition Technology

In 1998, when India sought to deceive the United States that it was about to test five atomic bombs, it had the physicists running the program wear false beards, makeup, and hats to hide the fact that they were converging on the test site for a test. The parking lot at

the test site was carefully controlled by Indian intelligence, so as not fill up with cars in the days before the test. This simple deception worked like a charm. The United States was clueless about the impending nuclear shots.[43]

Today, facial recognition technology could be used not only to track scientists, but also middle level government officials, officers and enlistees in the armed forces, and even security guards. The size of this data base might seem like it is too large to handle. But it is trivially small compared to the data maintained by companies today, or those of China's security police.

The key to using facial recognition technology is to link known individuals associated with various kinds of military operations, like alerting and dispersing a mobile missile force. This database would be segmented into different groups, using software now in daily business use in the United States, Europe, and China. To obtain the facial recognition data itself would require hacking into the appropriate systems in various countries.

This "linkage" of people in sensitive positions to their activities has already taken place. In 2018 the U.S. government blocked the purchase of a private U.S. company called MoneyGram by Ant Financial, a Chinese company. Ant is owned by Alibaba. The fear in Washington was that if MoneyGram were owned by China, Beijing could access not only the databases of the company itself, but also credit reports and other detailed information of hundreds of millions of Americans, including those employed by DoD and

43 The 1998 atomic test at Pokhran, India was a sophisticated deception program, with multiple parts. See "Pokhran '98: Satellites Nuked," *Geospatial World*, December 2, 2010.

the intelligence services. MoneyGram had ready access to virtually all the credit reporting databases in the United States. The fear was that Americans in sensitive positions and those in financial trouble could be targeted or blackmailed.

With facial recognition technology targeted individuals could be found on the street or driving their cars or taking the subway. All of this is quite common in China, and increasingly in the United States. These snapshots could indicate where, exactly, the individuals worked. This would automatically provide sensitive information, which could be used to assess which bureaus they worked in, for example, the Ministry of Defense. This information in turn could be linked with their cell phone use patterns, like route selection for their commute. Large deviations from standard travel patterns by multiple individuals would be a tip-off that something was up. Here, facial recognition is used to provide real-time warning. Given the real-time trend in facial recognition surveillance, an individual can often be located in minutes. The accumulation of this data at scale -- thousands of people mobilized for work at a crisis management center – could be extremely useful for many military purposes. It could, for example, be used to refine targeted killings on a large scale.

The technology for facial recognition now in use was written by the private sector. Off-the-shelf software is everywhere, and only small modifications would be needed for intelligence and defense use.

5G Tracking and Disruption

5G is the emerging set of standards for communications for the Internet of Things (IoT). It is the follow-on technology for the current mobile phone system, but with such extraordinary increases in information processing that it is critical for autonomous vehicles

(AVs), and many other sectors of the new economy. AVs require a tremendous volume of data exchange between vehicles on the highway, and their outside environment. AVs also link to other mobile networks for entertainment, business, and public safety.[44]

5G is the subject of great concern in Washington because a Chinese company, Huawei, is now a dominant leader in supplying the equipment. Huawei stands ready to control not only world markets, but even the United States market unless counter actions are taken. This has led in 2019 to the U.S. government banning Federal government use (especially military use) of equipment from Huawei, and from another Chinese firm, ZTE.

5G will allow for real-time interaction of systems of an unprecedented kind. It allows new application areas, such as the "tactile Internet." The tactile Internet, based on 5G technologies, would allow a doctor in London to operate robotic surgery instruments on a patient in Cape Town. This use of the web requires extremely low latency, that is, the time between a hand movement in London and its effects in Cape Town. A few milliseconds delay makes it seem that the patient is in London. There is a near instantaneous interaction.

One fear is that 5G technologies will lead to an unprecedented ability to track things. This is because of the exponential increase in radio transmissions and the number of antennas. 5G disruption strategies could be used to upset the modern systems a society depends on. Disruption of electric power, communications, and finance could

44 For an introduction to IoT in a mobile environment, see Constandinos X. Mavromoustakis, et al., (eds.), *Internet of Things (IoT) in 5G Mobile Technologies* (Springer, 2016); and Jonathan Rodriguez, (ed.), *Fundamentals of 5G Mobile Networks* (West Sussex, UK: John Wiley and Sons Limited, 2015).

paralyze a country. The simple act of filling the gas tank for a TEL and the vehicles that go with it would be impossible if the electric system were brought down. The effect would be to freeze targets in place. They would be awaiting orders that never come, or resources like fuel or electronic map updates.

Fears over 5G also cover more extreme examples. "Smart cities," for example, could be told to attack themselves. Commuter rail lines could be reprogrammed to crash with other trains. ATMs could be shut down or, worse, redirected to withdraw millions of dollars from accounts in order to sow chaos. The power grid could be directed to surge voltages to targeted parts of the grid, like military bases. This would cause overloads and blackouts.

It seems like science fiction to describe these possibilities. But 5G technologies are coming to the world faster than most people realize. Every nuclear weapon state has significant plans to upgrade their national telecommunications infrastructure to handle AVs, the IoT, and 5G.

Computer Hacks

One of the most important uses of cyber is espionage. This involves entering the computer networks of another state in order to search for information of military use. The planning of something as complex as dispersing mobile missiles is likely to be stored on PCs and computer networks. The required inventory of spare parts, diesel fuel, support vehicle maintenance, and even the lubrication schedules of TEL engines are all stored on computers.

Such mundane data may seem to be of little interest. But a vast amount of data is needed to manage a mobile missile force compared

to a fixed base force. When properly analyzed, the data is a gold mine of insights about enemy behavior patterns. Lubrication schedules, to take a trivial example, would provide a useful tip-off as to how many miles a TEL had been driven. If there were long periods between oil changes, this could indicate that dispersal exercises were few and far between. This could be a valuable piece of information regarding the readiness of the enemy force.

Higher up the command chain, computer hacks could be used to automatically send covert alert messages to intelligence units. This would require insertion of spyware into the enemy command and control system. But as events with the implant of the Stuxnet virus demonstrate, this is a decade-old technology.

Finally, it is possible that an intelligence service might "luck out" and find extraordinarily important information. The experience in the Cold War is that even highly sensitive secrets are often poorly protected. When the U.S.S. Pueblo was captured by North Korea in 1968 it carried a vast collection of papers, codebooks, and surveillance equipment. The NSA later declared this was the worst security breach in American history up to that time.[45]

The possibility that very sensitive information is mistakenly distributed to the wrong addressee, or to units with no need for it, is vastly greater than it has been in the past. The cost of sending anything has declined enormously because of email and attachments. The number of files sent is so great that simply checking for what documents are on which computer is an onerous, almost insurmountable task. There is likely to be a great deal of effort put

45 John Cheevers, *Act of War: Lyndon Johnson, North Korea, and the Capture of the Spy Ship Pueblo* (Dutton, 2013).

into searching enemy computers to find lucky hits, like code books, plans, or preplanned dispersal orders.

AESA Radar

Active Electronically Scanned Array (AESA) radar is a type of phased array radar with each radar element individually controlled by computer software. A standard phased array radar has all of the antenna elements controlled by a single transmitter. AESA radars can be pointed in different directions at the same time using different elements, a process called beam forming.

The significance of AESA is that the radar can track multiple ground targets at the same time. For example, a missile TEL and its support vehicles could be more readily identified and picked out from the background clutter. In addition, AESA radar can better pick out small targets because each antenna element can transmit on different wavelengths. Smaller vehicles traveling along with larger TELs are an example of a target set that AESA radars could find that would be more difficult for standard radar.

AESA radars are part of the F-35 fighter suite of electronic warfare and are on other aircraft in many countries. AESA radar is also put on satellites in order to track ground and sea targets more accurately (i.e., where there is a group of different shaped targets operating together). All the major powers, including India, have invested in the technology for this reason.

In recent years, AESA electronics has improved considerably both in performance and in shrinking the size of the package. It can now be deployed on drones and small aircraft.

Automated License Plate Readers

Automated license plate readers (ALPR) are computer vision cameras that read license plate numbers. The cameras may be stationary (attached to a building or telephone pole) or mobile (on a police car). The "reads" of the plates are linked to a "hot sheet" – a data base in the cloud, with a list of numbers that are of interest to the police or to an intelligence service. When there's a "hit" -- a match of a plate on the hot sheet -- a notification is sent. Automated license plate readers today are routinely deployed around the world for law enforcement purposes.[46] They can read thousands of plates in a short period of time.

ALPR technology has reached a high level of sophistication. They can work at night, in rain, and can deliver good read-outs even when the picture is snapped from oblique angles. They are deployed today on police cars and in fixed sites. Driving around a city, a patrol car with an ALPR can easily read thousands of plates per minute. The plates are automatically cross-checked with the hot sheet.

It would be reasonable to assume that intelligence services of the major countries could reduce the size of these cameras so that they would be virtually impossible to detect. Given the busy airwaves in most cities, it would be difficult to pick out their signals, which in any case could be hidden or disguised in various ways (e.g., with spread spectrum or burst transmission).

Of course, this system is only useful if a database of license plates was built up beforehand. For mobile missile location, one could

46 For an overview of ALPR, see *Automated License Plate Readers, Street Level Surveillance* (Electronic Frontier Foundation, 2016); also Benjamin Hayes, "U.S. Immigration and Customs Enforcement Use of Automated License Plate Reader Databases," *Georgetown Immigration Law Journal* 33:1 (Fall 2018), pp. 145-48.

track the support vehicles or the personal automobiles of the soldiers in the missile crew. It would also be useful to build databases for headquarters personnel, civilians and military. Furthermore, analysis of the data would reveal micro-behavior patterns.

In a full alert, for example, crew would be ordered to report to various headquarters units and military bases. This could be picked up hours before any mobile missiles were actually moving. It could give several hours or more of warning, and this could be a very dangerous time. Quick reaction alert (QRA) air or missile strikes before the missiles had dispersed could be used to destroy the peacetime missile locations themselves. Or the attacks could create roadblocks and bottle necks. An attacker could disrupt the dispersal and do so in a precise way with conventional weapons.

The output from ALPRs also could be double-checked with facial recognition data, visual contacts from security cameras, and cell phone tracking. In one application of ALPR, autos equipped with covert ALPR might be sent to drive around military bases or regions of a country if indications came of increased tensions.

Radio Beacons

Radio beacons are small, battery-operated radio transmitters that send signals to nearby smart phones or tablets. If the phone has a special app, a message is sent from the phone to a remote database notifying it that a customer has physically passed close to the beacon.[47] The app may be loaded onto the phone knowingly, as part of an

47 Beacon technology and its uses in business and marketing is explained in Stephen Statler, Anke Audenaert, Theresa Mary Gordon, and Phile Hendrix, *Beacon Technologies: The Hitchhiker's Guide to the Beaconsystem* (Apress, 2016).

advertising campaign or to qualify for product discounts (e.g., in a store). Or the app may be covertly installed under the mask of some other program designed to attract a particular audience. McDonald's apps have often been tied to marketing campaigns of professional sports teams (see below). Anyone who downloads the McDonald's app may unknowingly be linked to the team's marketing campaign.

Beacon technology is revolutionizing marketing. They are cheap, costing about $5-$30 per beacon, depending on the features. It has been estimated that by 2020 there will be 400 million beacons in use throughout the world.[48]

Sports are a good example of how beacons are used. Every professional baseball, football, and basketball franchise in the United States uses beacon technology. In one application, a customer comes to the ticket office to buy a ticket to an NBA game. Since he is a fan, he has downloaded the app for the Philadelphia 76ers, as an example. The beacon senses that he is close to the ticket window. It sends a signal to his cell phone that if he buys an upgraded (better) seat, he'll get an immediate 20 percent discount on that ticket. A cloud database knows how many seats are sold, and uses predictive analytics to estimate how many will be sold by game time. The actual discount, therefore, is dynamic. It is constantly adjusted to reflect the dynamic supply and demand conditions of the particular game. The customer can simply check the "yes" box and avoid the ticket line altogether. His credit card is automatically charged the appropriate mount.

There are ingenious marketing applications using beacon technology

48 "20/20 Vision: 400 million Beacons on Track for Global Deployment Within Four Years," *Geomarketing*, January 25, 2016.

and many of these are controversial. For example, there are reports that some NBA teams have downloaded apps to customer phones which turn "on" the microphone of the cell phone in the arena. Presumably, this produces a database of "talk" that can be analyzed using AI methods to determine how intensely involved in the game the fans are, their eating habits, and their propensity to purchase team clothing, paraphernalia, etc.

For locating mobile missiles, beacons could be placed innocuously at the entry to military bases, or at the entryway to a headquarters office building. It would be necessary to insert a special "app" on the phones of the "customers," the enlistees, officers, and civilians working in the defense command. This would not be particularly difficult. A marketing campaign to segment these is easily designed. For example, a fast food chain located near a military headquarters might offer a discount to "those who protect our nation." This discount would require them to download an app to their phone. It would get the customer a small discount at a fast food restaurant. But the app really would be a mask, a Trojan horse, for the beacon technology, with messages sent not to the individual, but to a cloud run by a foreign intelligence service.

There are many other use cases. Mobile beacons might be used to determine the location of missile convoys. Or routes for TELs could be lined with beacons to determine their location and direction. As with other technologies, the beacons could be cross-checked with ALPR, cell phone, and security camera hacks.

Augmented Reality (AR) and Smart Glasses

Augmented Reality (AR) is a technology where objects in the real world are augmented by computer-generated perceptual

information. The augmentations could be visual or auditory or in some other form.[49] When combined with smart glasses, there are important applications for target tracking.

Smart glasses are wearable computers that add information to what the wearer sees. They can be controlled by voice commands and can be directed to various tasks. For example, they may record a military exercise and be used to pick out key elements like TELs or particular types of missiles, or whether warheads were placed on the missiles. Or they can contain a heads-up display of data -- like license plates. In one application in China a facial recognition system built into smart glasses automatically displays onto the lenses in a heads-up display the identification card and criminal record of the person tracked.

In another application also in China, police spot a person of interest and walk by him wearing the glasses. Facial recognition cameras in the glasses take a picture. It is automatically uploaded to a cloud data base for comparison with the individual's name, address, occupation. On command, a cue is sent to track the person's cell phone.

Law enforcement in China uses uniformed and undercover police to wander the streets near sensitive facilities, like Tiananmen Square in Beijing. The purpose is to determine if protestors might be gathering in the streets leading up to the Square. But the same thing could be done near a military headquarters or intelligence center by foreign agents equipped with AR and smart glasses.

49 For an overview of augmented reality and smart glasses and their applications, see Robert Scoble and Shel Israel, *The Fourth Transformation: How Augmented Reality and Artificial Intelligence Change Everything* (Patrick Brewster Press, 2017).

Recently, some Chinese companies have advanced even this technology.[50] Full motion video can feed the facial recognition cameras, with night vision and geolocation abilities built into them. Another trend is to mass produce the glasses in order to drive down their cost. Low-end glasses can be bought today for $250. This low price reflects the fact that most of the cost of this collection system is in the upfront research and development, and in the software, rather than in the hardware. These are being sold to police and intelligence services around the world.

Applied to the hunt for mobile missiles, AR smart glasses could be used to detect the early stages of an alert. Agents wearing the glasses could pass by warhead storage areas and missile bases to determine the preparations for a dispersal. The glasses would be an ideal tool for insider attacks as well. Intelligence services could actually watch as the hydraulic lift of the TEL went into operation. Or, they could watch as nuclear warheads are mated with the missiles. This would provide real-time video of the final minutes before launch. It would clearly be a highly useful tactical warning indicator of attack.

Other uses of AR smart glasses are to track the senior officials in the high command. This would be useful for decapitation strikes on the nuclear command and control system. It should be noted that in the Cold War both superpowers put great effort into leadership tracking of senior political officials in Moscow and Washington.

Location Analytics

Location analytics tracks the movement of customers or vehicles to

50 "Chinese AR Start-Up Develops Smart Glasses," *South China Morning Post*, May 6, 2019.

analyze their behaviors. One application is to track cell phones in shopping malls to determine the dwell time of customers at different displays or in different parts of the store.[51]

Another application is for insurance companies to rate the "good driving" behavior of their customers. Today, they are widely used to offer discounts to drivers based on safe driving habits. These include accelerations, the number of left turns, following the speed limit, etc.

Originally, location analytic packages were in a USB stick that was plugged into a car. The recent approaches download software directly on to the driver's cell phone.

A cell phone with a location analytics package could be an excellent way to track a mobile missile force. This is because micro behaviors could be discovered, behaviors that the commanders in charge of the missile force could be unaware of.[52] For example, certain driving patterns, such as extreme caution when operating a big truck like a TEL, might be characteristic of a new driver. A new driver might be hesitant, and brake harder than an experienced one. This behavior would provide insight into how experienced the missile force's crew is. Extremely slow left turns would be another indication of

51 For up-to-date uses of location analytics, see David Z. Beitz, *Location Analytics for Business: the Research and Marketing Strategic Advantage* (Business Expert Press, 2018).

52 An example of such subtle behavior and its importance occurred in World War II. British intelligence was able to monitor what they called "the fist" of their agents inserted into Nazi-controlled France. Messages were transmitted to London by radio using Morse code. But each operator had a slightly different "fist." Some had slightly longer delays in the time between dots and dashes in sending a particular letter of the alphabet. There were cases when the agents in France were captured by the Germans, and Germans tried to send false information using the channels back to London. These fake reports were often immediately found to be fake, as the sender had a different "fist."

inexperienced operators. Both of these micro driving behaviors would be easily detected by existing software packages.

Behavioral biometrics have also been used to authenticate individual user identities.[53] The software measures hundreds of behavioral features of cell phone use (e.g., time between screen presses, right- or left-handed operators, pressure used, hand tremor, and many others). These are matched to user profiles to determine if an individual is who they say they are. These could be valuable tools for insider intelligence agents, or even for ensuring that the operator of the cell phone hasn't changed (e.g., as part of a deception operation).

If the applications were inserted into multiple phones, the interaction among vehicles in a convoys could be analyzed. Distances between trucks, speed, etc. could provide tip-offs regarding whether the warheads are with the TELs or kept back in storage.

Communication Intercepts

Intercepting enemy communications is one of the largest technology programs of most intelligence services in the world. World War II began with the U.S. failure to read Japanese messages. And the war was won by reading intercepts of German U-Boat traffic in the Battle of the Atlantic and of its army at D-Day.

There is a storied legacy of intercepts, and this tradition carries on into the 21st century. The war on terror and the insurgency in Iraq were a tremendous stimulus to research and investment into this area -- so much so that it has been copied by other countries, especially China, Russia, Iran, and North Korea.

53 See *Invisible Challenges, BioCatch's Game Changing Technology for Online Fraud Protection*, White Paper, BioCatch Corporation, April 2017.

Effective communications intelligence depends on collection, processing, and distribution of the information. It also depends on luck. But the chance of good luck increases with good collection and professional staffs who know how to process the data in a timely way. Distribution of the information almost always turns out to be an obstacle due to the desire of the collecting organization to conceal what they have, and how they got it. This is what was behind the Pearl Harbor failure. The United States had the information to estimate that a Japanese attack was coming, but it was never pulled together and read in a centralized, comprehensive way. It was scattered across different siloed departments. This is actually the reason that the main U.S. intelligence service was named the Central Intelligence Agency.

Cloud computing offers a powerful way to get around the siloed information problem. It is a technology that changes the game when it comes to horizontal integration of complex organizations. This capability by itself is no guarantee that seamless integration will actually happen. There are bureaucratic forces that work against it. Much of the strategy-technology work that goes on in business schools focuses on exactly this problem: how to drive change in organizations and offset bureaucratic tendencies in the other direction.[54]

Nonetheless, compared to the Cold War and other eras, there are technology innovations that radically improve an organization's performance in this regard – if leadership makes it happen.

54 One such course is the author's *Technology and Global Strategy*, taught at the Yale School of Management.

Tailing

One of the oldest intelligence methods is tailing an individual or group. In the Cold War there was a U.S. effort to track the Soviet leadership around Moscow. The idea was that if the Soviets were about to attack there were likely to be frequent meetings of the leadership in the weeks beforehand to go over the plan. This was extremely difficult given the nature of the task and the technology of that era. There were some breakthroughs, however. In one instance, the radios in the limousines of the Soviet leaders were hacked. The United States tracked the leaders and listened to their conversations as they moved about.

Now, technology radically improves the ability to tail a target. A seeker today can extend his range with long-distance laser cameras, as described in the next section. Beacons, license plate readers, and 5G tracking expand the collection area and the physical phenomenology. In addition, an agent can be pointed in the right direction of the target. Finally, the mass of wireless and utility radio frequencies in use almost everywhere makes it easier to conceal communications back to headquarters by trackers.

These points seem obvious. The next step in the evolution is to weaponize the agents. It is one thing to collect information about changes in the readiness of the enemy force; dispatching an agent to attack and disrupt this force is something else. Providing insider agents with beacons or designators to guide incoming missiles to a target is one example. Another is to stage diversionary tactics so as to clog traffic, slow down a convoy, and force it to communicate with headquarters. Assassination of key commanders (e.g.. those with launch codes) is another tactic. This is like the special operation

missions of World War II, the Cold War, and more recently the wars in Iraq and Afghanistan. But it now supercharged with technology.

Computer Vision, Covert Cameras, and LIDAR

The cost of very high quality cameras has dropped exponentially as is clear from cell phone cameras but so have the costs of other types of cameras. Computer vision deals with how computers can be made to have high level cognition from images or videos.[55] A simple example will show an application of this touchpoint.

Supermarkets spend tremendous sums just monitoring their shelves to replenish stock. Today in the United States robots now go around the store to take videos of the shelves. These are not just videos to be analyzed by a human manager. The robots have computer vision cameras in them. They scan the shelves and process data about which products, and what size, need replenishment. A Bluetooth radio channel is used. This scanned data is automatically compared with inventory in the stockroom, and with the incoming truck deliveries for the next few days. If there is a shortfall for a product, the software automatically sends a request to a supplier for more product.

While the purpose of the computer vision robot is to monitor inventory on shelves, it is also to substitute software for employees doing this job.[56] In other words, it is an example of eliminating jobs.

55 Rajalingappaa Shanmugamani, *Deep Learning for Computer Vision: Expert Techniques to Train Advanced Neural Networks Using TensorFlow and Keras* (Packt Publishing, 2018). TensorFlow and Keras are popular open source machine learning languages.

56 This discussion is based on Paul Bracken's visit to PepsiCo's Frito-Lay headquarters in Plano, TX on June 20, 2019 to discuss the use of robots in retail stores.

The supply chain increasingly is automated. Amazon has carried this technology further than anyone, and is opening retail stores without a single employee.[57] They use computer vision to charge customers by watching what they purchase, and linking this to the customer's credit card.

With current computer vision, video scans can differentiate products by brand and size. It "sees" that 16-ounce cream corn is running short, while 32-ounce cans can be supplied by on-site inventory. It can determine that Budweiser stocks are okay, but that Coors needs a reorder.

The next stage in this trend is to shrink on site inventory and replace it with "just in time" truck resupplies. In a few years, even the trucks will be autonomous, and will have no driver. The broader point is that computer vision is a large trend in business, leading to many new innovations in mobile tracking of every conceivable product.

It is worth noting also that the upfront cost of computer vision isn't in the robots or in the cameras. These are cheap. Rather, it is in the software. Once the computer vision software is developed, the marginal cost of producing another robot is very low. This has important consequences. Most military weapons -- aircraft, tanks, cruise missiles -- have high marginal costs. A decision to add one additional F-35 fighter to the force costs $ 100 million. The decision to add computer vision to many drones would be close to zero. This is characteristic of digital technologies. In business school parlance,

57 "Spurred by Amazon, Supermarkets Try Swapping Cashiers for Cameras," *Wall Street Journal*, July 7, 2019.

digital technologies "scale well." More is better, and it doesn't cost very much to produce a lot of these things once the upfront development costs are made.

A related touchpoint is LIDAR, for light detection and ranging. LIDAR uses pulsed lasers to paint a target. The return signal is measured for slight discrepancies with the transmitted signal to determine the shape and size of the object. LIDAR is useful for rapidly building 3-D terrain models and for quickly mapping a city. It is one way to quickly map a geographic region to determine elevations, obstacles, masking terrain, and valleys. All of this would be essential to plot flight paths for hypersonic and cruise missiles against mobile missiles. This is because mobile missiles can show up in varied physical environments, certainly compared to fixed sites. That is why there is a need to quickly compute the feasible attack angles that can be used for flight angles of an attacking force.

LIDAR deployed on drones could rapidly build 3-D terrain models. This would be useful if the enemy missile force chose an unexpected area to operate in. Drones could be sent to the area, along with other sensors. More generally, computer vision could be employed by secreting cameras on telephone poles or as attachments to cell phone antenna boxes. They could be powered off of this electricity source. This deployment would also give them the advantage of seeing over longer distances.

Recently China has scored breakthroughs in LIDAR technology. Their sensors have very long range, out to about 25 miles and they can take pictures of man-sized targets through thick fog.[58] This type

58 "Long Range 3-D LIDAR May Enhance Military Operations," P*hotonics Media*, May 11, 2019.

of sensor would be useful for seeing through forested areas to find hidden targets, yet another touchpoint.

Social Media

Another touchpoint between mobile missiles and intelligence is social media. While this is a new field there are reasons to believe that there will be major interactions in the years ahead. In 2017 and 2018 alone there were six separate cases of touchpoint interactions between mobile missiles and intelligence collection.[59] These included mistaken reports of incoming missiles about to hit Hawaii and Guam; error-filled Tweets issued from a U.S. command center about movement of nuclear weapons; and a test firing of a Minuteman missile from California. There was also a false report of a North Korean nuclear alert that was somehow sent out over Japanese TV channels to warn the population to take cover. All of these occurred in a peacetime situation, and nothing really serious resulted from the incidents.

However, it's not hard to see how this kind of thing could be dangerous in a crisis. False reports on Facebook or Twitter of "sightings" of nuclear missiles on the move in Israel, North Korea, or China could cause panic. The reports might be false -- or not. Moreover, deep fakes have become extremely good in recent years. Images or videos of missiles on the move posted on Instagram could trigger alert levels to ratchet upwards.

Something which cannot be ruled out is purposefully creating panic

59 Nautilus Institute, Preventive Defense Project, Stanford University, and Technology for Global Security, *Social Media Storms and Nuclear Early Warning Systems*, January 8, 2019.

and disorder for the purpose of diverting an enemy to defend against insider attacks. To take a hypothetical example, if China or Russia could make it seem to the United States that North Korea was going on nuclear alert by dispersing its mobile missiles, this might be a way to counter U.S. moves around Taiwan or in the Baltic. Washington might feel that the crisis was spinning out of control. This could force the United States to temper its action. There have already been reports that Beijing has engaged in cyber attacks masked to look like they emanated from Pyongyang.

The Nautilus report cited above suggests several different kinds of social media touchpoints with nuclear weapons. Ill-informed celebrity tweets about complicated military issues that the national leadership doesn't understand is one kind. Another are field reports that are combed for data about the location of mobile missiles. Still another type are false alarms. The use of social media to sow chaos in a nation to disrupt its nuclear preparations is another. Chaos would increase traffic jams, raids on stores, and diversion of staffers and crew to protect their families.

Engine Vibration Analysis

Every diesel, gasoline, or electric motor has small deviations from its blueprint design specifications. These usually are in the audio frequency range but there are other vibrations at higher frequencies. This feature has been used to track drug smugglers on boats and airplanes. It requires that a data base of frequency signatures be compiled beforehand. Next, a "shotgun microphone" is pointed at a target boat in a harbor to pick up its engine signature. This is automatically compared to the signals stored in a data base of known, cataloged signatures of drug operators.

The same technology would work for ground vehicles like TELs, support trucks, and staff cars. The engine signatures of particular vehicles would need to be recorded in advance. But this could be done with readings taken on a specially fitted cell phone. Detection of vehicles tagged as being part of a mobile missile force support group would provide another touchpoint. In addition, acoustic sensors on telephone poles, or covert sensors deployed at key locations could handle this process remotely and automatically.

SLAM Technology

Simultaneous Location and Mapping (SLAM) technology is used for robotic mapping and navigation to enable an unmanned vehicle (drone, automobile) to maps its environment, and at the same time, keeps track of its own position and movement in that environment. The robot vehicle is placed in an unknown environment, one that doesn't use GPS or beacons, and it simultaneously maps out the environment as it moves about. SLAM technology mainly consists of algorithms and software. There are some hardware features, since the algorithms are tailored to the particular environment. SLAM's sensors and algorithms are designed to process certain kinds of data. This could be visual "pictures," sounds, hacked cell phone calls, heat, AESA radar, and other touchpoint data sources. SLAM is also designed for multi-sensor input. This includes switching from one type of sensor inputs to another, depending on conditions.

This description of SLAM technology is somewhat abstract. A very practical example illustrates the idea more clearly. The Roomba 980 is a robot floor vacuum cleaner that has been sold in the U.S. mass

market since 2015.[60] It can be purchased today in any big box retail store or over the web. The Roomba 980 vacuums the floor. But when the Roomba is unboxed it is in an unknown environment, a house with a particular layout. The 980 collects and stores data about the home's layout: the exact distance between floor lamps, tables, and sofas, the number of chairs around a dining room table, and room dimensions. Ceiling height could be easily measured. It uses the data to optimize a cleaning plan, and can be preset to clean at any time. When its battery is low, the 980 automatically returns to a wall charging outlet without any additional commands. The recorded data about room layout is sent over a Wi-Fi connection -- an information chain – to the Roomba corporation.

The algorithms in the Roomba 980 that process the largely visual information use SLAM technology. Other data could be used in different applications. Autonomous vehicles use SLAM in the form of LIDAR (i.e., laser distance measurements). Algorithm details would change, but the underlying technology is SLAM. In the Roomba 980 the intent is to sell the data to other companies like Amazon Alexa and Google Homes.[61] Here, it could be used to improve room acoustics to allow better use of AI-controlled smart speakers. Or, it could be used to optimize lighting, redirect security cameras, and adjust thermostats – automatically, without human command. It would give a company a precise inside map of the house floor plan along with furniture and room size. The Roomba 980 sells today for $700, with the price dropping.

60 See iRobot Roomba 980, Wi-Fi Connected Robot Vacuum Cleaner, product description at iRobot.com.

61 "Your Roomba's Map of Your House Could Soon Be for Sale," *Popular Mechanics*, July 25, 2017.

A hypothetical reconnaissance use of SLAM would be to build it into drones. The drone could then fly over a region and decide on its own, without human orders, whether it was more useful to turn on sensors that monitored cell phone calls or cameras to photograph ground targets. Or it could automatically switch on the appropriate camera for a suite on board, the one most appropriate to the target. Note that in this example drones with SLAM technology could also fly away from targets to transmit their data collection "take" to a headquarters from a position that wouldn't be detected. This would allow covert communications; the targets would be less likely to know they were being tracked.

The revolution now taking place with autonomous vehicles is only possible because of advances in SLAM technology.[62] SLAM requires constructing and updating a description of an unknown environment while keeping track of its own location and movement. SLAM uses multiple types of sensors to feed these algorithms, and it is an important technology for AV operation and collision avoidance. LIDAR, cameras, and other sensors are integrated to guide robots, drone swarms, and AVs around complex, changing environments.

For locating mobile missiles, mobile command posts, or trucks with atomic warheads SLAM technology offers a way to spot these targets on the move. The shapes of these targets are different, made up of edges, protuberances, and other distinctive forms. Especially

62 For a readable account of SLAM technology in action see Nick Polson and James Scott, *AIQ, How Artificial Intelligence Works and How We Can Harness Its Power for a Better World* (New York: St. Martin's Griffin, 2018), pp. 80-95. For a more technical description of SLAM, see Peter Corke, *Robotics, Vision and Control* (New York: Springer, 2017); and Roland Siegwart, Illah R. Nourbakhsh, and Davide Scaramuzzah, *Introduction to Autonomous Mobile Robots, Fundamental Algorithms in MATLAB* (Cambridge: MIT Press, 2011).

for conventional attack of targets where vehicles may be spread over a large area, SLAM technology offers a way for unmanned weapons to go after the highest value targets. This would likely be the nuclear warheads before they were placed on the missiles. Call these the strategically important targets (SITs). SLAM technology could guide an incoming attack – of hypersonic and cruise missiles, armed drones, F-35s – to seek out these SITs.

SLAM is also ideal for mapping indoor target spaces, like a weapons fabrication building, nuclear weapon laboratories, or command and control bunkers. SLAM can be placed in smart glasses so that anyone wearing them who gained entry to these facilities, such as a repairman, could precisely map out the interior wall positions and room layout. This would be useful for targeting and warhead selection.

The Value Chain for Hunting Mobile Missiles

Value chains are one of the most widely used tools in planning complex business enterprises. They are used to decide which part of the value chain to strengthen. And they focus attention on how tightly different links should be coupled with each other. Value chains are part of the core curriculum of management education, and are especially useful for understanding new technology.

One more aspect of value chains is worth raising. They work in <u>all</u> countries. It would be hard to analyze Apple, Alibaba, Siemens, Mahindra, or Uber without understanding their value chain. Yet these firms are from many countries.

The use of value chains in security studies is new, however. But given the increasing importance of advanced technologies like AI and

cyber in defense, they offer a new way to analyze the revolutionary technology changes now taking place.

The value chain puts the focus on new capabilities and postures, rather than on technologies. It is therefore closely related to strategy in ways that include technology – but not in the narrow way that is often analyzed. Given the spread of advanced technology to many countries, this is particularly useful because it "works in all countries." Every major country, and many secondary states, are building complex, technology-intensive forces. The lopsided emphasis of nuclear missiles by North Korea, or the armed drones of Iran, are usefully looked at in this framework. Other examples include China's strategy of anti-access forces, the U.S. use of AI, and applications of cyberwar, drones, etc.

The complexity of these systems – measured either by the number of different technologies, geographic scale, or time latency – is far beyond anything deployed in the Cold War. Some methodology is needed that gets its arms around this complexity. This isn't only for acquisition purposes. It is also for fundamental reasons of civilian control of the military. Absent some larger framework that is above the technologies themselves, political leaders will be in the dark about what programs they are approving.

The purpose of a value chain is to organize the complexity. It is worth underscoring two points about this complexity. Complexity that isn't understood gives power to specialization. This can be fatal for true civilian control. There are many cases where these issues are discussed while overlooking the big picture challenges of the emergence of the new technologies.

Second, advanced technologies now are spilling over into the

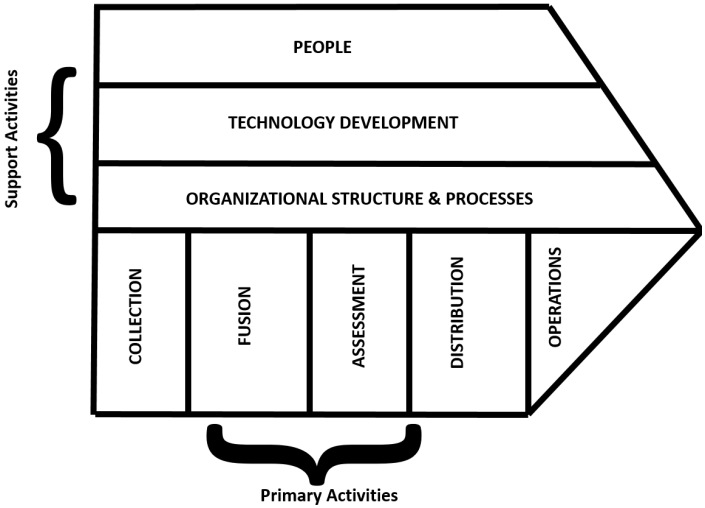
nuclear arena. Every major nuclear power in the world today has a modernization program underway (United States, China, Russia, India). These forces are linked to anti-command structure attacks, ASAT, and increasingly automated responses. Understanding how these forces interact with one another is one of the most important questions of our time.[63]

An unavoidable question in any complex enterprise is how to organize the many different activities that go into it, and how to align it with overall strategy. Specific questions here include: How should information be structured so that efficient operations and rational investments can be made for the "next" organization? What new technologies should be adopted and when?

The central idea of the value chain is that any business needs to be broken down into smaller, understandable, more manageable activities. These activities are linked one to the other in some logical order. For example, the hunt for mobile missiles requires finding the target, and this logically precedes the act of destroying it. The "finding" activity further involves different search activities, like drones, satellite tracking, cyber hacks, etc. The "killing" activity involves aircraft, cruise or hypersonic missiles, or cyber attacks. These are linked in a value chain to the finding process.

An illustrative example value chain for this is shown in the following diagram.

63 This point is the covered in Paul Bracken, "Nuclear Command and Control in a Multipolar World: Big Structures and Large Processes," *Orbis* (forthcoming).



As there are five primary activities: collection of information from reconnaissance various technologies, fusion of this data from several sources (e.g., drone video, cell phone and security cameras), assessment of the information, distribution of information to commanders and weapons, and finally operations. It should be emphasized that operations could also mean increasing one's military posture to a higher readiness level (e.g., moving strike forces closer to the target). Operations could also include political declarations to convey a message or send a signal. The operations, then, could be deterrence, increased readiness, or political signaling.

Value chains also include support activities because they are so important. These secondary activities are indirectly linked to the execution of the mission, but they are essential for its success. They consist of having the right people in the organization, those who are competent and trained. They would also include things like drawing from an innovation base of national or international technology.

North Korea's technology development drew upon Chinese and Russian sources, as well as commercial firms.

Organizational structures and processes are also relevant. This would include intelligence collected by allies. As an example of changes in organizational structure, the 2017 creation of the U.S. Cyber Command as a specified command system was an important change.

Every complex military enterprise has a value chain. North Korea's nuclear forces are an example. It has a more simplified nuclear value chain than the United States or other major powers. Its "collection" system gives it warning of attack. We know from several sources that this consists of agents placed in Seoul. Also, it consists of the information gathered from international news organizations. In 2007 Pyongyang tested a missile, launched moments after a launch of the U.S. space shuttle in Florida. This operation was linked to the U.S. test. The close timing of the North Korean launch signaled that it could get a missile off before a U.S. attack could hit targets in North Korea. I would describe this value chain as a demonstration of North Korea's launch-on-warning capability.

It is worth making several points about finding mobile targets for major powers like the United States and China. These points apply to finding land-based mobile missiles, ships, aircraft, and submarines. The technologies for finding these targets will differ, of course. But there are some general developments that characterize the value chain for all of these missions.

First, the value chain shown above is being digitized. Wherever possible, formal computer linkages and information chains are handling more and more of the work. Manual processes are being

replaced with digital ones. This is very important because it allows other, new information-processing technologies to be brought to bear on the mission such as AI, data analytics, and deep learning.

Digitization means that storage of the data about target location and movement is becoming cheaper and faster because of Cloud technology. Data which in the past would have been filed into separate organizational silos is now combined in one place – the Cloud -- to give an overall picture of the environment. It can be updated with very low latency compared to manual processes. There are other implications that follow from digitization, and these are significant because the emerging arms race now consists as much in this information-processing area as it does in the number of weapons themselves.

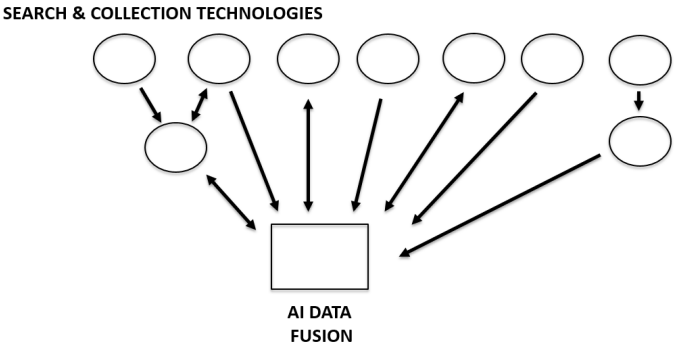
A second significant development is that military value chains are becoming much more tightly coupled. Perturbations are transmitted horizontally through information chains far more quickly. The systems are becoming more reactive. Nuclear forces in the Cold War were moving in this direction. This was because of the short warning times for the collection sensors like satellite early warning and underwater sensor grids. But this trend much longer times that what is shaping up now. The difference is that information-processing technologies using AI, data analytics, and deep learning are going to be more quick reacting and tightly integrated in the primary activities of the value chain.

Primary Activities in the Hunt for Mobile Missiles

The focus here is on the primary activities in the hunt for mobile missiles. To tie the value chain into our earlier discussion of search and collection activities, it should be understood that the "value" in

the value chain is achieved from the integration and correlation of the data collected from the various touchpoints. Tracking cell phones of crew members in the missile force is one thing. Correlating it with drone video and satellite imagery gives an altogether more reliable indication of location.

The first two elements in the primary activity value chain would be collection and fusion. A graphic indication of these elements is shown in the figure below.



The circles in this figure correspond to the various touchpoints. The solid lines with arrows are information chains. And the fusion part of the value chain is drawn to emphasize the critical importance of AI technologies. AI responds to changes in the external environment, (e.g., North Korea disperses some nuclear missiles or increases readiness levels, or there is a partial call-up of specialists and crew in preparation for dispersal). Here, the "finder" builds a reactive system that can dispatch additional search effort and increase its own readiness level.

The solid lines in the diagram are information chains. These are the big data "pipes" of the value chain. Noteworthy here is that these data flows handle a large variety of data. This, too, is an enormous change from the Cold War. Then, reconnaissance was all about photographs, intercepts, and radar. The variety of reconnaissance data today is staggering: images, text, optical signals, social media, email, video, and facial recognition are all part of the collection. All of these are digital bits consisting of 0's and 1's. This is another difference from the Cold War, when collection was analog.

There are other differences with the Cold War that are useful for contemplating the new world we are in. For example, it is often said that "the world is analog, while collection intelligence is digital." The intent of this statement is a warning. We are collecting a lot more information today, and it is digital. Yet, ultimately, it doesn't describe the reality of the real world – which is analog. It includes people, subtle distinctions, and cognitive features which are analog, not digital. The strong and unrecognized bias toward digital descriptions may lead us to overlook or deemphasize other kinds of important information from psychology, politics, and mass behavior. Analysis of this important point would take us beyond the scope of the present study. But it isn't hard to see that it may be critical for maintaining stability.

Several additional insights come out of this framework for analyzing the hunt for mobile missiles. First, not all of the search and collection technologies are likely to prove feasible or necessary. The hunt for mobile missiles doesn't depend on success across all fronts. For this reason, only 9 circles are drawn compared to the twenty touchpoints listed earlier.

A second point is that using multiple, independent reconnaissance technologies controlled by AI offers an entirely different way to think about mobile missiles. Most studies have focused on the search for "the" breakthrough technology, for example, one that can see through clouds or look underground. This is unlikely to ever develop. It reveals as much as anything else a bygone world of "super" technologies, rather than the integration-driven processes of AI.

Finally, the value chain also illustrates the importance of big data. It is only in recent years that data bases have been able to handle the vast amount of information collected in real time. The U.S. Office of Personnel Management hack in 2015 led to the loss of 20 million records. This is quite "small." For a country like North Korea or Pakistan, perhaps 20,000 people might be involved in the missile program, to include the crews, supporting staff, guards, custodians, etc. This is an easily managed scale for today's big data analytics.

The next link in a value chain in the hunt for mobile missiles is assessment. In any military operation, there is going to be assessment of the formal system by senior leadership. Leadership here refers to senior officers and political authorities responsible for national security. It is possible that this assessment function could be taken on by AI-automated systems. It is also possible that there could be splits in judgement, so that assessment of events could be contested. This is hardly new. The Cuban missile crisis saw deep splits in assessment of the situation in Cuba. The key point here is that there is nearly always an assessment element in any complex military operation. It is possible for this assessment to become thoroughly

routinized from long-standing practices.[64] It is also possible for assessment to be biased in various ways, such as groupthink.[65] Our only argument is that there is an assessment process of some kind.

An unremarked feature of the Cold War was when a situation had anything to do with potential nuclear operations the president was put into the value chain. The U-2 reconnaissance aircraft was developed to be used by the Air Force to take overhead photographs inside the Soviet border. Its purpose was to get a better estimate of the size and deployment locations of Soviet nuclear forces. However, President Eisenhower intervened in this collection process. He insisted that the CIA control the U-2 program, and more, demanded that he approve each overflight.[66] One reason for this was to manage the risks of getting the U-2 shot down by having a final civilian review the dangers. But another reason was to ensure that an overflight wouldn't take place at a politically sensitive time. Only the president could decide this.[67]

Some kind of senior political level intervention into the value chain is necessary. Otherwise, standard operating procedures (Steinbruner), groupthink errors (Janis) or, in the future, AI, could mishandle

64 This is the core argument in John D. Steinbruner, *The Cybernetic Theory of Decision, New Dimensions of Political Analysis* (Princeton: Princeton University Press, 1974).

65 For groupthink, see Irving L. Janis, *Victims of Groupthink: Psychological Studies of Foreign Policy Decisions and Fiascos* (Boston: Houghton Mifflin, 1972).

66 Wolfgang W. E. Samuel, *Silent Warriors, Incredible Courage: The Declassified Stories of Cold War Reconnaissance Flights and the Men Who Flew Them* (Jackson, MS: University of Mississippi, 2019), p.

67 Ironically, this control failed when a U-2 was downed over Soviet territory in May 1960 as President Eisenhower was set to travel to Geneva for a meeting with Soviet leaders. The result of this debacle was that Eisenhower canceled U-2 flights over the Soviet Union altogether.

the situation. The assessment element received a great deal of think tank and scholarly attention in the Cold War. It needs to be looked at again. This is for the obvious reason that errors here are particularly serious. But it is also because of "new" issues. Nuclear multipolarity has increased the number of nuclear decision-making centers compared to the Cold War. And technology has tightened the value chain of nuclear operations. For both of these reasons, the academic studies of the Cold War need a review and updating.

The last two elements of the value chain, on the right side of the above figure, are distribution of the information and operations. These are critically important and extremely sensitive. At the most basic level, distribution of information with today's technology means that the location of enemy missiles will be given to strike forces. Otherwise, the information is useless. In the past this occurred using manual processes and through layered hierarchies. This produced additional reviews -- and it produced time delays. These delays may not have been long, but certainly they tended to days, as in the Cuban crisis. These circuit breaker delays are no longer as apparent with automated alerting and response systems.

The reason for having a mobile missile force is to move it around so the enemy can't find it. This introduces lots of problems for the hider. Target assignments may change as the missiles move about, and their range coverage will vary. This also means that anyone tracking these missiles needs to have the relevant data linked to weapons whose job it is to hit them. What this means, in turn, is a continuous updating of targeting computers in the weapons. There's a kind of real-time coevolution between the two systems. This is an example of the general trend noted by Nazli Choucri and David Clark in their recent study of international relations in the cyber

age.[68]

There is a history of intelligence never distributed to those who could have used it. This is the story of Pearl Harbor. In the Pueblo crisis of 1968, the location of the U.S. intelligence ship was tightly held inside the Navy. No one else in the Navy or the Air Force was told to monitor its location or condition. As a result, when the Pueblo was seized by North Korea, there were no ready alert forces that could be launched to defend Pueblo, or to attack the North Korean forces who hijacked it. Interestingly, the U.S. alert aircraft in the area had nuclear bomb racks installed, and President Johnson decided against sending them on this mission. It took 24 hours to find ready non-nuclear weapon carrying aircraft, and by this time it was too late.

The broader point here is how tightly linked the entire value chain is. Different countries will come up with different answers to suit their needs and their tastes. Alert conditions will impact all of the links in the chain. With the addition of cyber, hypersonic, stealth, and other forces, it becomes necessary to distribute this information because the reaction times are so short. Also, there are bureaucratic issues here that could interfere with operations. Broadly speaking, the military would prefer to distribute this information in real time, and to have controls on the system built in for political override of these increasingly automatic processes. Civilians may not really be in charge because they lack knowledge of the intricacies of these systems. Alternatively, there may be breakdowns in the process that no one has ever thought of before (as happened in the Pueblo case).

68 Choucri and Clark, *International Relations in the Cyber Age, op cit*.

In sum, every nuclear power is now building a set of collection technologies and linking them to the forces. Some of these are "tight" and some are "loose." Value chains are a useful analytic tool to look at this phenomenon across many countries. Value chains in security studies are new, but they offer great promise to help leaders and their staffs, and analysts think through where technology is taking us.

Part IV

MOBILE MISSILES AND THE NEW ARMS RACE

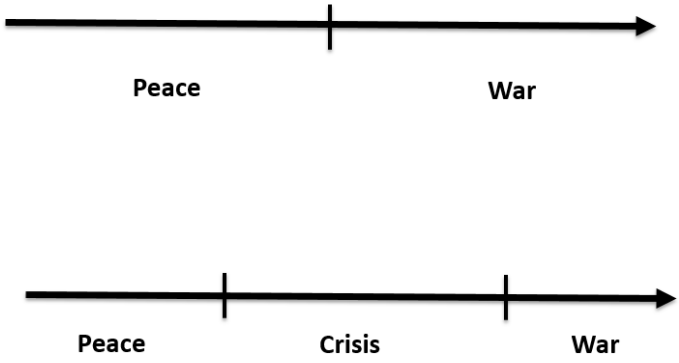
We now turn to the importance and impact of mobile missiles on the international security situation. This subject is divided into two parts: tactics and strategic. Roughly speaking, tactical issues covers how mobile missiles impact relatively short time interactions -- such as surprise attack, crises, alerts, dispersals, and escalation control. These would typically take place over hours, and days to perhaps a few weeks. Strategic issues describe longer term developments such as the arms race and its hazards, innovation, and ways that advanced technologies could spill into the nuclear aspects of long term rivalry. These strategic issues would extend over many years and quite likely decades. Use of the term "tactics" is not intended to convey lack of relative importance, as in "strategy and tactics." Instead, it is closer in its meaning to crisis interactions that arise from the technologies involved, missiles and reconnaissance.

Tactics Related to Mobile Missles in a Crisis

Mobile missiles introduce new issues into many aspects of crisis stability and crisis management: surprise attack, crisis management, alerts, dispersals, escalation control, and political signaling. This has been a pattern in the nuclear age going back to the late 1940s. Certain new technologies come into being – bombers, ICBMs, SLBMs, tactical nuclear weapons, satellites – and they change the incentives for different kinds of actions. National strategies can be based on this. For example, for much of the Cold War the United States sought to drive the Soviet force to sea, that is, to encourage Moscow to put more warheads on its submarines and fewer on its ICBMs. The study of this kind of interaction has fallen out of favor in recent years and this is probably unfortunate.

It should be emphasized that no one is suggesting or recommending the tactics described here. This study is not meant to be a military plan. Rather, the purpose here is to get certain issues on the table for further analysis – namely, those that follow from the shift to mobile missiles that has taken place in much of the world, and at the same time, the greater ability to track these missiles.

The interaction of a mobile missile dispersal with enemy intelligence can lead to some precarious dynamics. In order to understand how this could happen, we need to go beyond the simplified view of nuclear operations that guides much of the public discussion. This view is shown in the top part of following figure.



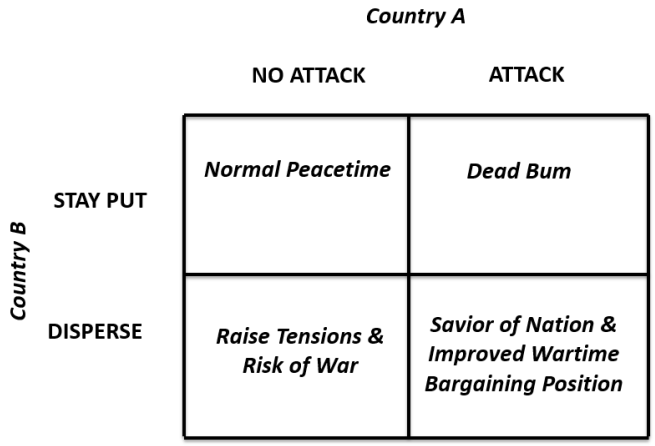
In much discussion about nuclear war the top picture is advanced to describe the situation. Country A builds up a capability to destroy Country B's nuclear forces to a degree that it removes B's ability to retaliate. If B has mobile missiles, A must track them. Once A has done this to a sufficient degree, a situation of crisis instability arises, the upper time line in the figure.

While this may describe certain situations, it by no means covers all of them – or even the most likely ones. No one believes that nuclear war is just another type of military action. Even North Korea, to take what is perhaps an extreme example, surely understands that it faces national destruction if it gets into a nuclear war.

A situation where posturing, alerts, and low-level moves is much more likely to describe actual crises. I would venture to say that over 90 percent of analysts who have seriously studied nuclear operations agree with this statement. So, here, the question becomes: How do mobile missiles play in a crisis?

Ordering dispersal of a nuclear mobile missile force is an extraordinary decision. It has never occurred, either in the Cold War or now, in a second nuclear age. It will be the most significant, provocative decision a leader ever makes. It has never been studied in any detail to include the new technology of mobile missiles and reconnaissance systems.

Consider the different aspects of the decision using the same abstract model used above of two countries, A and B. In the event of tensions, Country B would like to reduce the vulnerability of its nuclear force. If it does nothing and Country A builds up it strike capability, it will become a sitting duck for a disarming attack. It is important to understand this situation. Dispersing the missile reduces its vulnerability but the act of doing so is provocative and dangerous, because it could cause Country A to strike first. Yet, not dispersing has its own risks because it presents an ideal target to Country A. In B's thinking, even if A has no intention of attacking, its bolstered strike capability plus B "bunched" atomic warheads in soft storage areas may cause A to change its mind. This is very different from Cold War crises for several reasons. First, A can launch a conventional counterforce attack that doesn't include nuclear weapons. That way, there will be relatively little collateral damage. A second difference is that in today's world, A and B may not be two risk-avoiding mature superpowers, as in the Cold War. Any combination of major and secondary powers could constitute the two countries. Consider the United States and North Korea. The stakes and cultures involved here are so different than the Cold War as to make it pale in comparison. The closest analogy would be the Cuban missile crisis – if Fidel Castro and Che Guevara had nuclear weapons of their own.



Finally, something that is possible now is that a third party may enter the conflict to finish off the loser, or to take advantage of the crisis in a variety of other ways. The United States or China is unlikely to stand back from a crisis that turns into war on the Korean peninsula.

The decision of country B to disperse its mobile missiles is closest to the United States decision of an emergency launch of its nuclear bombers to make them less vulnerable in the Cold War. This never happened at any time in the Cold War by either side. It was far too provocative and risky. But it may not appear so in the new world of mobile nuclear missiles – and many countries facing this decision.

The dynamics of these interactions are complicated, but they may be summarized in the following matrix. Here, Country B has two choices. It can keep its missiles in peacetime storage positions – "Stay Put." Or it can order a dispersal of its mobile missiles – "Disperse." If B stays put and there is no attack, this is the normal peacetime posture. But if B stays put and there is an attack by A,

then the leader making this call is likely to be a dead bum. He's a leader who miscalculated, and whose nuclear deterrent power was destroyed.

If B does disperse and there is no attack, he has raised tensions enormously and increased the risk of war. He has done this because the chance of an accidental launch is much greater, and also because A interprets the dispersal as a preparation for attack. Given this, he's got little to lose. A is better off trying to disrupt the attack of a dispersed force rather than holding back and accepting its full weight.

Given the range of actors for A and B (North Korea, India, China, the United States, Russia, Israel), and the need to disperse the missiles to use them, we really are in a different world than the Cold War.

But there's another aspect to all of this that has to be considered. Dispersal can be used for political signaling, and also for communication and bargaining. Suppose B disperses to show resolve, or to signal its intention to hard bargain in the crisis. It depends on who, really, A and B are. But the combinations and actions are daunting. It would seem to be reasonable to think that these tactics strengthen the power of a weaker state. Take the U.S.-North Korea case. Dispersal gives the United States more barraging leverage in a crisis, because North Korea can hold Japan and South Korea as hostages. If North Korea had an H-bomb-tipped ICBM able to reach the United States – which it shows every sign of getting – it has even more leverage.

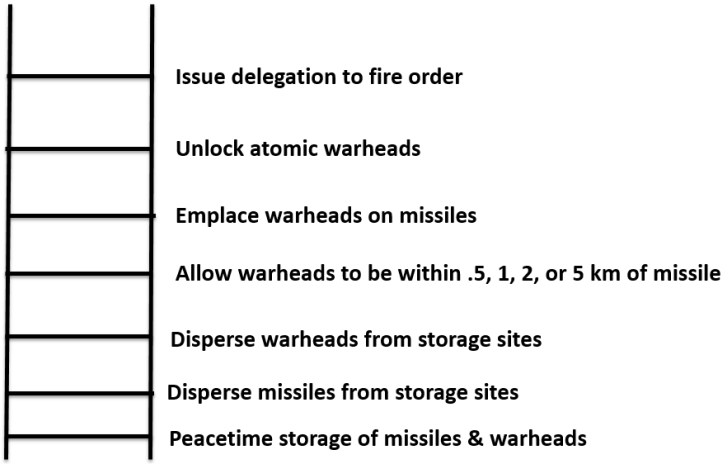
A country could disperse part or all of its missile force to frighten its enemy, or to get it to back down in some political dispute. This

is the world of signaling and nuclear head games that figured so prominently in the Cold War. Country B could go on partial alert to send a message: "this crisis is really getting dangerous, and if you're smart you will back down. Otherwise, I may be forced to take the next step on the escalation ladder." Head games like this were used throughout the Cold War. It defines the world of B-52 airborne alerts, provocative U-2 overflights, and spoofing attacks in unexpected locations. In the Cold War the search technologies were periodic. Over the next decade they are going to be continuous, and far more able to penetrate deep into the enemy command system.

It is useful to explore the dispersal decision a little more analytically because it is so important and so overlooked. Its importance lies in that it shifts the locus of nuclear dynamics to lower levels of the escalation ladder. In other words, it deals with the oft-stated view that "North Korea would never be crazy enough to launch a nuclear weapon because they know they would be destroyed immediately afterward." Even were this true, North Korea might well be crazy enough to disperse its nuclear missiles. In most crises, that's all they may need to do.

If North Korea were to order a dispersal of its missile force, there are many other choices it would also need to make. So far as I can determine, these choices have received little or no attention in government, academic, or think tank studies.

Consider the decisions that come with reliance on mobile missiles.



As described earlier, no country in the 21st century puts atomic warheads on its mobile missiles in peacetime. From peacetime storage locations, missile and warhead dispersal is over two separate tracks. One involves missile dispersal. This entails assembling a crew both for the missile, and also for reinforced headquarters and support operations. The signature for this could be large, and with the new collection technologies, it is going to be detected.

The second track is dispersal from protected storage of the atomic warheads themselves. Every country we know of, including going back to the early Cold War, has separated the warheads from carriers. It was only in the late 1950s and 1960s that the superpowers married their warheads to missiles on a day-to-day basis. And this was in their ICBM and SLBM forces. So, it seems unlikely that these two tracks would be merged early in a dispersal process. Far more likely is to keep them separate, and to emplace the warheads on the missiles deep into the alerting process. Otherwise, decision makers

lose substantial control over their force.

This means that there are two decisions. One is to disperse the missiles. The other is to disperse the warheads. When both have been dispersed, there is then the question of how physically close they are to each other. One way a country can reduce the chance of an accidental or unauthorized launch is to keep a safe distance between the warhead and missile. In the diagram, this is indicated by a formal rule: keep the warhead no closer than .5 km, or 1, 2, or 5 km distant. There's reason to believe that such rules are used by many of the "new" nuclear weapon states.

Exactly what this distance is will depend on a number of factors. But there is reason to believe that this is handled by specified "safe distances" between the two, distances which can be reduced if it looks like a war is going to occur. All of this, the two-track dispersal decisions and the safe distance specification, occurs in the crisis period in the above timeline. This is yet another reason to focus on this crisis period.

The next big decision is to emplace the warhead on the missile. For mobile missiles, this is likely to happen in the field, and it needs to occur when the missile is in the horizontal position. Otherwise one would need a cherry picker bucket truck to put the warhead on. This seems unreasonable for obvious reasons.

The next step is to send the code needed to unlock the warhead on the missile so that it can launch and detonate. These codes are likely to be tightly held in many countries.

The last step on the ladder diagram is to issue pre-delegation fire orders. These are the orders as to what happens in the event headquarters is

destroyed or if enemy fires interrupt communications between them and the field. It is certainly possible that a headquarters will not wish to give these out, for it raises the risk of accidental launch. But if such authority is not issued, then the enemy has a window of opportunity to fire against the command and control system, in the hope that field missile units won't launch.

There are additional dangerous steps on the escalation ladder. The force could be placed on negative control. This means that it should fire unless it receives a coded signal at periodic intervals, say once every two hours. But leaving these details aside, a broader point needs to be underscored.

All of the steps described above are touchpoints. They can be detected with the right technology. The probability of this goes up if there have been years of watching, studying, and analyzing the missile operations. The continuous interaction between hider and finder may take place in a short period of crisis time. But if it is to have any real chance of locating missiles and warhead, it must be based on years of collection and analysis. The finder needs to understand the hider in detail. The finder cannot throw certain collectors together – drones and cyber – and expect to find very much.

The central claim made here is that a new kind of operational entanglement and political signaling is being built. Much of the military and political dynamics around mobile missiles will occur in this region of the escalation ladder rather than the bolt from the blue attacks that dominate most analyses.

More, skilled maneuvering in this region, informed by restraint and guile, could provide major competitive advantage. Escalation to nuclear war looks likely to arise from poor performance in this part

of the escalation space. Most studies in the United States still focus on far higher levels of escalation, like all-out major conventional wars or nuclear exchanges. These studies overlook the obvious point that in today's world even conventional attacks occur in a nuclear context. This is the case in East Asia, South Asia, and in Europe.

Strategic Aspects of Mobile Missiles

Strategic aspects of mobile missiles cover longer term problems associated with advanced reconnaissance technologies and moving targets. But there is a larger change in the context of this topic. The United States after World War II saw itself in a position of technological primacy in both war and business. Measured by Nobel prizes, university leadership in STEM topics, government support of research, and business dominance of aerospace, computing, and communications there was no other player close to the United States. The Soviet Union, which challenged American leadership in space, was considered so odious that while Moscow was certainly a rival, it was not one that anyone wanted to copy.

The technology of the post-war period -- jet aircraft, the transistor, integrated circuits, computers, lasers, and satellites -- showed U.S. primacy in a highly visible way. U.S. universities were the envy of the world, as was American science more generally.

Technological primacy was key to the Cold War because it allowed the United States to win that competition without turning into a garrison state like the Soviet Union. Simply to give one example of this, the United States never had more than 18 Army divisions throughout the Cold War. The Soviet Union, in contrast, had 150 – 200 divisions in peacetime. This situation came about because of a substitution of capital, in the form of technology, for labor. It was a

truly extraordinary development.

After the Cold War, technology gave the United States "splendid" military victories in the two Gulf wars. These campaigns saw almost no U.S. casualties in their opening phases. Moreover, American companies like Apple, Google, Facebook and others dominated new industries.

It has come as a shock in the United States to see developments that negate this primacy. Only in the 2010s has this realization taken hold in the educated public, business, and Congress.

Two examples where the assumption of American primacy has been undermined are worth naming. First, the rise of China to become a technologically advanced nation has shown that there is no permanent monopoly on U.S. technology primacy. China's rise was welcomed for decades by the United States. The fielding of mobile missiles in China, advanced command and control, and other technology intensive systems in the 2000s was not seen as especially troubling, at least outside of the Pentagon. By the 2010s, U.S. attitudes shifted. China's ability to track U.S. ships in the western Pacific, and to target them with land-based missiles, raised profound issues. The question became, Could the military balance in the Pacific and East Asia be changing? It is fair to say that most assessments of this question were in the affirmative. China might not win a war with the United States but China was surely building an impressive counterforce strike capability against U.S. bases and ships.

China's move into business with AI, AVs, and 5G telecoms showed that China was not a narrow military power, like the Soviet Union had been. It was a serious technologically advanced state that did

not accept U.S. leadership in international relations or in business. Before these developments, the question in Washington was whether U.S. technological advantage was eroding. Now, the question isn't about the United States falling behind; rather, it is about whether the U.S. can ever regain a position of technological primacy.

What does this appreciation of the technological situation mean for arms races? The answer is a great deal. The United States is trying to catch up not in a narrow military way with China and others – to track its missiles facing Taiwan and Japan. Rather it is trying to prove itself as being the dominant player in technology, both to China and to many others.

This challenge involves a sense of who we are as a nation, and how we can improve to regain technological superiority. The United States is now in an arms race to prove this point. This willingness to engage in an arms race demonstrates a commitment. Moreover, Congress, the educated public, and those benefiting from Washington's largess from increased funding for technology are likely to go along with this sentiment. The United States prides itself on its technological successes -- the Panama Canal, the national highway system, the moon landing, and victory in the Cold War. Big technology is a deep element of the American experience.

It is in this context that an emerging arms race needs to be viewed. Some countries, in particular the United States and China, are out to prove something that goes beyond mere political-military objectives. There are higher objectives than these. This perspective, to the extent that it is correct, has an important policy implication. The question may not be how to prevent an arms race; rather, it a question of how best to contend in an arms race, if we must. This question includes

ways to dampen the most dangerous features of an arms race, and ways to channel it that are likely to produce some level of restraint.

In addition to national character and mood factors driving technological investment, there are distinct "new" features of an arms race today that are important. The study of arms races has virtually disappeared since the end of the Cold War. For this reason, many features of emerging great power rivalry haven't received the attention from an arms race perspective. They are important because new kinds of arms races are shaping up, and there is little appreciation of them.

Arms races need to be better understood if we are to advance the public policy debate beyond the usual banal calls against armaments. It is all very well to decry the militarization of the heavens and robot weapons. Doing so draws attention to the problem. It shows that one's heart is in the right place but it doesn't really get at the heart of the problem -- because we don't yet know what this heart is. We are groping in the dark at the beginning of a new technological era, a second nuclear age, and at the same time, a rapidly changing international order. Many people turn to low-resolution descriptions taken from history to describe our world. There are calls to prevent another arms race, or to claim that no one wins an arms race. Yet, the situation is more complicated than this.

We don't understand this new world, just as decision makers and analysts didn't understand their worlds in 1914 or 1948. But these two cases are different. In 1948, people tried to grapple with the first nuclear age. I would assert that these efforts were successful in dampening the arms race that followed -- compared to what it could have developed into in the absence of a higher level perspective.

What is offered here isn't a blueprint of what our world will look like; it is an exploration of certain of its features, with the hunt for mobile missiles as an exemplar of where things are going.

The "New" Arms Race

Arms races involving technology began with the industrial revolution. Technology was an important source of advantage in peace and war. In peacetime, industrial capacity measured the war potential of a nation. In war, production of armaments proved to be critical in World Wars I and II and in the Cold War.

Although these dimensions of competition are still present in the international system, there are some new elements as well. Thus, the italics in this subheading. One element of arms races today is that they are highly segmented relative to earlier arms competitions.

Investments are not made in all technologies, but rather in certain technologies. More precisely, and using one of the arguments of this report, investments are made not so much in weapons – missiles, bombs, satellites, cyber – as they are in value chains. For example, the United States and China are engaged in a military competition. But it's less about numbers of weapons than it is about value chains. China is constructing a complex anti-access system that is best thought of in terms of a value chain for limiting U.S. military presence in the western Pacific. The United States, in turn, is building a counter value chain to this anti-access system.

A value chain description could be offered for the United States and Russia as well. Or it could describe the rivalry between India and Pakistan. India has shown it has much greater technological capability in its demonstration of ASAT and in the commercial

IT sectors. Also, Delhi's various "Cold Start" strategies rests on building a conventional value chain and tightly integrating it with quick reaction alert (QRA) forces.

Nonetheless, within these value chains, there are "segmented" technologies. Segmentation is the process of dividing technologies into different groups. Certain technology segments are especially important. Technology segments often develop their own bureaucratic dynamics, generally to prefer one technology over another. Even critical complementary technologies may be excluded or overlooked because of this. The battleship arms race between Germany and Britain in the early 20th century is an example. It emphasized the large battleship rather than submarines or aerial reconnaissance for spotting enemy battleships. These came only after the war had started.

In the Cold War, likewise, there was a "segmented" nuclear arms race at various times, one that led to grotesque numbers of these weapons on both sides. The point is that arms races may go off into their own self-contained techno-bureaucratic worlds for certain segments, as battleships and nuclear weapons did. Today, it would seem that cyberwar and AI are fulfilling this role in the emergent arms races.

Another key point is that in a multipolar world advanced technology is available to many countries, not just two superpowers, and not just to major powers. North Korea has an H-bomb with some not implausible ability to reach the United States. This really is a "new" feature of arms races. At no other time in history have major powers lost their monopoly over advanced military technologies. This is now clearly the case, and it has important implications.

One of the most important of these is that advanced technology has served to heterogenize arms races. The common view of a one-size-fits-all model for an arms race is unlikely to describe future competitions. This model is founded on the Cold War nuclear competition between the United States and the Soviet Union. It developed into a model for both restraint (arms control) and advantage (the Reagan military buildup). The technology positions and politics today simply don't adhere to such a homogenized view. North Korea's situation and technology are simply too different from India or Russia's or Israel's. So, in the future there are likely to be a much wider range of arms races between more countries, measured by investments, technologies, and value chains.

One very important question here is related to the hunt for mobile missiles. It is the degree to which major powers will emphasize the finding of moving targets. The answer ranges from "not at all" to an "all-out emphasize." Clearly, the not- at-all answer doesn't describe the many activities taking place in this area. On the other hand, the all-out emphasis has its own problems. If the United States were to declare that it was making an all-out effort to track the mobile nuclear forces of China and Russia, the chance of a nuclear arms race would go up to near certain levels. The United States doesn't wish for this to happen.

The exclusion of the extreme answers points to an important conclusion. That is, that the hunt for mobile missiles isn't an all-or-nothing activity. It is a continuous spectrum, not a binary variable.

This spectrum describes some really important policy issues. If the United States decides to the left of the spectrum, the "not at all" side, then barring a surprise in negotiations with Pyongyang, Washington

is making a de facto decision to accept a "MAD" nuclear relationship with North Korea -- that is, both sides would be capable of inflicting unacceptable nuclear damage on the other. This, I would argue would bring us into a new global order, one where any U.S. activity in East Asia and the western Pacific is greatly hamstrung.

Alternatively, if Washington decides for an all-out program to hunt North Korea's mobile missiles, there are also many strategic consequences. One is that China and Russia will be threatened by this, as the same reconnaissance technologies may be aimed against their mobile forces. They are likely to have their own responses.

The policy community in the United States needs to think all of this through. At present the United States is moving in a direction to emphasize the search for mobile missiles – but this bottom up approach needs strategic direction from the top.

The Coevolution of Nuclear Weapons and Reconnaissance

The employment of nuclear weapons was always limited by reconnaissance. In the Cold War it was slow, costly, and inadequate. Only fixed targets were easily found, like missile silos, or air bases with bombers on them, or submarines in port, and these became vulnerable only in the latter part of the Cold War.

This continued into the 21st century. It began to change with the new technology of cameras, mobile phones, cube satellites, drones, big data, AI, etc. These technologies could be organized into an integrated value chain for tracking mobile targets.

The main point is that the Cold War nuclear arsenals grew because the other side's arsenals did. This was the overwhelming reason, although domestic politics played a part. The nuclear situation is

different now. The ability to hunt mobile missiles is getting faster, cheaper, and better.

What this means is that nuclear arms races are not driven by additional missiles of the other side but, rather, because reconnaissance technologies are getting better. The coevolution of nuclear arsenals in the Cold War was driven by the other side's missiles – and politics. Now it will be driven by the coevolution of missiles and reconnaissance.

Coevolution is one of the exciting new frameworks of the social sciences. In technology, it is now clear that one of the drivers in digital innovation is a coevolution of software and hardware. The view that it is driven by Moore's Law alone, a hardware feature, is incomplete. In AI there is a similar development. The algorithms behind AI have shifted from purely logical deductions to ones that improve their performance based on data taken from large samples of facts in the world. This is what is behind neural nets and deep learning.[69] AI coevolution is now between the algorithms and the world.

This leads to a different way to look at nuclear weapons, arms races, and arms control. Consider that academic deterrence theory has no variable in any of its models to represent reconnaissance. There are institutions that count the nuclear weapons in exquisite detail (CIA, SIPRI, IISS, many specialized think tanks) with no consideration for how reconnaissance improvements impel others to increase their nuclear forces to offset them.

69 See Kai-Fu Lee, *AI Superpowers, China, Silicon Valley, and the New World Order* (New York: Houghton Mifflin Harcourt, 2018), pp. 6-8.

This coevolution matters for strategy as well. The United States has been attempting for a long time to counter the larger forces of other countries with technology. Technology "offsets" force structure. But there are kinds of important offsets missed by this. One is that North Korea (Pakistan) can offset U.S. (Indian) reconnaissance improvements with more mobile nuclear missiles. The hopes of many that the new nuclear states will somehow embrace minimum deterrent strategies may be unrealistic because of these technologies.

Process Innovation

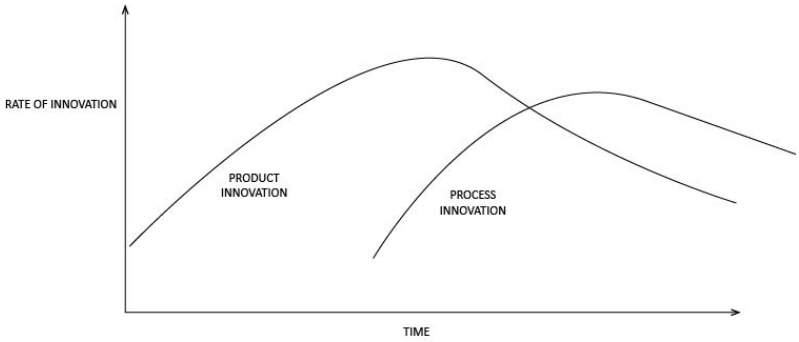
Much of the new arms race will be in process improvements rather than in the number of weapons, or the features of these weapons. A process is defined as a flow of work or information. Much of the technology revolution in business in the past decade has taken the form of process innovations.

Think of Disney World. It's a theme park, of course. But it's also a giant, hi-tech process machine. Visitors are directed to park their cars, buy tickets, wait in line, schedule a ride, dine, and check in to their hotel all through carefully designed processes. Disney's "digital transformation" is all about optimizing these processes, more than it's about using technology to build a better ride.

The militaries of China, Russia, and the United States over the last decade are also built on processes. Collecting information, organizing it, translating it, decrypting it, and getting it to users. These information chains are what provide the day to day tracking of enemy targets of all kinds. Optimizing these processes is a lot more important than acquiring one more missile or F-35 airplane.

A great deal of research has been done on process innovation in

economics and in business schools.[70] One of the most interesting findings of this work is the difference between product and process innovation, and the relationship between them. Across a very wide set of industries, from automobiles to retail to high tech, there's a consistent pattern.[71] Most innovations at first center on product improvements. When these top out, the innovation shifts to process innovation. This relationship is shown in the following diagram.



70 See Richard A. Goodman and Michael W. Lawless, *Technology and Strategy, Conceptual Models an Diagnostics* (Oxford University Press, 1994); C.K Prahalad and M.S. Krishnan, *The New Age of Innovation, Driving Cocreated Value Through Global Networks* (McGraw Hill, 2008); David J. Teece, *Managing Intellectual Capital: Organizational, Strategic, and Policy Dimensions* (Oxford University Press, 2000).

71 James M. Utterback, *Mastering the Dynamics of innovation* (Harvard Business School Press, 1996).

This is what is now happening in military technology. For this reason, it offers insights into what an the arms race in AI, cyber, deep learning, etc. may look like. It says a great deal about the hunt for mobile missiles as well. First, let's understand how this applies to military technology.

Consider the cruise missile. This was a "product innovation" developed in the 1970s. The cruise missile offered a way to attack the enemy with "pilotless aircraft." Through the 1980s and 1990s this "product" was improved. Terrain matching radars were put in the missile to guide it to its target. Then GPS guidance made it even more accurate. Other improvements made the missile more reliable. By the early 2000s there was not much more that could be done to make U.S. cruise missiles better. They were so accurate at this point that it made little economic sense to invest in technologies that would buy another 1-2 meters of accuracy.

The problem, however, was that when a target was found, say in Afghanistan, it took 24-48 hours to land a missile on that target. This was because of the bureaucracy associated with targeting: reviews back in Washington for collateral damage, and getting authorization if the target was located near civilian areas. The result was that, by the time the missile was fired, the target had fled. Or, the target moved, unaware that it even was a potential target. The enemy soon learned that the best way to avoid American missile attack was to move frequently.

The solution that came out of this was an improved process. Simple changes in information flows and automated reviews drawing on data bases of sensitive facilities were instituted. The review process was streamlined. The result was that the time between target location

and firing went from 24-48 hours to 1 hour or less. This was a game changer. It made the cruise missile far more useful, a lot more useful than improved accuracy, or buying 100 additional missiles.

From a higher level perspective, this case shows the declining benefit from product improvement (the weapon) and the rising performance of a process improvement. Achieving more accuracy, and incorporating a bigger warhead hadn't given improved performance. The locus of innovation shifted from product to processes.

In many defense technology areas, the locus of innovation is undergoing the same shift. The process technologies are AI, data analytics, deep learning, information chains, edge computing, and Cloud storage. This applies to the hunt for mobile missiles with special relevance. Because the really big payoff for finding mobile missiles is going to come from process improvements: digitizing and tightening the value chain, search and collection with information chains, and Cloud innovation are the high payoff areas. At the same time, it means that 5G technologies, power, transportation, and financial system vulnerabilities can be attacked through better processes: algorithms, deep learning, AI, and hacks.

The next arms race is going to be a process-intensive arms race. It's unlikely to produce the huge nuclear arsenals of the Cold War, or the fantastic force structures of 200+ divisions of the Soviet Union. This offers a different way to understand arms races: rather than weapons, it's about processes. It means radical changes in the military acquisition system.

Conclusions

Most advanced technology for national security has its origin in bottom up rather than top down needs. It is driven by operational rather than strategic considerations. The need to track terrorists after 9/11, to disrupt uranium enrichment in Iran, counterinsurgency in Iraq and Afghanistan, and to interfere with North Korea's missile tests -- all of these "felt needs" have produced colossal innovation.

Top-down innovation is rare. The original atomic bomb project is an example of it. Without U.S. government support, and the backing by President Roosevelt, it would not have come into being during World War II. There are other top-down technologies as well. The decision to build a hydrogen bomb by President Truman, the ICBM program of the 1950s, Sputnik, and the moon landing are examples.

But most new technologies are not like this. There was no clear recognition or support for Panzer forces in Germany. Hitler had nothing to do with their development until years into his rule. Army officers and technological visionaries saw where armored forces could go if developed in the right way. But they had to push the innovation of tank units from the bottom up.

One feature of bottom-up programs is that their long-term consequences are rarely foreseen. This is understandable. People focus on felt needs, the problems of the time. They don't think about other things. Henry Ford said that, if he had asked people what they wanted, they would've asked for "a faster horse." The operational mindset of the military today reflects this mentality. It looks to solve the pressing problem, whether catching terrorists or finding missiles. It isn't in the nature of people to anticipate enlarged uses of technology.

No one saw the consequences of the laser or the integrated circuit in the 1950s. However, this inability to foresee longer term consequences does not mean that new technologies are ignored. They are supported, and supported very well to solve local, immediate problems. In the United States the current wave of digital technologies is like this. After 9/11, driven by the demands of counterterrorism and counterinsurgency, government entered the picture to give them enormous financial backing. This investment from DoD and the intelligence community had immediate payoffs, like slowing down Iran's uranium enrichment or catching insurgents in the Middle East.

Most of these technologies -- hacking, cyberwar, facial recognition, search, cloud computing, and data analytics -- had been developed to a high level in commercial markets that had nothing to do with military uses. They were bottom up but originated in an entirely different market.

One difference between today's digital revolution and the Cold War is that today's technologies are much harder to monitor in terms of their capability. The Cold War deterrence forces took years to build and were highly visible from satellites, intercepts, and old fashion news gathering.

Now, the ability to track mobile missiles uses computer algorithms, vast data centers, cloud computing, and deep learning. The "work" of finding these missiles is done in secretive organizations. Taking a satellite picture tells you nothing about what is going on inside. There are ways to penetrate this world, using insiders, turncoats, and cyber espionage. And this, no doubt, will be a growth industry for decades to come. The mushrooming scale of intelligence around the

world is testament to this.

Another feature of today's digital technologies also stems from the fact that it is bottom up. Cold War civilian leaders did not need a degree in physics to understand the impact of nuclear weapons. Now, it's very difficult for anyone to anticipate where the technologies are leading. People with computer science PhD's are little better able to do this than a politician. This makes civilian control of the military a challenge. By civilian control, I mean shaping the next military enterprise so that it meets the needs of the national interest, but at the same time goes beyond to establish a system of order that isn't overloaded with risks arising from the very technologies that were built to improve the national interest.

The Cold War, again, is a good example. This rivalry could have led to Armageddon. The arms race could have been much more intense, and for this reason more dangerous than it actually was, but for choices made by the two superpowers that dampened it. No one put nuclear weapons in space, or tampered with warning satellites, or attacked nuclear command and control.

More fundamentally, at no time in the Cold War did either side ever seriously consider a calculated strike on the other. Nuclear war could have arisen from some other cause, of course, such as accident or misunderstanding.

But it isn't possible to say this today. Nuclear war is "thinkable" by North Korea, in South Asia, and in the Middle East. This is the environment we are in, and it's a very different one from the Cold War. The hunt for mobile missiles is an exemplar of this reality. The way mobile missiles are tracked is from deep learning of multiple data inputs linked in a value chain. Cloud computing,

cyber, data analytics, and other integrating technologies are linked to strike weapons. These new reconnaissance technologies spill over into nuclear rivalry because that's what the targets are, other people's nuclear missiles.

I offer this conclusion about spillover without offering ideas or strategies for preventing it. We are in a position akin to 1960. Writing then, Herman Kahn argued that the real purpose of arms control was to "buy time," even though no one really knew what to do with this extra time. The arms race had "super-sized" H-bombs, ICBMs, jet bombers, and nuclear submarines. If this technology evolution was projected ten or twenty years into the future, frightening and destabilizing possibilities looked highly plausible. What Kahn was saying was that people needed to step back from the present with all of its dangers to pause and take a broader perspective. It was to use a time of tremendous change to formulate a better strategy and for better thinking, even though in 1960 it looked as if there was no audience for it, or even ideas of how to use the extra time. Bringing the problem to the surface in this way was a useful step, because it spread appreciation of just how dangerous the arms race would get on its current path.

This is good advice today. We need to go beyond the narrow measures used to solve the felt problems of the day. There are far-reaching impacts of the new technology on the arms race, measures that go beyond the ability to accurately track North Korean missiles. For one thing, most of the "nuclear action" involving these missiles seems likely to involve complex nuclear head games of dispersal for political signaling. For another, the ability to track mobile missiles will have far-reaching implications for arms racing among the major powers with each other. China and Russia will notice U.S. innovations here,

as we have noted their innovations. Unless a broader, more sober view of the hunt for mobile missiles is taken, one that goes beyond narrow measures of performance, the world is going to see much more dangerous nuclear crises, as well as arm races that go beyond what is necessary for prudent security.

GLOSSARY

This report uses a number of concepts and terms from management theory, business school, and technology management research. Since many of these terms many not be familiar to students of political science, history, or other social studies approaches to defense studies, they are defined in this glossary for convenience and reference.

Advanced Technology - Technology packages made up of AI, machine learning, computer vision, drones, satellites, cloud and edge computing, signals intelligence, data analytics, phone hacks (e.g., StingRay), 5G, and security and traffic camera hacks, automated license plate readers, etc.

Artificial Intelligence (AI) - the science of making machines do things that would require intelligence if done by people.

Augmented Reality (AR) – interaction with a real-world reality where objects are enhanced by computer-generated perceptual information. AR does not replace sensory data like VR. It adds to the real-world sensory information to augment or enrich certain of its features. Example: filters on a camera network that highlight particular individuals or groups.

Autonomous Vehicle (AV) – a vehicle that senses its environment and operates with little or no human input.

Backdoor – access to a computer system that bypasses customary security mechanisms. Developers often create a backdoor so that an application can be serviced or updated or for troubleshooting purposes.

Beacons – low-energy radio transmitters that broadcast identifiers to nearby electronic devices (receivers). The signal triggers smartphones, tablets, and other devices to perform actions when in close range of a beacon (e.g., to track a phone's location, movement, or conversations picked up on its microphone). Beacons are cheap and widely used by business in retail, shopping malls, etc.

Big Data – a field that systematically extracts information from data sets that are too large or complex to be handled with traditional statistical software. Big data describes methods not only for very large data sets, but for real-time analysis, and for analysis of very different types of data. Example: real-time data fusion of drone video, security camera hacks, intercepts, and cell phone use in a mobile missile convoy.

Cloud Computing – refers to "always on," on-demand computer resources – data storage and computing power – without direct, active management by a user. It provides software, intelligence, and analytics over the web ("the Cloud") that is faster, cheaper, and more efficient than in-house mainframe computers.

Coevolution - the influence of closely associated technologies on each other and in their evolution. Each technology exerts selective pressures on the other, thereby affecting its evolution. Examples: missiles and reconnaissance technology.

Computer Vision - a field of AI that uses computers to recognize and understand images or videos.

Data Fusion – integrating multiple data sources to produce better assessments than that provided by any individual data source. Example: tracking a vehicle by monitoring the operator's cell phone

and fusing the hacked phone data with drone video of the truck's location, speed, and direction.

Data Poisoning – an adversary feeding misinformation to an AI system to corrupt, trick, or defeat it. Companies have developed sophisticated data poisoning strategies in finance, retail, and ride sharing to deceive regulators.

Digital Transformation – a nebulous term, but broadly speaking, using technology to remake processes or products.

Deep Learning – a part of machine learning that uses artificial neural nets. Deep learning is a key technology that allows drones with computer vision cameras to recognize a TEL or truck used to carry atomic warheads to mobile missiles.

Dominant Design - a design that is widely accepted by the market or governments, with important impact on the kinds of follow-on innovation. Military examples: the nuclear triad of ICBMs, bombers, and SLBMs; aircraft evolved through several dominant designs: biplanes, propeller driven aircraft, swept wing jets, stealth.

Edge Computing – computations on remote devices in the field with limited processing power, and not on a central server or a PC. The idea is to bring AI to traffic lights, security cameras, drones, or other gadgets without connectivity or extensive communications to a centralized server. For military use, edge computing offers stealth as it cuts down on communications, reducing the chance of detection. Examples of military edge computing: AI for target selection by armed drones, sensor nets operating in enemy territory, or cyber war modules implanted inside enemy computers or electric power grids.

Electromagnetic Pulse (EMP) - a super-energetic radio wave that destroys electronics over large geographic regions. EMP blinds satellites, radars, and other sensors, and can obliterate weapons and networks using computer chips. EMP could paralyze nuclear command and control. Over a 1- to 2-year time period, it could kill millions of people due to starvation, disease, and societal collapse.

Exemplar - a technological program or achievement that serves as an outstanding example of a strategic concept (Thomas Kuhn). Examples: Vasco da Gama's sea route to India; Manhattan Project; Sputnik; U.S. moon landing; AI win over humans in Go.

Fingerprinting (computer) – information collected about a remote computer for the purpose of identification and network mapping. The information could be browser type, screen resolution, modem channels, etc. Example application: mapping exactly which computers are used to alert a missile force or to support the move of atomic warheads.

5G – fifth generation standards for cellular technology and broadband access. 5G is a central element of AVs and the IoT.

First Nuclear Age - nuclear weapons in the Cold War

Generative Adversarial Networks (GANs) - An AI technique with two neural networks contesting each other in a zero-sum game theory framework. GANs mimic and tweak various probability distributions of data (voice, image, text) to trick observers into accepting a falsified picture of a situation. Example uses include false flag warning, deception, spoofing, and political signaling.

Geofencing - the use of GPS, RFID, computer vision, cell phone tracking, etc. to create electronic geographic boundaries, with software to trigger a response when a mobile device enters or leaves a "fenced" area. Examples: a congestion toll triggered by driving south of 60th street in New York; cell phone tracking in a mall that that indicates shoppers are in a particular store area, or part of the mall.

Hypervigilance - a greatly heightened state of sensory sensitivity to an impending event, often with exaggerated behaviors (from Irv Janis).

Information – data provided in context.

Information Chains – the set of linked processes and systems that move important data from one place to another in an organization. Example: drone video and cell phone system monitoring collected on the perimeter of an organization, and delivered to an assessment center.

Innovation Platform – a foundational technology for building other software applications. Examples: Microsoft's Windows, Google's Android, Amazon Web Services, Uber's ride sharing (Uber's platform has been used for food and other deliveries).

Internet of Things (IoT) – connected, smart physical devices that "talk" to each other for purposes of coordination and frictionless operation. Disruption of the IoT is a major security concern.

ISR - intelligence, surveillance, and reconnaissance

Latency – the time it takes for a response following some stimulus; or the time it takes to move a packet of data from one point in an

organization to another.

Location Analytics – the process of gaining insight from the location or geographic elements of data. Example: using cell phone tracking from a network of towers to locate particular vehicles (e.g., staff cars, military support trucks), and to use this information to automatically direct a flock of drones to a closer inspection of these targets.

Machine Learning - a form of AI that enables a system to learn from data rather than through explicit programming.

Major Powers, Secondary Powers, and Groups (MSG Framework) - a techno-economic framework that groups nations by their economic and technological ability. Major powers have a 2020 GDP greater than $3 trillion and considerable technological ability. Secondary powers fall below this threshold. Group refers to subnational sets of people (e.g., terrorists, criminals, etc.).

Nuclear Posture - organizations, technical systems, and doctrine associated with nuclear forces. There are conventional, cyber, and space postures as well.

Platform - software that connects individuals to organizations for a common purpose or to share a common resource. Examples: Airbnb, Uber, Facebook, Google search. Defense example: software, sensors, and algorithms that target a "supply side" of weapons (missiles, cyber attacks) with a "demand side" of mobile targets. The targets may be on land (mobile missiles), at sea (ships), or in space (satellites).

Process – a flow of work or information. Examples: the "go" order for nuclear launch; transmission of code words to put forces on alert.

Quick Reaction Alert (QRA) Weapons - weapons that can be fired on extremely short notice because they are linked to touchpoint data with continual updating of target location. Examples: hypersonic missiles, armed drones, F-35s, warships – if they are linked to a real-time, dynamic updated command and control system.

Reconnaissance - military observation of a region or target to locate an enemy or to determine their strategic characteristics.

Simultaneous Location and Mapping (SLAM) Technology - technology for constructing a map of an unknown environment while at the same time tracking agents or targets within it. SLAM algorithms are tailored for field performance. Example: AR eyewear worn by an agent that maps out a building's interior spaces and simultaneously applies facial recognition technology to the employees in it.

Second Nuclear Age - the spread of nuclear weapons for reasons that have nothing to do with the Cold War.

Software Development Kit (SDK) – computer code implanted in an app (Facebook, Instagram) that links to other applications; or which turns on device features (microphone, camera, Bluetooth receiver). SDKs may be camouflaged or masked so the individual is unaware they have been downloaded.

Spin Off - defense technologies with significant commercial applications. Examples: computers; jet engines; GPS; transistors, integrated circuits.

Spin On - technology developed for commercial purposes adapted for defense. Examples: Hadoop data bases; neural nets; computer vision.

Stalkerware – apps designed for tracking and covert surveillance. Example: concealed app on a cell phone that reports the location, phone numbers called, or that can listen to conversations using the phone's microphone or camera.

StingRay – a cellular phone surveillance device installed in an authorized cellular network to intercept calls and get locations. StingRays can be put in network boxes on telephone poles or on airplanes to track their targets.

Synergy - the interaction of two or more technologies to produce a combined impact greater than the sum of their individual impacts. Example: GPS, cell phone network, and payment systems combined to produce automobile ride sharing service (Uber, Lyft).

Systemically Important Target (SIT) – an enemy weapon whose use might cause severe damage or devastation. SITs require heightened surveillance and close monitoring. Example SITs: computers for strategic cyber attack, nuclear warheads, mobile missiles.

Tactile Internet - an emerging part of the internet that uses 5G technology with extremely low latency (milliseconds) and high reliability. Uses include AVs, and robotic surgery where there is constant and extensive interaction with a rapidly changing environment.

Tight coupling –performance of a group of activities that are highly dependent on each other. Search technologies of the Cold War (satellites, U-2 aircraft, signals intelligence) were loosely coupled compared to those of today's tightly coupled systems (drones, cell phone and camera hacks, cyber penetrations, cloud computing).

Transporter, Erector, Launcher (TEL) – a vehicle used to transport, erect, and fire a missile.

Touchpoints - any way that a missile or warhead interacts with an adversary's intelligence system (e.g., cell phone track of a crew member, a radio intercept, drone video, appearance on a hacked security camera, satellite picture). "High touch systems" exploit the large amounts of data available from digital technologies. Example: integrating cell phone data of individuals with automated license plate readers.

Value Chain – a widely used methodology taught in business schools describing the ordered, interlinked activities of an organization used to deliver a product or service. This "product" could be military attack, warning, deterrence, or political signaling. Advanced technology has tended to "tighten the value chain" in many commercial industries.

Video Analytics – computer vision and machine learning technology that automatically analyzes the content of immense amounts of video to detect temporal and spatial events. Example: automated monitoring of a hacked traffic congestion camera system to detect particular vehicles (e.g., crew member of a missile force, a specific staff car) from their license plates or other features. The sheer volume of video data precludes human monitoring.

About the Author

Paul Bracken is Professor of Management and Political Science at Yale University. A member of the Council on Foreign Relations, he served on the Chief of Naval Operations Executive Panel for many years. His undergraduate degree is from Columbia University in engineering, and his Ph.D. is from Yale University in operations research -- and he is an avid ham radio operator K3SOC. Bracken is a leading professor in Yale's executive education programs. He is the author of many books, including *The Second Nuclear Age, Strategy, Danger, and the New Power Politics* (Henry Holt).

FOREIGN POLICY RESEARCH INSTITUTE

Our Mission

The Foreign Policy Research Institute is dedicated to bringing the insights of scholarship to bear on the foreign policy and national security challenges facing the United States. It seeks to educate the public, teach teachers, train students, and offer ideas to advance U.S. national interests based on a nonpartisan, geopolitical perspective that illuminates contemporary international affairs through the lens of history, geography, and culture.

Offering Ideas

In an increasingly polarized world, we pride ourselves on our tradition of nonpartisan scholarship. We count among our ranks over 100 affiliated scholars located throughout the nation and the world who appear regularly in national and international media, testify on Capitol Hill, and are consulted by U.S. government agencies.

Educating the American Public

FPRI was founded on the premise that an informed and educated citizenry is paramount for the U.S. to conduct a coherent foreign policy. Through in-depth research and events on issues spanning the geopolitical spectrum, FPRI offers insights to help the public understand our volatile world.

Championing Civic Literacy

We believe that a robust civic education is a national imperative. FPRI aims to provide teachers with the tools they need in developing civic literacy, and works to enrich young people's understanding of the institutions and ideas that shape American political life and our role in the world.

WWW.FPRI.ORG

Published by the Foreign Policy Research Institute
September 2020

Author: Paul Bracken

Edited by: Alan Luxenberg
Design by: Natalia Kopytnik

Foreign Policy Research Institute

The Foreign Policy Research Institute is dedicated to producing the highest quality scholarship and nonpartisan policy analysis focused on crucial foreign policy and national security challenges facing the United States. We educate those who make and influence policy, as well as the public at large, through the lens of history, geography, and culture.

Foreign Policy Research Institute

1528 Walnut Street, Suite 610
Philadelphia, PA 19102

215-732-3774 www.fpri.org