# 1AC

### 1AC – Cyber Sovereignty

#### Internet fracturing collapses trade

Sarah Box 16, Economist in the OECD Directorate for Science, Technology and Industry, with; Jeremy West; 2016, “Economic and Social Benefits of Internet Openness,” OECD Digital Economy Papers No. 257, https://www.oecd-ilibrary.org/docserver/5jlwqf2r97g5-en.pdf?expires=1583006282&id=id&accname=guest&checksum=48A074043793053419187C3F80E2D03B

There is a growing literature on the positive effects of the Internet on trade and the potential costs to trade of policies that introduce frictions to “business as usual” data flows on the Internet. Internet openness facilitates international trade for existing businesses by making it easier for suppliers to connect with existing consumers who are located beyond the borders of the supplier’s home country (or countries) and by improving logistics control. Openness can also boost trade by providing access to a wider customer base via e-commerce. And it enables new firms to enter more geographic markets and (for the most efficient ones) to enter global value chains (GVCs). At the same time, Internet openness and digitisation make it possible to complete transactions and deliver products, services, and payments faster and more efficiently by replacing some physical trade with online trade (in books and music, for instance – or with more complex products via online shipment of designs followed by local production such as with 3D printers).

GVCs are central to the trade and Internet story. Behind aggregate trade data lie a huge number of intermediate trade flows, with inputs sourced globally and stages of production shifting from location to location to complete a final product. Both goods and services may be produced in GVCs – electronics and cars are common examples where design, raw material, production and marketing inputs are spread across countries. One can also think of aircraft, clothing, film animation, law briefs and medical advice being created in GVCs. The rise of GVCs has been made possible in part by technological advances, notably the information management systems that allow firms to co-ordinate their participation in GVCs. The combination of GVCs and the Internet has not only enabled firms in developing countries to more easily engage in international trade (by specialising in one stage of a chain, e.g. auto electronics), but also smalland medium-sized enterprises (SMEs), as digital platforms enable even tiny firms (micro-multinationals) to connect with global suppliers and purchasers.

Given the pervasiveness of GVCs, seamlessly moving potentially large amounts of data across countries is an essential part of supporting intermediate and final trade flows and allowing firms to participate in GVCs. In other words, reductions in Internet openness could create significant impediments to trade. Small frictions may multiply into large barriers, especially if production is split into stages that entail numerous border crossings where imposed frictions multiply. The Swedish National Board of Trade suggest that policies such as data localisation requirements (where firms are either forced to store data and locate data centres within a country’s borders, or have restricted ability to move and process data across borders) could lead a firm to reorganise its GVC, either moving or closing parts of its operations, with service to end-users being restricted in some cases (2015: 14-15). Ezell et al. (2013: 46-47) make a similar point, noting that localisation barriers to trade, including restrictions on data, undermine firms’ ability to participate in global networks because the barriers raise costs and reduce technology diffusion. The Software Alliance (BSA, 2014) additionally highlights the trade-dampening effect of country-specific technology standards and other forms of “digital protectionism,” such as nationally-oriented IT procurement.

#### \*Nuclear war (was gonna swap w/newer impact eventually)

Nouriel Roubini 17, professor at NYU’s Stern School of Business and Chairman of Roubini Macro Associates, was Senior Economist for International Affairs in the White House's Council of Economic Advisers during the Clinton Administration, 1/2/17, ““America First” and Global Conflict Next,” <https://www.project-syndicate.org/commentary/trump-isolationism-undermines-peace-worldwide-by-nouriel-roubini-2017-01>

Trump, however, may pursue populist, anti-globalization, and protectionist policies that hinder trade and restrict the movement of labor and capital. And he has cast doubt on existing US security guarantees by suggesting that he will force America’s allies to pay for more of their own defense. If Trump is serious about putting “America first,” his administration will shift US geopolitical strategy toward isolationism and unilateralism, pursuing only the national interests of the homeland.

When the US pursued similar policies in the 1920s and 1930s, it helped sow the seeds of World War II. Protectionism – starting with the Smoot-Hawley Tariff, which affected thousands of imported goods – triggered retaliatory trade and currency wars that worsened the Great Depression. More important, American isolationism – based on a false belief that the US was safely protected by two oceans – allowed Nazi Germany and Imperial Japan to wage aggressive war and threaten the entire world. With the attack on Pearl Harbor in December 1941, the US was finally forced to take its head out of the sand.

Today, too, a US turn to isolationism and the pursuit of strictly US national interests may eventually lead to a global conflict. Even without the prospect of American disengagement from Europe, the European Union and the eurozone already appear to be disintegrating, particularly in the wake of the United Kingdom’s June Brexit vote and Italy’s failed referendum on constitutional reforms in December. Moreover, in 2017, extreme anti-Europe left- or right-wing populist parties could come to power in France and Italy, and possibly in other parts of Europe.

Without active US engagement in Europe, an aggressively revanchist Russia will step in. Russia is already challenging the US and the EU in Ukraine, Syria, the Baltics, and the Balkans, and it may capitalize on the EU’s looming collapse by reasserting its influence in the former Soviet bloc countries, and supporting pro-Russia movements within Europe. If Europe gradually loses its US security umbrella, no one stands to benefit more than Russian President Vladimir Putin.

Trump’s proposals also threaten to exacerbate the situation in the Middle East. He has said that he will make America energy independent, which entails abandoning US interests in the region and becoming more reliant on domestically produced greenhouse-gas-emitting fossil fuels. And he has maintained his position that Islam itself, rather than just radical militant Islam, is dangerous. This view, shared by Trump’s incoming National Security Adviser, General Michael Flynn, plays directly into Islamist militants’ own narrative of a clash of civilizations.

Meanwhile, an “America first” approach under Trump will likely worsen the longstanding Sunni-Shia proxy wars between Saudi Arabia and Iran. And if the US no longer guarantees its Sunni allies’ security, all regional powers – including Iran, Saudi Arabia, Turkey, and Egypt – might decide that they can defend themselves only by acquiring nuclear weapons, and even more deadly conflict will ensue.

In Asia, US economic and military primacy has provided decades of stability; but a rising China is now challenging the status quo. US President Barack Obama’s strategic “pivot” to Asia depended primarily on enacting the 12-country Trans-Pacific Partnership, which Trump has promised to scrap on his first day in office. Meanwhile, China is quickly strengthening its own economic ties in Asia, the Pacific, and Latin America through its “one belt, one road” policy, the Asian Infrastructure Investment Bank, the New Development Bank (formerly known as the BRICS bank), and its own regional free-trade proposal to rival the TPP.

If the US gives up on its Asian allies such as the Philippines, South Korea, and Taiwan, those countries may have no choice but to prostrate themselves before China; and other US allies, such as Japan and India, may be forced to militarize and challenge China openly. Thus, an American withdrawal from the region could very well eventually precipitate a military conflict there.

As in the 1930s, when protectionist and isolationist US policies hampered global economic growth and trade, and created the conditions for rising revisionist powers to start a world war, similar policy impulses could set the stage for new powers to challenge and undermine the American-led international order. An isolationist Trump administration may see the wide oceans to its east and west, and think that increasingly ambitious powers such as Russia, China, and Iran pose no direct threat to the homeland.

But the US is still a global economic and financial power in a deeply interconnected world. If left unchecked, these countries will eventually be able to threaten core US economic and security interests – at home and abroad – especially if they expand their nuclear and cyberwarfare capacities. The historical record is clear: protectionism, isolationism, and “America first” policies are a recipe for economic and military disaster.

#### AI arms race causes extinction

Anand Ramamoorthy 18, Dept. of Anaesthesiology, UW-Madison; and Roman Yampolskiy, Computer Engineering and Computer Science, University of Louisville, February 2018, “BEYOND MAD?: THE RACE FOR ARTIFICIAL GENERAL INTELLIGENCE,” https://www.itu.int/en/journal/001/Documents/itu2018-9.pdf

The possibility of such an AGI leading to so-called artificial superintelligences (ASI) via intelligence explosion (a scenario where the AGI recursively improves itself to the point of exceeding human-level intelligence to an unpredictable extent), has led scientists, philosophers and technologists to consider the existential risks (to humanity) posed by the development of AGI. Unlike technologists and techno-futurists, AI and machine-learning researchers are more conservative in their estimates as to when such a system (or multiple such systems) can be expected on the scene. It is to be noted that the machine learning/AI research community is mostly unsure as to whether AGI would come to be or result in ASI. There also exist optimistic views on AI development which provide a healthy counterbalance to the apocalyptic visions commonly encountered in the media [6].

That said, 48% of the expert respondents in a recent survey [7] did agree that “society should prioritize work on minimizing the potential risks of AI”. A recent report from the U.S Government’s Office of Science and Technology Policy examines the state of the art in AI technology and provides an overview of the benefits and risks of AI, concluding with policy recommendations for the administration [8]. AI and AI safety are predicted to be vital to both economic development and national security [9]. It stands to reason that such considerations cut across borders, and are shared by nation-state stakeholders in the AI sector. AI arms races can happen in the context of “narrow” AI systems as well as AGI development. In the former instance, the most salient manifestation of such a race would be adversarial programs, administered by militaries around the world, to develop intelligent controllers and autonomous weapons systems. This possibility has attracted tremendous attention from AI safety experts as well as ethicists who rightly fear the ramifications of such systems being introduced into human armed conflict. The second type of AI arms race concerns multiparty, adversarial programs aimed at developing the world’s first AGI.

Here we examine the prospect of AGI development in terms of escalation and arms races between diverse actors and stakeholders: state actors, non-state (corporate) actors, and rogue actors. We conclude by providing policy recommendations aimed at mitigating the risks identified.

2. ARMS RACES AND AGI: BEYOND MAD?

The success of The Manhattan Project and the deployment of nuclear weapons by the United States military in the Second World War led to a new kind of international conflict, a nuclear arms race, where powerful nations sought to acquire the same destructive capabilities as the U.S.A. This resulted in a world where an unstable peace is kept alive, informed to a significant extent, by the doctrine of mutually assured destruction (MAD) in addition to global non-proliferation efforts. A detailed discussion of the current understanding of MAD and the status of nuclear non-proliferation is beyond the scope of this paper. It suffices to note that examining the case of MAD in its original context provides insights that can be used to understand the role of disruptive technologies in international conflict (for case studies of such technologies see [9]). AGI, if and when it happens, may well be the final disruptive technological development engineered by humans. AGI represents a level of power that remains firmly in the realm of speculative fiction as on date. It stands to reason that if true AI were achievable, state actors would be invested in achieving this and with priority if possible. Such a quest for priority might have disastrous consequences due to corner-cutting when it comes to safety, and has been described as “racing to the precipice” [10]. An AI arms race is often spoken of in the context of the development of autonomous weapons systems which become increasingly sophisticated, changing the face of warfare. Were we to adopt Clausewitz’s observation that “war is the continuation of politics and with other means” [11] and examine international conflict, it becomes obvious that the role of AI would extend well beyond, and emerge well before, armed conflict. A nation equipped with a fully general AI, would stand to benefit in the negotiation of conflict and agendas, regardless of means. If said AI were both general AND endowed with the ability to act in the world (i.e., not merely an Oracle-in-a-box as some have proposed, see [12] for an analysis of AI confinement), then, all arguments pertaining to the existential risk posed by AI would apply. Having AI systems autonomously determine the deployment of weapons in armed conflict is one major route to potential catastrophe, but we would like to emphasize that matters are likely to become fraught even before this development.

AGI development would push the global security strategy beyond what is currently in place. In the event of human control over the AGIs (which is a problem worth examining in its own right), MAD would not be sufficient to avert catastrophe. This would be because of the greater complexity associated with AGI and the capabilities such a system would present to human controllers, for instance, the AGI of a particularly belligerent state could calculate the optimal means to mortally destabilize the economy of a rival state (however powerful), or develop weaponized code disseminated globally to control, if not disrupt, vital systems such as power grids and communication networks. In other words, the cyber- warfare capabilities of an AGI-assisted nation-state would pose a serious threat to global stability and humanity. The current forms of narrow AI are capable of interfering with communication services. AI- enabled surveillance across communication networks is likely to become the norm. AI tools with the potential to perturb or alter the content of communications are already in development (see https://lyrebird.ai/ for an interesting example in the context of mimicking human speech; see also: https://lyrebird.ai/ethics/). An AGI with access to the Internet and communication networks in general would be able to, depending on its objectives (or of those who deploy it), selectively impede communication across a certain network/region, or fabricate misinformation to probe human responses if it develops the objective to understand social impact of communication networks. Much as these scenarios remind us of science fiction, it is worth noting that we encounter reports of computational propaganda or technology-assisted disinformation with increasing regularity. On a more optimistic note, an AGI that is constrained to cooperate with humans could help envision more efficient use of resources for optimizing the communication networks we have available, or design altogether novel and better architectures.

#### Innovation leadership solves emerging threats

James Kadtke 18, Ph.D., Senior Policy Analyst at the National Nanotechnology Coordinating Office, former Executive Director of the Accelerating Innovation Foundation and adjunct faculty at the National Defense University and George Mason University, with; John Wharton; March 2018, “Technology and National Security: The United States at a Critical Crossroads,” INSS Defense Horizons https://www.researchgate.net/publication/323534130\_Technology\_and\_National\_Security\_The\_United\_States\_at\_a\_Critical\_Crossroads

American leadership in science, technology, and innovation (ST&I) has been the foundation of U.S. national security for decades. Advanced technology, along with America’s ability to operationalize it into transformational capabilities, has long given us a military advantage. This advantage has provided superiority on the battlefield and for our broader national security apparatus. Today, however, our technological superiority is increasingly being challenged by near-peer and asymmetric competitors. Globalization of science and technology, emerging and unpredictable threats (both manmade and natural), conventional and emerging weapons of mass destruction, and an inversion of technology flow from the private to public sectors all present challenges to our national security.

To meet these challenges, the United States must develop a clear, synchronized, and actionable national strategy that drives advances in science, technology, and innovation in all domains (land, sea, air, space, cyber) to assure our economic and national security. While maintaining military technology overmatch remains a key national security objective, promoting technology development by the private sector at home and around the world and then harnessing that development in ingenious ways will be increasingly important for economic prosperity as well as for national security. The recently released National Security Strategy of the United States also points to research, technology, invention, and innovation as key elements of our national power.1

The Trump administration has a historic opportunity now to re-invent the U.S. Government’s relationship with the private sector and the international community to retain our country’s technological dominance throughout the 21st century. Our national security ST&I enterprise must be able to meet rapidly evolving threats, establish and maintain strategic partnerships, employ swiftly changing technologies, cope with diminishing resources, and benefit from accelerating globalization. The U.S. national security ST&I enterprise derives its strength from Federal agencies in collaboration with academia, industry, and global partners. If we are to continue to maintain technological preeminence and ensure our national security, we must evolve and adapt to meet these emerging threats and challenges. The United States must think strategically, and in fact geostrategically, 2 to manage and enhance its national ST&I resources.

America is at a critical crossroads. New generations of advanced technologies are on the verge of dramatically changing global society.3 Many other nations are now investing heavily in research and commercialization capabilities to create or exploit these new advances. At the same time, the United States has often been de-investing in many technology areas over the last decade or more and is on a path to losing its global competitive advantage. This will have dire consequences for the future of our economy, military, and society at large. However, with a firm recommitment to enhanced and strategic investments in science (research), technology (commercialization), and innovation (cultural change), the United States can retain international leadership for decades to come.

The Global Technology Revolution For decades, advanced ST&I activities were mostly conducted by a handful of wealthy nations. Today, however, there is a radical change happening in how and where science and technology development are being conducted. The commercialization and globalization of the internet, which has led to tremendous innovation in social interaction and commerce over the last two decades,4 is also now creating a global scientific enterprise.

Scientists the world over can easily collaborate and share data and analytic tools. Technology communities from different disciplines are cross-fertilizing to create new disciplines (for example, nano-robotics). Multinational research companies move ideas, people, and resources across national boundaries with ease to maximize efficiency. A growing community of “do-it-yourself ” scientists who can conduct fundamental research in their own homes are appearing worldwide. And most importantly, a growing number of countries are investing heavily in science, technology, and commercialization activities as a path to high-value economic growth and increased military capabilities. The result of these trends is that the rate of innovation today in science, technology, and high-tech product development is unprecedented in history and continues to accelerate.5

New generations of highly advanced technologies are already being deployed throughout global society and they will dramatically alter our way of life, as well as our economic systems and military capabilities. Nations, corporations, universities, and tech-based consortia are pushing hard to develop and deploy these advanced technologies since the financial and economic returns are potentially enormous. Some of the revolutionary technologies that will appear within the next decade include:

◆ A continued buildout of information and communication technology infrastructure (WiFi, satellites, mobile devices) will provide cheap or free internet access to virtually everyone around the globe. A June 2017 report by the U.S. Army War College has warned of the “coming age of unbridled hyper-connectivity.”6

◆ Human–machine interfaces where mobile devices will be replaced first by wearables, then embeddables, and eventually devices directly interfaced to the brain, raising serious new privacy and security issues.7

◆ Using synthetic biology and gene editing, scientists will be able to create entirely new life forms that can perform a variety of radically novel tasks but at the same time, pose unknown risks.8

◆ Artificial intelligence and advanced robotic devices will become highly functional and cheap, and personal robots and autonomous infrastructure (such as driverless cars) will be common but may create dangerous new cybersecurity vulnerabilities.9

◆ Production and distribution facilities will become largely autonomous and seamlessly interfaced globally (that is, the Industrial Internet of Things), creating a mega-infrastructure for industry potentially not controlled by any one nation, which could displace millions of workers worldwide.10

◆ Commercial nanotechnology companies will create completely new kinds of materials and products that will make obsolete many existing product lines, for example, smart materials that automatically heat, cool, change optical properties, or never wear out, as well as nano-machines. These creations, however, may raise serious environmental and military risks.11

◆ Facilitated by nanotechnology and synthetic biology, new generations of renewable energy technologies will be deployed, for example, highly efficient solar cells or energy harvesting technologies, which may disrupt the current global economics of energy.

◆ Enabled by cheap launch capabilities (for example, by SpaceX), commercial space companies may by 2020 begin mining asteroids and the moon and fabricating products in space, but widely available space access may also facilitate wholly new mechanisms for malicious actions by rogue states or terrorists.12

Many, if not most, of these disruptive technologies are the direct result of decades of research investment by the U.S. Government and private sector. However, because of a variety of factors, the next generation of new technologies may likely be commercialized and produced outside of the United States, which will create a strategic and long-term threat to our nation’s well-being.

America’s Strategic Technology Challenges

The United States has become a great power in part because it has historically fostered creativity, entrepreneurship, and innovation. After World War II, because of the vision of President Roosevelt’s science advisor Vannevar Bush, the United States created the first S&T enterprise, a formal collaboration between the Federal Government, corporations, and academia. Funding investments in this enterprise are widely credited with creating over half our growth in GDP since World War II and have enabled one of the most powerful militaries in the world. Yet today, the dominance of our S&T enterprise is on the verge of being overshadowed by international competition. This is due to multiple factors both domestic and foreign. Many countries are now dramatically increasing their investments in science, technology, and commercialization, particularly in Asia, and including many nontraditional players such as Vietnam and Singapore. A May 2016 report by the National Science and Technology Council pointed out the “dramatically increased capacity for science and technology around the world.”13 At the same time, U.S. government funding (in constant dollars) has remained roughly flat over the last couple of decades and has even gone down since 2013. Moreover, the fraction of U.S. investments in the global S&T enterprise has dropped from about 39 percent in the late 1990s to about 31 percent by 2015.14 The trend therefore is that the U.S. S&T enterprise will be a progressively smaller part of the global S&T enterprise, and the United States will produce a progressively smaller fraction of scientific breakthroughs and high-tech products in the future. This portends a future in which the United States will be driven into economic decline, and our military strength will be compromised because we no longer have the technology dominance we have depended on since the 1940s (see figure).

In addition to funding, many common practices by foreign powers are undercutting the U.S. technology base. This includes strategic and coordinated cyber-theft of intellectual property, unfair or asymmetric access to technology markets and trade, aggressive foreign acquisition of small U.S. tech companies, poaching of intellectual talent, lax or non-existent foreign environmental and health regulations, and corporate espionage, among others. The U.S. Government has often turned a blind eye to many of these issues over the years, and this has compromised our leadership in several critical technology areas (for example, aerodynamic and hydrodynamic design).15

Within the United States, we have been witnessing the slow degradation of the competitiveness of our own domestic S&T enterprise. Decreased or inconsistent funding of S&T programs or target disciplines is a key factor and, more broadly, the lack of clear national strategic technology plans, as well as political support for research investments and commercialization frameworks. Other factors affecting the health of our national S&T enterprise include burdensome regulation of tech companies, regulatory uncertainty in emerging technology areas, inconsistent research tax incentives, the complex Federal contracting and acquisition process, poor public-private sector cooperation in many areas, and the technological literacy of our workforce. All these factors affect or degrade the efficiency and profitability of our S&T enterprise and make us progressively less competitive in the globalizing technology landscape.

From a grand strategic perspective, one might observe that in the decades to come, in a world dominated by pervasive advanced technologies, the countries that are most able to create, acquire, and utilize these disruptive technologies will lead the world. This technological capacity will be one of, if not the, most important global resources.16 Technological capacity will become the new oil.

Organizing for Future U.S. Technological Leadership

Our future well-being and security as a nation depends on us maintaining technological preeminence throughout the coming decades. Our national political leadership, working in concert with U.S. corporate leaders and academia, have a historic opportunity to change our national trajectory to ensure this future. This will require more than the occasional Federal technology initiative, political photo op, or unfunded mandates that have characterized many U.S. ST&I commitments over the last decade. It will require a re-thinking of the framework for our national ST&I enterprise and developing a new paradigm for public-private coordination with a commitment to shared goals. Fortunately, the issue of maintaining U.S. technological leadership has been increasingly debated in public policy circles, and there is growing political support to act now.17

#### But, Chinese leap-frogging goes nuclear

Matthew Kroenig 18, Deputy Director for Strategy, Scowcroft Center for Strategy and Security Associate Professor of Government and Foreign Service, Georgetown University, 11/12/18, “Will disruptive technology cause nuclear war?” https://thebulletin.org/2018/11/will-disruptive-technology-cause-nuclear-war/

Recently, analysts have argued that emerging technologies with military applications may undermine nuclear stability (see here, here, and here), but the logic of these arguments is debatable and overlooks a more straightforward reason why new technology might cause nuclear conflict: by upending the existing balance of power among nuclear-armed states. This latter concern is more probable and dangerous and demands an immediate policy response.

For more than 70 years, the world has avoided major power conflict, and many attribute this era of peace to nuclear weapons. In situations of mutually assured destruction (MAD), neither side has an incentive to start a conflict because doing so will only result in its own annihilation. The key to this model of deterrence is the maintenance of secure second-strike capabilities—the ability to absorb an enemy nuclear attack and respond with a devastating counterattack.

Recently analysts have begun to worry, however, that new strategic military technologies may make it possible for a state to conduct a successful first strike on an enemy. For example, Chinese colleagues have complained to me in Track II dialogues that the United States may decide to launch a sophisticated cyberattack against Chinese nuclear command and control, essentially turning off China’s nuclear forces. Then, Washington will follow up with a massive strike with conventional cruise and hypersonic missiles to destroy China’s nuclear weapons. Finally, if any Chinese forces happen to survive, the United States can simply mop up China’s ragged retaliatory strike with advanced missile defenses. China will be disarmed and US nuclear weapons will still be sitting on the shelf, untouched.

If the United States, or any other state acquires such a first-strike capability, then the logic of MAD would be undermined. Washington may be tempted to launch a nuclear first strike. Or China may choose instead to use its nuclear weapons early in a conflict before they can be wiped out—the so-called “use ‘em or lose ‘em” problem.

According to this logic, therefore, the appropriate policy response would be to ban outright or control any new weapon systems that might threaten second-strike capabilities.

This way of thinking about new technology and stability, however, is open to question. Would any US president truly decide to launch a massive, bolt-out-of-the-blue nuclear attack because he or she thought s/he could get away with it? And why does it make sense for the country in the inferior position, in this case China, to intentionally start a nuclear war that it will almost certainly lose? More important, this conceptualization of how new technology affects stability is too narrow, focused exclusively on how new military technologies might be used against nuclear forces directly.

Rather, we should think more broadly about how new technology might affect global politics, and, for this, it is helpful to turn to scholarly international relations theory. The dominant theory of the causes of war in the academy is the “bargaining model of war.” This theory identifies rapid shifts in the balance of power as a primary cause of conflict.

International politics often presents states with conflicts that they can settle through peaceful bargaining, but when bargaining breaks down, war results. Shifts in the balance of power are problematic because they undermine effective bargaining. After all, why agree to a deal today if your bargaining position will be stronger tomorrow? And, a clear understanding of the military balance of power can contribute to peace. (Why start a war you are likely to lose?) But shifts in the balance of power muddy understandings of which states have the advantage.

You may see where this is going. New technologies threaten to create potentially destabilizing shifts in the balance of power.

For decades, stability in Europe and Asia has been supported by US military power. In recent years, however, the balance of power in Asia has begun to shift, as China has increased its military capabilities. Already, Beijing has become more assertive in the region, claiming contested territory in the South China Sea. And the results of Russia’s military modernization have been on full display in its ongoing intervention in Ukraine.

Moreover, China may have the lead over the United States in emerging technologies that could be decisive for the future of military acquisitions and warfare, including 3D printing, hypersonic missiles, quantum computing, 5G wireless connectivity, and artificial intelligence (AI). And Russian President Vladimir Putin is building new unmanned vehicles while ominously declaring, “Whoever leads in AI will rule the world.”

If China or Russia are able to incorporate new technologies into their militaries before the United States, then this could lead to the kind of rapid shift in the balance of power that often causes war.

If Beijing believes emerging technologies provide it with a newfound, local military advantage over the United States, for example, it may be more willing than previously to initiate conflict over Taiwan. And if Putin thinks new tech has strengthened his hand, he may be more tempted to launch a Ukraine-style invasion of a NATO member.

Either scenario could bring these nuclear powers into direct conflict with the United States, and once nuclear armed states are at war, there is an inherent risk of nuclear conflict through limited nuclear war strategies, nuclear brinkmanship, or simple accident or inadvertent escalation.

This framing of the problem leads to a different set of policy implications. The concern is not simply technologies that threaten to undermine nuclear second-strike capabilities directly, but, rather, any technologies that can result in a meaningful shift in the broader balance of power. And the solution is not to preserve second-strike capabilities, but to preserve prevailing power balances more broadly.

When it comes to new technology, this means that the United States should seek to maintain an innovation edge. Washington should also work with other states, including its nuclear-armed rivals, to develop a new set of arms control and nonproliferation agreements and export controls to deny these newer and potentially destabilizing technologies to potentially hostile states.

These are no easy tasks, but the consequences of Washington losing the race for technological superiority to its autocratic challengers just might mean nuclear Armageddon.

#### Democratic consolidation solves great power war---solves disads---stopping China from exporting digital authoritarianism is key

Bruce Jones 19, Brookings Senior Fellow of Foreign Policy, Center for East Asia Policy Studies, with; Torrey Taussig, non-resident fellow; February 2019, “Democracy & Disorder: The struggle for influence in the new geopolitics,” https://www.brookings.edu/research/democracy-disorder-the-struggle-for-influence-in-the-new-geopolitics/

2019 marks the third decade of a world that has been largely free of the risk of direct great power conflict. Thirty years ago, the fall of the Berlin Wall and democratic openings across Central and Eastern Europe not only heralded the fall of the Soviet Union, but also symbolized the widespread appeal among citizens for a democratic model of governance. The quarter-century that followed was unique in world history: For the first time, democratic states dominated the structure of world power with neither a peer military competitor nor a rival model of governance with which to contend. The United States, in particular, stood unrivaled on the world stage, exercising global unipolar reach.

It is in vogue now to look back at the period of American hyperpower as one of over-extension and overreach, and to focus near exclusively on America’s Middle East wars. As consequential as those were, the dynamics of that period were wider and more nuanced. It was an era that saw multilateralism flourish and wars of all forms decline (although terrorist acts did not). Global GDP rose and the percentage of the world’s population living in absolute poverty declined steadily. There was cautious optimism about trends toward great power cooperation and away from proxy warfare—an optimism that was interrupted by 9/11 and the Iraq War, but not reversed.

This was also an era that laid the seeds of present-day challenges. Advances in technology and globalization, spurred by lower trade barriers, boosted global GDP but also led to the dislocation of middle-class livelihoods in many Western societies, sowing political tensions.

Now, in the wake of the global financial crisis, two critical dynamics have unfolded concomitantly. First, the powerful democracies of the trans-Atlantic community (the bulwark of the Western-led order) are facing political turmoil at home and setbacks in the liberal quality of their own governments.

Second, the democracies find themselves losing ground internationally to authoritarian powers bent on breaking the hold of the democracies on the character of the international order.

The concurrence of these two phenomena leads to this essential question: What role will leading democracies, and democracy itself, play in the changing international order?

Over the past year, 33 Brookings scholars examined the interplay between domestic and international challenges to democracy in critical countries and regions. The key findings of this project make for challenging reading for those citizens and policymakers committed to defending the space for democracy in international affairs, but there are also grounds for optimism and for mobilization.

At this crucial geopolitical juncture, democratic states are under increasing strain from an interconnected set of domestic challenges—political, economic, and cultural. Key regions and countries around the world are experiencing a recession in democratic liberalism caused by a culmination of long-term challenges including ineffective governance, economic inequality, and socio-cultural upheaval. Backsliding among advanced democracies across the West is most prominently a crisis of liberalism, as economic grievances along with identity-based struggles have resulted in the rise of populist movements on both the left and right of the ideological spectrum, some of which have authoritarian tendencies. In emerging and non-Western democracies, the internal challenges are more prominent in the service delivery realms, where governments prove incapable or unwilling to reduce corruption and violent crime. While all democracies—advanced and emerging—have always struggled with certain internal political, economic, and social weaknesses, such faults in the modern democratic state have become more acute in the wake of the global financial crisis.

The result is a prevailing perception among analysts and policymakers that, following decades of advancements, democracy’s momentum has run its course. In fact, not all trends are negative: The consolidation of democracy across parts of Asia and Africa means that globally, more people now live in democracies than at any point in history. Still, several of the world’s most powerful democracies have been sapped of strength at a critical moment in time.

Against a backdrop of economic and political tensions, illiberal and authoritarian leaders are gaining power through electoral processes and following an illiberal playbook to weaken liberal democratic norms from within. Today, a powerful contest of ideas runs not only across states but also through them, as illiberal and authoritarian-leaning individuals and parties are consolidating control within democratic systems. Current governments in Hungary and Poland and an increasingly authoritarian Turkey under President Recep Tayyip Erdoğan represent the forefront of illiberal and neo-authoritarian challenges within the EU and NATO. The success of these illiberal forces in gaining power through electoral means highlights the separation of liberal principles—ideas that promote individual liberties, and legislative and judicial checks on the executive—from democratic processes such as elections that translate popular will into policy. Even more than a setback in democracy, their efforts are emblematic of a crisis of liberalism.

Worryingly for the Western institutions in which they operate, illiberal actors across the West and beyond at times appear to be forging a loose “nationalist international,” with shared disdain for liberal domestic and multilateral arrangements. The illiberal playbook has also opened space for outside authoritarian interference; some political forces are acting with direct political and economic assistance from Vladimir Putin’s Russia. The insidious nature of the challenge is that no single move in isolation appears to be an existential threat to democracy, and popular support behind these movements makes it difficult for defenders of liberal democracy to develop effective responses.

The interplay between internal strains and external efforts to exacerbate them has weakened the leverage of the political West. The phase when the United States and other like-minded states could enlarge the democratic community through democracy promotion efforts with manageable domestic and international pushback has ended. The global financial crisis and the rise of China have triggered a deep level of introspection within the political West. The world’s most important shaping power, the United States, is in strategic disarray and appears to be withdrawing from its commitment to supporting and exemplifying democratic standards. The European Union, the other bulwark of the liberal order, has turned inward, facing domestic instability caused by characteristics inherent to a more open order, including economic integration, low trade barriers, and the free movement of people. The authoritarian powers, briefly scared by democratic uprisings in the Arab world and then Ukraine, have gained confidence that they can both suppress dissent at home and build competing networks of influence abroad, with limited effective resistance from the major democracies.

As a result, regions of contestation have emerged across the developing and industrialized world. It is a competition of influence that involves political, economic, and military tools—and it is increasingly digitalized.

In the developing and emerging countries of Latin America, Africa, and Asia, investments in infrastructure, energy, and technology are turning from tools of G-20 cooperation into tools of great power competition—with the West losing ground. In the Middle East, there has been a return to the kind of proxy warfare that so devastated the “third world” during the Cold War. In Europe, China’s increasing economic engagement is softening the continent’s resolve, especially at a moment of American unilateralism, and Russia has found vulnerabilities to exploit and to advance its direct political interference. In East Asia, China has shifted from a strategy of constraining American dominance to one of asserting Chinese hegemony. Geopolitics in the region, defined increasingly by Sino-U.S. rivalry, will test the strength of both consolidating democracies and advanced democracies.

Globally, tools for digital authoritarianism implemented by Russia and China present Western states with a new set of challenges, and ones that represent the future of competition. Moscow continues to deploy non-conventional tools such as cyberattacks and disinformation campaigns throughout Europe and in the United States. China’s focus is primarily domestic, employing powerful digital tools to control and surveil its domestic population. But Beijing in the future may seek to export an authoritarian model, which is increasingly backed by technologies for digital censorship and monitoring. Advancements in artificial intelligence will only make the challenges more formidable in the years ahead.

#### China agrees to Space cyber-war norms in exchange for US recognition of Chinese cyber sovereignty---coop broadly solves malign Chinese cyber activities and its international promotion of internet sovereignty

Ariel (Eli) Levite 19, nonresident senior fellow in the Nuclear Policy Program at the Carnegie Endowment; and Lyu Jinghua, visiting scholar with Carnegie’s Cyber Policy Initiative, 1/24/19, “Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?,” <https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213>

The road to hell, it is often said, is paved with good intentions. While there is no dearth of sound ideas for de-confliction in cyberspace, China and the United States have nonetheless experienced and will most likely continue to go through periods of intense friction triggered by a series of policies adopted and actions their governments undertake to assert their sovereignty and promote their respective national interests. But at the most fundamental level both parties do have a common interest in working together to effectively manage and control their differences, avoid military conflicts, and build together a more benign international environment. Serious military conflict may be caused by not only traditional security issues in hotspot regions, but also by friction in the newer security domains, especially space and cyberspace.

Crisis in cyberspace presently holds particularly ominous prospects for escalation between China and the United States for several reasons. First, there is the attribution challenge. Mutual suspicions, which currently run high on both sides, may result in flawed attribution of the responsibility for malicious cyber activity and result in miscalculated response. Second, cyber offense is viewed as an asymmetric tool by less advanced countries. Both China and the United States present tempting targets for some risk-takers to launch cyber attacks, trying to hit-and-run. As cyber threats are always imminent and often anonymous, they might lead to misunderstanding between the two big powers. Third, nations that benefit most from cyberspace, such as China and the United States, are also the ones most vulnerable to cyber attacks. This fact results in a higher potential that they may be inclined to be preemptive in the event of a cyber threat. Fourth, the U.S. government’s professed doctrine to retaliate with all appropriate means to cyber attacks may be useful for deterrence purposes. But if actually implemented, it could also gravely escalate an ongoing crisis. Retaliation may quickly lead to discharge of fire in physical domains in response to cyber incidents or, at a minimum, to Chinese anxiety that this may be the case regardless if warranted, and the implementation of corresponding Chinese measures in anticipation of such U.S. action.

But none of this is truly inevitable. The hard-core security, economic, and political interests of both states do align. China has been most explicit that this is the case and has repeatedly expressed its desire to maintain a stable relationship with the United States. In his report delivered at the 19th National Congress of the Communist Party of China, Chinese President Xi Jinping advocated the idea of fostering “a new type of international relations and build[ing] a community with a shared future for mankind, which included building a framework for major country relations featuring overall stability and balanced development.”35 Furthermore, the International Strategy of Cooperation on Cyberspace issued by China in 2017 emphasized the importance of peace and stability in cyberspace, listing it as one of the nine action plans. This document clearly declared China’s commitment to “participate in bilateral and multilateral discussions on confidence-building measures, take preventive diplomatic measures, and address various cyber security threats through dialogue and consultation.”36

What’s more, China professes a positive attitude toward playing an active role in promoting global cyber governance. To build a community for a shared future in cyberspace, which is an integral part of the community with a shared future for mankind, international cooperation on cyber governance is indispensable. Xi reiterated the “general trend and common aspiration of the people to promote the reform of the global cyberspace governance system by sticking to a multilateral approach with multi-party participation from the government, international organizations, internet enterprises, technology communities, non-governmental institutions, and individuals.”37 China supports UN efforts to adopt resolutions regarding information and cybersecurity and actively takes part in the processes of UNGGE; promotes cooperation among member states in SCO, BRICS, and ARF; and consistently enhances bilateral partnerships on cybersecurity. Following a consensus reached with the United States in 2015 during Xi’s visit, China has signed cybersecurity agreements with five other countries in three years, including the UK, Australia, Russia, Brazil, and Canada. From this perspective, more cooperation with the United States in the political-military dimension could not only improve bilateral relations but also set examples for further cooperation with international society.

The U.S. government undoubtedly shares the same ambition to develop constructive governance of cyberspace, and is also wedded to a vision for doing so that combines multilateral instruments with bilateral U.S.-Chinese ones. Even the otherwise mercurial Trump has weighed in to ease the sanctions his administration has imposed on ZTE for violating U.S. law, as a personal gesture to Xi, and has more recently professed similar willingness to step in once again to resolve the extradition case of a Huawei senior official. He has done so even in the face of vociferous opposition from some security hawks in the United States. But compatibility of interests, lofty visions, and even ad hoc constructive steps will not suffice here. They have not been sufficient thus far to prevent the downward spiral in trust between the two nations. So what is ultimately necessary is a grand bargain, inevitably at the presidential level. Not quite at the same scale as when former U.S. president Richard Nixon opened to China but quite similar to the one struck originally between Obama and Xi in 2015, albeit one that subsequently goes much further in its implementation mechanisms. Only such action could open the way for the two nations to break the current impasse and start implementing constructive steps of the nature contemplated above.

Let us be clear. This is not about trading core national security interests of either party. In fact, quite the reverse, it is about safeguarding them. Similar to the reciprocal steps presently being discussed between the United States and China in the bilateral trade area, it is merely about prioritizing concerns and interests. Some of the steps that could facilitate such a grand bargain reside altogether outside the security realm, such as in the domains of trade and investments. Others might be in the security realm but outside cyber, such as on progress toward North Korea’s denuclearization. But ultimately there also has to be at least some cyber component of the grand bargain for it to have the desirable effect in cyberspace.

What we put forward for consideration here is a cyber quid pro quo that derives its inspiration from the overall Chinese approach toward cyberspace stability as outlined by Xi. As we envisage it, what would be required would be for both sides to undertake reciprocal gestures of goodwill toward cyber stability. Toward that end, the United States could be expected to move toward accepting, in some form, the Chinese concept of cyber sovereignty, thereby addressing the primary Chinese anxiety about domestic stability. To be more explicit, the U.S. contribution would be to show deference to the Chinese government and people on how they wish to govern cyberspace domestically. In return, the United States could expect China to reciprocate its goodwill by accepting to apply rather different rules to international cyber rules of the road generally, and to its cyber conduct toward the United States in particular.

In practice what we have in mind is that the United States would not endorse but would nonetheless explicitly recognize the right of China, as it is presently inclined, to apply what is now a rather intrusive cyber monitoring regime internally in the interest of ensuring domestic stability. For its side, China would explicitly accept (once again without necessarily endorsing) that the United States applies its own conception of international cybersecurity and self-defense in both peacetime and at times of war. This would require China to be receptive to U.S. cyber sovereignty concerns by taking far more assertive measures to enforce its policy of preventing and punishing the use of Chinese territory, by any party, to conduct cyber attacks against the United States (and others), and to recognize that cyber weapons use in wartime would be governed by the same rules that apply to the employment of other weapon systems in self-defense.

We believe that such understandings are compatible with both nations’ separate as well as common core interests in and beyond cyberspace. Such understandings would greatly benefit the international community, precisely in the ways envisaged by Xi at the 19th Communist Party Congress. Xi has already taken the first bold step in this direction in his historic 2015 cyber understanding with Obama, true to the famous adage from Lao Tzu that “the journey of a thousand miles begins with a single step.”38 The time has now come to undertake the next step in cyberspace.

#### Key to peaceful coexistence between internet models---otherwise, inevitable clashes cause tech decoupling, internet fracturing, and Chinese autocracy promotion

Geoffrey Hoffman 18, cyberpolitics researcher, Master’s degrees from Columbia University and Tsinghua University, 2/28/18, “A clash of cyber civilizations,” https://www.merics.org/en/blog/clash-cyber-civilizations

Censorship and surveillance versus a free and open internet: China's ideas of cyber sovereignty are incompatible with how liberal democracies define cyberspace. Despite these inevitable conflicts, the two models could coexist in relative peace as long as governments focus on the shared goal of cyber defense.

There has been little need for the term “cyber sovereignty” among democratic states: the Internet, by its nature, operates under an aegis of freedom and cooperation. However, as the international system slips away from American unipolarity, a competing model of cyber sovereignty has emerged in China that seeks to bind cyber borders to online censorship and surveillance. Given that democracies will always be hostile toward censorship, can these two models coexist? More importantly, should they?

This clash has been building since at least 2010, when, in retaliation to China’s Operation Aurora cyber attacks on a large number of U.S. firms, Google and the U.S. government publicly confronted China on its Internet censorship practices. The repercussions are now widespread, including U.S. distrust of Chinese telecom companies and China’s pressuring of foreign academic journals to engage in censorship. Yet, both the Chinese and Western models of cyber sovereignty share a fundamental pillar of cyber defense, which offers a path toward a more peaceful coexistence. However, in order to understand the challenges of the two working together, it is first necessary to explore their differences.

China seeks to govern cyberspace in analogy to geographic borders

For China, the heart of cyber sovereignty is cyber borders. Last year, China’s Ministry of Foreign Affairs and the Cyberspace Administration of China jointly released a white paper, “International Strategy of Cooperation on Cyberspace,” which asserts that, as a basic norm in international relations, the principle of territorial sovereignty includes cyberspace. To that end, China seeks to govern its cyber borders similarly to its geographic borders, with the surveillance and censorship systems of the Great Firewall (GFW) serving as its cyber border wall and customs. The impetus for China’s stringent virtual private network (VPN) regulations is, in part, to strengthen its cyber borders by closing the gap in the GFW that VPNs create. However, the crackdown also exacts certain costs, such as from businesses and researchers, and knowingly allowing this toll underscores China’s commitment to cyber sovereignty.

China’s Internet strategy is based on implementing a traditional Westphalian concept of sovereignty as absolute control over national borders. Western democracies have been groping toward a different model that is based on the sovereignty concept underlying the post-World War II liberal international order as exemplified by the United Nations, the international trading system, and the international human rights system. Under this concept of sovereignty, countries use their sovereign right to enter into agreements with one another to construct institutions that mutually restrict states’ freedom of action both toward one another and toward their own citizens. Applying this concept to the cyber sphere means attempting to establish norms, treaties, and institutions that offer collective protections, such as restricting attacks, coordinating defenses, and sharing information and tools.

The two models have different structural strengths and weaknesses. For the Western model, upholding cyber sovereignty primarily rests on Internet freedom and cyber defense. As China’s cyber sovereignty is vulnerable to the free spread of information, its two pillars are censorship and cyber defense. The Chinese model is therefore a more difficult undertaking in the sense that it necessitates retooling the inherently free and open Internet to accommodate surveillance and censorship. Yet, it offers the advantage that censorship provides better cyber defense, and China thrives on the benefits of that coupling through its cyber borders. Alternatively, the Western model’s solution to the puzzle of how to improve cyber defense without sacrificing Internet freedoms is through international cooperation based on mutual trust and understanding. As a result, the strength of the Western model scales with the number of participants.

Clashes over censorship are inevitable

As the models continue to mature, clashes will become more frequent. Since cyber defense is not zero-sum, conflicts will revolve primarily around censorship, and each challenges the other in both passive and active ways. For the Western model, one passive force of influence is its wealth of important websites, such as for news, research, or social networking, that the GFW blocks. China attempts to counter this influence by building its own versions of these websites. Active measures include applying political pressure to improve Internet rights and the development of censorship circumvention and privacy tools. For the Chinese model, cyber borders radiate a passive effect of self-censorship over foreign websites that wish to avoid GFW blocks. Democracies, in turn, resist by pillorying websites that self-censor. Actively, China seeks a more state-centric system of governance for the Internet, and it may be testing a new approach to ask foreign websites to censor themselves.

A recent example of this approach was China’s request of Cambridge University Press (CUP) to censor the website of its journal The China Quarterly for visitors from China. Disturbingly, CUP assented for several days before reversing its decision—demonstrating both the vulnerability and resiliency of open societies to this type of influence. One of China’s aims might have been to measure the resistance to its influence, but such actions engender greater mistrust. Australia, for instance, has appropriated the Solomon Islands undersea Internet cable contract from Huawei due to security concerns and fears of China’s meddling in its domestic politics, illustrating the challenges of entanglement. The CUP and Huawei examples also point to the models’ particular paradoxical struggles. China’s posture of non-interference—which led to its model in the first place—employs interference to succeed. Moreover, while a democratic state strives for cooperation in cyberspace, it does so with deep ties to Internet freedom, and these two impulses vie to guide its relationship with China in opposing directions.

Mutual cyber defense pacts with China are possible

Although in competition, the models are not wholly disparate and exclusive. China has been willing to participate in the Western model’s open-ended multilateralism; last year, for example, Canada and China signed a cyber defense pact agreeing not to conduct attacks on each other’s private sectors. Further, to a certain extent, Western states do engage in censorship and cyber border protections: the leaked U.S. National Security Council memo discussing a nationalized 5G network to guard against future threats from China offers one example. The memo’s existence also calls attention to how threats to the models may come from within: from private sector greed, for instance, such as the dissolution of net neutrality protections in the U.S., or from Chinese Internet users resisting censorship. It is also important to note that some countries take various hybrid approaches to these models, such as Singapore which engages in a high level of surveillance but not censorship. It is too early to tell whether cyber borders or cooperation will be more effective at combining security, access to necessary information, and control over potential threats, or whether the models will instead stabilize into a bipolar parity.

The success of one model may influence the other. If the Western model eclipses China’s in cyber defense capability, it could force China to prioritize cyber defense over censorship. In these circumstances, China may be willing to open its cyber borders to some degree in order to participate more fully in cooperative protection efforts, forfeiting some facility for censorship. Conversely, deficiencies in the Western model could likewise compel democratic states to fortify their cyber borders and surrender certain Internet freedoms.

Cooperation with China risks normalizing censorship practices

Peacebuilding efforts are crucial; yet, last year, the United Nations reached a dead end in codifying a set of cyber norms to temper cyberspace’s anarchic character. Martha Finnemore recently wrote, “Contestation of cyber norms is to be expected, particularly because changing technology constantly creates new situations.” Thus, a particular difficulty with cyber norms is that they must be flexible enough to assuage fears of the unknown yet concrete enough to be meaningful. Cyber sovereignty presents an opportunity here, as it is a set of elemental cyber norms that offers a comparatively stable locus for the norm-building process.

The issue of censorship will remain non-negotiable, both for democracies and for China. However, if—as with the Canada-China agreement—the countries focus their Internet relationship on the shared goal of cyber defense, the two models may be able to coexist in relative peace. Cyber defense norms, treaties, and institutions may yield enough common ground to mitigate, somewhat, the inevitable conflicts over censorship in the years ahead. Democratic states now face a dilemma: the door to cooperation with China on cyber defense is open, but it requires overlooking China’s domestic censorship practices, and, in doing so, hazards further normalizing these practices. On the other hand, doing nothing may widen the gulf between the models and fracture the Internet even further.

#### Competition between models causes AI arms racing and US-China war

Nicholas D. Wright 19, nonresident associate in the Nuclear Policy Program at the Carnegie Endowment, 2019, “Global Competition” https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B\_0161\_WRIGHT\_ARTIFICIAL\_INTELLIGENCE\_CHINA\_RUSSIA\_AND\_THE\_GLOBAL\_ORDER.PDF

Global Institutions and Norms

Global institutions and norms also form a significant arena for competition. More broadly, China and Russia have pushed back against a, perhaps idealistic, conception of a free, borderless global internet. China uses its market power to influence technical standards, ‘normalize’ domestic control and shape norms of behavior through international organizations. Such states may conceive of these as strategically defensive measures necessary to ensure domestic control, but to observers they may seem offensive.

Context

The US, Chinese, and Russian models’ potential attractiveness will only be one factor in these states’ global competition for influence—albeit potentially an important one if the twentieth century competition between regimes offering plausible, competing versions of the future is a guide. Other critical factors will include relative power, economic self-interest and historical grievances (e.g., Sino-Japanese antagonism)—as well as a good dose of luck.

However, while one must view such competition between alternative types of digital domestic political regimes against the broader backdrop of a rising China, resurgent Russia and enhanced “Gray Zone” competition between states—in many ways that context renders a plausible alternative to liberal democracy even more significant. Scholars of Chinese global influence such as David Shambaugh have long noted a gap in its social system’s appeal as a competitor to liberal democracy (Shambaugh, 2013), which these new technologies may help fill. Part III of this work examines the export and emulation of the models in global competition.

Domestic Political Regimes and Foreign Policy Decision Making

A second way that domestic political regimes affect global competition is by affecting states’ foreign policy decision making. States’ decision making is crucially affected by both internal and external factors, with arguments for the primacy of one or the other overstating the case (for discussions see e.g., Waltz, 2001; Zakaria, 1992).

Aspects of domestic regimes, such as bureaucratic or domestic political audiences, can profoundly affect foreign policy decision making. This is seen in the case of democracies, for example where the specter of repeating a quagmire like “Vietnam” constrained various US administrations. Historical analysis of multiple episodes show the importance of public opinion in various different ways (Snyder and Borghard, 2011; Trachtenberg, 2012). The bureaucratic level also matters, shown for instance in classic studies of decision making during the Cuban Missile crisis (Allison and Zelikow, 1999). Various interest groups also matter in authoritarian states, and may matter differently in different types of authoritarian states (Weeks, 2008). Russia under Vladimir Putin is not the same as Russia under the incredibly powerful mid-nineteenth century Tsar Nicholas II. Arguably, Chinese leader Xi Jinping has consolidated far more power than his immediate predecessor Hu Jintao.

Part IV of this work examines how the development of digital authoritarianism may affect Chinese foreign policy decision making. For example, if digital authoritarian controls mean Chinese leaders have less to fear from their popular disquiet, they may be able to take more risks and back down (or ramp up) tensions in crises. Future work must extend this to examine Russia and the United States.

Global Military Dimensions

The AI-related technologies also affect the military dimensions of global competition. This may act on the longer term, such as through fears on all sides of spiraling AI arms races. It may act on escalation during crises (e.g., Herb Lin, chapter 19). It may increase the importance of “hacking” more broadly within warfighting (e.g., Martin Libicki, chapter 18). AI in information operations may play a key role in the “Gray Zone” conflict that has become such a feature of global competition since 2012 (Wright, 2017). The domestic security implications of AI discussed above may also directly feed into thinking about the use of force or other means externally. Domestic security thinking informing external operations were arguably seen with Russia’s recent external use of information operations (Soldatov and Borogan, 2015); and are arguably seen historically in the links between the People’s Republic of China’s thinking on domestic security and its external use of military force (Scobell, 2003).

One critical challenge that may arise from the development of sophisticated digital authoritarian states relates to the profound asymmetry in vulnerability that will create between the United States and China. Such asymmetries can be a cause of profound instability, as is seen now by the US asymmetric dependence on space making that a dangerously tempting target in Sino-US escalation scenarios (Wright, 2018). Recent events show the US political system’s potential vulnerability to foreign digital interference—but if the Chinese regime builds the indefensibly vast digital systems of social governance that it plans, consider how vulnerable they may feel in 5-10 years’ time if that were threatened with disruption. Regime security is often held to be the Chinese leadership’s primary motivation, and attacks on that system may be perceived as threats to the regime. What would happen in a crisis 10 years hence if the then crucial social governance systems in a major city such as Chongqing were essentially turned off? Chinese domestic social governance systems that become ever more reliant on vast digital systems will be tempting targets for adversaries—a fact likely to prompt Chinese regime insecurity that may feed a spiraling security dilemma.

#### Decoupling driven by cyber disputes collapses innovation, causes Chinese tech leap-frogging, and wrecks democracy

Ian Bremmer 18, political scientist and president of the Eurasia Group, with; Nicholas Thompson; 10/23/18, “The AI Cold War That Threatens Us All,” https://www.wired.com/story/ai-cold-war-china-could-doom-us-all/

The Cold War wasn’t inevitable in 1945. The United States and Soviet Union had been allies during World War II, but then a series of choices and circumstances over a five-year period set the conflict on its self-perpetuating track. Similarly, as we can now see in the cold glare of hindsight, it was never inevitable that the digital revolution would inherently favor democracy. Nor is it inevitable today that AI will favor global authoritarianism to the permanent disadvantage of liberalism. If that scenario comes to pass, it will be because a series of choices and circumstances precipitated it.

In the original Cold War, two ideological foes created rival geopolitical blocs that were effectively non-interoperable. The US was boxed out of the Soviet bloc, and vice versa. The same could easily happen again, to disastrous effect. A new cold war that gradually isolates the Chinese and American tech sectors from each other would starve the US of much of the fuel it now relies on for innovation: American companies depend heavily on the Chinese market for their profits and for engineering and software talent. At the same time, it could actually create the kinds of dangers that hawks warn about now: It would increase the risk that one side could surprise the other with a decisive strategic breakthrough in AI or quantum computing.

Right now, maintaining a degree of openness with China is the best defense against the growth of a techno-­authoritarian bloc. That’s not the way American leaders are headed, though.

A little over six months after Donald Trump’s inauguration—and his invocation of “American carnage”—the administration launched a sweeping investigation into China’s trade practices and alleged theft of US technology via cyberspace. That investigation has mushroomed into a steadily escalating trade war, with the US launching tariffs on billions of dollars of Chinese goods and new investment and export restrictions on technologies that China considers key to AI and to its advanced manufacturing ambitions.

The confrontation is about much more than trade. The Trump administration has made it official US policy to protect the “national security innovation base”—White House shorthand for America’s leading technology and talent—from China and other foreign economic predators. In January, Axios published a leaked White House presentation that recommended the US work with its allies to build a 5G network that excludes China, to prevent Beijing from grabbing “the commanding heights of the information domain.” The presentation likened the 21st-century struggle for data dominance to the WWII-era race to construct an atom bomb. Then in April, the US Commerce Department hit ZTE, a leading Chinese telecommunications equipment firm that was gearing up to work on China’s 5G network, with a seven-year ban on doing business with US suppliers; the department said ZTE had violated the terms of a sanctions settlement. (The US later lifted the ban.)

For US security hawks, the prospect that China might dominate both 5G and AI is a nightmare scenario. At the same time, Washington’s escalating pushback against China’s tech ambitions has made Xi even more determined to wean his country off Western technology.

This is a very different philosophy from the one that has guided the technology sector for 30 years, which has favored deeply enmeshed hardware and software supply chains. Shortly before Trump’s inauguration, Jack Ma, the chair of Alibaba, pledged to create a million jobs in the United States. By September 2018, he was forced to admit that the offer was off the table, another casualty in the growing list of companies and projects that are now unthinkable.

Global work in AI has long taken place in three spheres: research departments, corporations, and the military. The first sphere has always been marked by openness and cooperation; to a lesser extent, so has the second. Academics freely share their work. Microsoft has trained many of China’s best AI researchers and helped nurture many promising AI startups, and Alibaba, Baidu, and Tencent employ US engineers at their research hubs in Silicon Valley and Seattle. An AI-driven breakthrough in Shanghai—say, in diagnosing disease through more accurate scans of medical images—can save lives in Shawnee. But national security concerns have a way of overriding commercial considerations. For now, the political momentum appears to be driving the two countries’ tech sectors apart to such a degree that even collaboration between researchers and corporations could be stifled. The schism could well define how the struggle between democracy and authoritarianism plays out.

#### Coop key

Amy Chang 14, Research Associate at the Center for a New American Security, December 2014, “Warring State: China’s Cybersecurity Strategy,” <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Warring%20State%20-%20China%27s%20cybersecurity%20strategy.pdf>

The CCP’s self-preservation priorities drive its foreign policies and foreign cyber activity, which complicates U.S. ability to shape China’s behavior in cyberspace. Many within the United States – from the government to the military to civil society – consider China’s activity as specifically targeted against U.S. interests and assets. In reality, Chinese aims are more diffuse, comprehensive and based on domestic concerns. This means that China would be more likely adhere to international norms and standards of behavior when they allow for sufficient flexibility of interpretation to serve these domestic interests (such as supporting the legitimacy of the Communist Party and maintaining internal political and economic stability). As a result, properly understanding the drivers of Chinese behavior and foreign policy is essential for U.S. effectiveness in negotiations, norm building, and policymaking toward China, regardless of whether the policies are aimed at improving the U.S.-China cyber relationship or at imposing costs on negative behavior.

This report refers to Chinese cyber strategy as “network strategy,” because in China the term “cyber” is rarely used and not fully congruent with how the term is understood in the U.S. policy community. Semantic issues such as these reveal the deep gaps between the two countries’ security infrastructures: While the United States uses the term “cybersecurity”6 to refer to the protection and defense of a wide array of electronic and communications information, China uses the term “network security” (网络安全, wangluo anquan) to refer more specifically to the protection of digital information networks. The term “information security” (信息安全, xinxi anquan) refers to a broader swath of information and communications systems. A more in-depth explanation of terminology will follow.

This report intends to inform U.S. policymakers and analysts interested in cybersecurity of China’s network security strategy, as well as how China views the United States in the cyber domain. It aims to assist in navigating the bilateral cyber relationship, with hopes that improvements in this realm would ameliorate other tensions of the broader U.S.-China relationship. This report focuses on understanding the sources, motives, ideologies, and bureaucratic structure of the Chinese network security strategy.

With China as a key player in international and U.S. cybersecurity considerations, understanding China’s intentions and objectives would aid both the public and private sectors in finding areas of common interest and contention, as well as opportunities for behavior shaping (e.g., deterring or punishing bad behavior in cyberspace). Armed with a deeper understanding of China’s network security strategy, the United States could improve defenses against malicious cyber activity targeting U.S. assets and gain leverage in disincentivizing China from continuing these activities. It would also allow the United States to make tailored improvements in its defense against antagonistic Chinese cyber activity. Finally, it could alleviate concerns about the prospect of cyber conflict instigated by either side, which has in recent years placed stress on the bilateral relationship. A follow-on policy brief to be released in early-2015 based on this research will offer recommendations for U.S. policymakers on how to improve U.S.-China cybersecurity relations, alter China’s risk calculus to deter negative behavior in cyberspace, and modify norms for operating in cyberspace.

### 1AC – Cyber ASATs

#### Outer-space and cyber-space are converging---geopolitical competition and failure to clarify applicable I-law are fueling aggressive strategies

David Fidler 18, the James Louis Calamaras Emeritus Professor of Law at Indiana University, Adjunct Senior Fellow for Cybersecurity and Global Health at the Council on Foreign Relations, 4/3/18, “Cybersecurity and the New Era of Space Activities,” https://www.cfr.org/report/cybersecurity-and-new-era-space-activities

The tasks of securing outer space and cyberspace are converging. The internet increasingly depends on space-enabled communication and information services. Likewise, the operation of satellites and other space assets relies on internet-based networks, which makes these assets, like cars and medical equipment, devices on the internet of things. New government actors, companies, goals, and technologies are expanding and transforming space activities. However, neither space policy nor cybersecurity policy is prepared for the challenges created by the meshing of space and cyberspace, which could increase national security risks.

To meet these challenges, government, industry, and international action is needed. The Donald J. Trump administration’s National Space Council should develop cybersecurity recommendations for space activities, and federal agencies should prioritize these within the government and in cooperation with the private sector. In crafting needed legislation for commercial space activities, Congress should bolster industry efforts to strengthen cybersecurity. Private-sector actors should strengthen their adoption of cybersecurity best practices and collaborate with one another on improving implementation of cybersecurity strategies. Internationally, the United States should pursue collaboration on space cybersecurity through the North Atlantic Treaty Organization (NATO), plurilateral space cooperation mechanisms, and bilateral forums.

Cybersecurity Comes to the Final Frontier

Outer space has been a national security priority for spacefaring nations since the 1950s. Governments started space programs for intelligence, military, political, and scientific purposes and developed countermeasures against space-based threats from rivals, such as anti-satellite capabilities. Countries managed security competition by banning weapons of mass destruction in space and cooperating on peaceful uses of space. Government programs catalyzed private-sector adaptation of dual-use technologies to provide satellite communication services.

Despite the importance of satellites, the U.S. General Accounting Office concluded [PDF] in 2002 that efforts on critical infrastructure protection did not include the satellite industry, but should do so. Similarly, cybersecurity has not been a priority in government and private-sector space endeavors. One leading analysis [PDF] asserted that cybersecurity discussions often overlook space activities’ vulnerability to cyberattack. For example, neither the UN governmental group of experts (GGE) on outer space nor the UN GGE on cyberspace addressed the convergence of their respective agendas.

Governments, critical infrastructure, and economies rely on space-dependent services—for example, the Global Positioning System (GPS)—that are vulnerable to hostile cyber operations. Geopolitical competition fuels the militarization of space, which heightens state incentives to devise cyber espionage, interference, and attack strategies against rivals’ space operations. The United States suspects that China has engaged in cyber operations against U.S. satellites. Chinese military writings emphasize [PDF] the need to target satellites to “blind and deafen the enemy.” The then commander of Air Force Space Command, General John E. Hyten, told Congress in 2016 that “adversaries are developing . . . cyber tools to deny, degrade, and destroy” [PDF] U.S. space capabilities that support war fighting, critical infrastructure, and economic activity. Other countries likely believe the United States is preparing to conduct cyber espionage, disruption, and attack operations against the space assets of rival states.

The commercialization of space heightens cybersecurity concerns for many reasons, including market incentives to lower costs and innovate quickly, often at the expense of software and hardware security. Entrepreneurial activities—dubbed the New Space sector—are underway in space transport, space tourism, asteroid mining, lunar operations, and missions to Mars. A small-satellite (“smallsat”) revolution involving spacecraft far smaller than traditional satellites is unfolding. Networks of linked smallsats can provide internet access, communications, data storage and transmission, imaging, and remote sensing. This next generation of satellites harnesses innovations in computing, electronics, miniaturization, imaging, sensors, big data, and artificial intelligence. Satellite services for Earth observations from space are growing. They support many policy and commercial purposes and contribute to agricultural productivity, transportation efficiency, and environmental monitoring. Commercial space activities use cutting-edge technologies and produce valuable data and are, thus, targets for cyber espionage, including economic cyber espionage, and cybercrime.

Challenges

Space agencies, the satellite industry, cybersecurity researchers, nongovernmental bodies, and intergovernmental satellite organizations show increasing awareness of the space cybersecurity challenge. Nevertheless, experts are worried. NASA’s then chief information security officer, Jeanette Hanna-Ruiz, warned that “it’s a matter of time before someone hacks into something in space.” Chatham House’s David Livingstone asserted that “people are just shuffling . . . paper around” and suggested that only “a disaster” might catalyze serious action. Josh Hartman, a former senior Pentagon official and Air Force officer, argued before the satellite industry’s first cybersecurity summit held in 2017 that, on cybersecurity, “most of the space community . . . has their heads in the sand.” The “attack surface” of space activities is expanding, but governments and industry are not taking adequate action.

Protecting space activities requires understanding the particular cyber vulnerabilities that arise in various space operations. For example, satellite cybersecurity encompasses the satellite itself, transmissions to and from Earth, and ground stations. U.S. military and intelligence satellite systems are vulnerable to kinetic and cyberattacks. Civilian smallsat systems might also prove insecure, given the lack of cybersecurity in their design, their use of commercial off-the-shelf components, and the vulnerabilities potentially created by connecting satellites to operate as complex, orbiting networks.

Neither international law nor diplomacy has grappled effectively with space cybersecurity. Multiple bodies of international law are relevant, but controversies about whether and how international law applies to cyberspace have adversely affected cyber diplomacy. Such travails have elevated the prominence of nongovernmental efforts to clarify international law’s application in cyberspace, such as the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. However, states continue to conduct cyber operations that violate international law. For example, the UN International Telecommunication Union prohibits interference with satellite transmissions, yet such interference frequently occurs.

#### Causes use or lose---escalates crisis---dialogue solves

Laura Grego 20, senior scientist in the Global Security Program at the Union of Concerned Scientists, 1/8/20, “The New U.S. Space Force Will Make Space More Dangerous, Not Less,” https://www.worldpoliticsreview.com/articles/28452/why-the-trump-space-force-will-make-space-more-dangerous

But keeping space secure also requires reducing the threats to satellites. On this score, the Space Force is likely to make space a more contentious and dangerous environment, not less. It’s not just Trump’s rhetoric about dominance in space that is harmful; resources for the new military service will be provided to “deter aggression in, from, and to space.” This will create incentives within the national security bureaucracy to hype the threat of space weapons, and to then build new weapons to counter them.

In a speech last spring outlining his priorities for space, Gen. David L. Goldfein, the chief of staff of the U.S. Air Force, stated that, “It’s not enough to step into the ring and just bob and weave… At some point, we’ve got to hit back.” What Goldfein failed to mention is that the U.S. already has more sophisticated anti-satellite technology than potential adversaries like Russia and China. In fact, having anti-satellite weapons actually does very little to keep one’s own satellites safe from attack. Yet military leaders appear to believe that reserving the option to deny the use of space to potential adversaries is more important than the benefits that come with a less weaponized space.

What’s more, unconstrained development of space weapons will make space more dangerous, costly and unpredictable to use. It will make conflict on Earth riskier, too. A space environment that is perceived as threatening may create an incentive to “use or lose” satellite-enabled military capabilities as a crisis approaches, potentially speeding up conflict. Goldfein underscored this point in remarks following a series of space conflict simulations conducted by the Air Force last month. “In every war game,” he said, “we determined that if you move first in space, you’re not guaranteed to win. But if you move second, you’re likely to lose.”

In the absence of robust international agreements to protect satellites and the outer space environment—the 1967 Outer Space Treaty does not specifically ban non-nuclear weapons from being tested in space or put into orbit—more countries are developing weapons that can destroy satellites in orbit, leaving fast-moving bits of debris that can stay in space for decades and later damage other satellites. When India obliterated its own satellite with an anti-satellite weapon last March, Prime Minister Narendra Modi expressed pride afterward that it had joined an “elite club of space powers.” Testing anti-satellite weapons, much less engaging in an actual conflict in space, can have profound and lasting effects on space. For example, the destruction of a single large satellite in low-Earth orbit would more than double the amount of dangerous debris in these important orbits.

Sensible constraints on this kind of behavior, and limits on dangerous space weapons technologies, would go a long way to augmenting stability, preserving the space environment and avoiding an arms race. But attempts to hammer out such constraints have seen little success. The United Nations Conference on Disarmament has been deadlocked for decades. Negotiations over the European Union’s proposed International Code of Conduct for Outer Space Activities—which would require signatories to resolve not to damage or destroy any satellite except for reasons of safety, self-defense or to avoid debris production—foundered in 2015. Last year, a group of U.N.-convened governmental experts looking at space arms control concluded their deliberations without coming to consensus recommendations.

Still, the outlook is not all bleak. Even without binding legal instruments, no state has ever intentionally destroyed another’s satellite. And in 2018, 87 U.N. member states agreed to voluntary guidelines to protect the long-term sustainability of the space environment.

However, despite the United States having the most investment in space—nearly half of operational satellites are American—it has put very little effort into space-related diplomacy. While the Space Force is big news for the Pentagon, the State Department is nowhere to be seen. Russia and China have repeatedly submitted drafts of their preferred arms control arrangement to the U.N. Conference on Disarmament, most recently in 2014. Their proposed treaty would include binding prohibitions on placing weapons in space and using force or threatening the use of force against satellites. The United States repeatedly rejects these proposals as flawed but declines to provide its own alternative vision.

Despite, or perhaps because of, the deep ideological divides between the world’s great powers, it is critically important that they keep engaging with each other, if only to avoid miscalculation. Information about potential adversaries’ technical capabilities is plentiful, especially in a highly visible domain like space. But assessing their intentions is notoriously difficult. The U.S. and Russia have built some shared understandings over the course of decades of diplomatic engagement, but Washington has little such common ground with China. As a result, the world’s two largest economies risk misinterpreting each other in potentially very serious ways.

Understanding an adversary’s intentions brings more clarity to decision-making in a complex operating environment and may help manage or resolve a conflict more successfully. In 2010, Lincoln P. Bloomfield Jr., a veteran U.S. national security official, warned that without a history of bilateral understandings or crisis management in conflicts involving emerging domains like outer space and cyberspace, there would be “no credible basis for anyone around the president to attribute restraint to the adversary, no track record from which to interpret the actions by the adversary.”

Those risks have not faded in the ensuing decade. If anything, they have multiplied. Doubling down on new space weapons and creating a dedicated Space Force while neglecting to vigorously pursue sensible negotiated constraints seems a sure path to a dangerous future, after having wasted billions of dollars.

#### Cyber and space militarization in parallel with terrestrial security competition makes escalating U.S.-China conflict likely---Taiwan, ECS, SCS, etc---the plan solves by winding down tensions and building trust

Ariel (Eli) Levite 19, nonresident senior fellow in the Nuclear Policy Program at the Carnegie Endowment; and Lyu Jinghua, visiting scholar with Carnegie’s Cyber Policy Initiative, 1/24/19, “Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?,” <https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213>

Compatible visions of the digital economy and comparable power in generating, processing, and using data make the United States and China natural partners to team up and devise understandings to shape cyberspace and its uses in ways that serve their respective national interests and global stability. Yet shared interests and even lofty intentions are no guarantee for collaboration. Both states have their own particular interests in what China sees as informatization and the United States as cyber. Some of these divergent interests or preferences are rooted in different societal values. Others are grounded in specific political and security concerns and requirements that are not only different in the two countries but also at times almost diametrically opposed. For example, the two differ radically on the role of government, let alone the party, in management of cyberspace, freedom of speech (and censorship), citizens’ privacy, and cyber sovereignty.9

Differences are not confined to the general approach toward internet governance. The two countries also seem to think differently about the militarization of cyberspace, the application of international law to cyberwarfare, and the legitimate scope and purpose of cyber espionage. These differences are profound and threaten to undermine the otherwise rosy prospects for bilateral collaboration in cyberspace. They are manifest in the growing suspicion between the United States and China over the security of products made by Chinese vendors of advanced telecommunications equipment; the promotion of the “made in China 2025” policy; and the promotion by China of data retention rules. These reflect the profound mutual distrust on everything associated with cyberspace, data, and well beyond, such as their integration with artificial intelligence technology. This distrust is only deepened by the broader, escalating bilateral trade disputes. Taken together, these trends could threaten the international digital economy writ large, as well as the fragmentation of the internet. Distressingly, they increasingly undermine overall trust in the bilateral relationship.

The risks inherent in this situation are even greater when one considers parallel developments in the security domain. Tensions have been rising between the United States and China over the growing U.S. concern over Chinese military capabilities and modernization, and issues ranging from Taiwan and the East China Sea to the South China Sea and beyond.10 China has similar concerns stemming from the United States’ own military modernization and policies adopted by the United States from Asia Pacific rebalance to Indo-Pacific Strategy and the militarization of space. All these hold serious potential for conflict between the United States and China. If conflict erupts, it would certainly reverberate far and wide. One of the earliest and most destabilizing venues for conflict would be cyberspace, thanks to the potential military utility of early employment of cyber assets. Cyber actions in these scenarios also hold serious escalatory potential, complicating the challenges of keeping conflicts below the level of outright military confrontation and could gravely exacerbate the task of managing such crises.

TOWARD CHINA–U.S. DE-CONFLICTION IN CYBERSPACE

Severe friction as well as profound distrust are certainly disconcerting but they do not necessarily prevent the United States and China from cooperating to prevent the most destabilizing sorts of actions in and through cyberspace. Indeed, some of the sources of tension could also act as incentives to find constructive channels for de-confliction and trust building.

The modern history of arms control may provide a useful guide here. During the Cold War, arms control became a major paradigm for managing great power relations. It was an important means for preventing rivalry and distrust between the United States and the Soviet Union (and subsequently Russia) from spilling over into outright confrontation and an uncontrolled arms race. Naturally, the focus then was predominantly on nuclear weapons and their means of delivery, and on mechanisms to expeditiously address potentially escalatory misunderstandings.

For multiple reasons, cyber does not lend itself to similar measures. Cyber capabilities mostly are dual purpose (far more than nuclear technology) and largely invisible. The key players in cyberspace, unlike nuclear powers, are private sector entities. Verification of commitments pertaining to cyberspace is anywhere between difficult to impossible. Cyber weapons are also viewed as eminently usable compared to nuclear weapons, with certain applications designed, certainly by the United States, to have discriminate, localized, and/or transient effects.

Yet for all the striking differences between cyber weapons and nuclear weapons, the core logic and goals of arms control still apply to cyberspace. Arms control seeks to reduce the likelihood of war, the damage of war if it does occur, and the costs in peacetime of preparing for war. The potential of cyber to precipitate and escalate confrontations and conflicts suggests that the mechanism itself for dialogue and understanding embodied in arms control is even more compelling in the cyber domain in general, and in the U.S.-China context in particular.

#### Those scenarios go nuclear

Michael O’Hanlon 20, senior fellow and director of research in Foreign Policy at the Brookings Institution; and Gregory B. Poling, director of the Asia Maritime Transparency Initiative and a fellow with the Southeast Asia Program at CSIS, 1/14/20, “ROCKS, REEFS, AND NUCLEAR WAR,” https://amti.csis.org/rocks-reefs-and-nuclear-war/

As the 2020s begin, the world can breathe a collective sigh of relief that the United States has so far avoided a major military crisis with China. Over the past decade, China challenged the lawful rights of U.S. partners and allies in the western Pacific, built massive artificial island bases in the disputed Spratly Islands, and actively sought control over all the waters, seabed, and airspace of the South China Sea. Yet the United States has maintained its access to those waters, deterred any major Chinese use of force against its neighbors, and helped support the efforts of Japan to maintain administrative control over the disputed Senkaku Islands in the East China Sea. U.S. strategy has been notably less successful in preventing China from robbing Southeast Asian partners, including U.S. ally the Philippines, of their resources and rights in the South China Sea. But the United States has at least slowed China’s advance while avoiding war.

It would be unwise, however, to assume that the status quo is stable. Deterrence has not failed—yet. China is unlikely to do something as brazen as forcefully denying U.S. Navy or commercial ships access to the South China Sea, attacking American or Japanese bases, or intentionally sinking Filipino sailors in disputed waters. But Beijing continues to probe and test U.S. and allied resolve, provoking low-level crises which could easily escalate. Current U.S. strategic thinking could trigger disproportionate responses that would cause such crises to spiral out of control. That is the way World War I began a century ago—and it could happen again.

War games seem to confirm these historic lessons. One of us has taken part in numerous simulations over the last five years asking seasoned experts and officials to role-play how Chinese, Japanese, Filipino, and American leaders might respond to crises in the South and East China Seas. The results are typically sobering. Some end in a rapid Chinese fait accompli, such as the seizure of a disputed island with minimal cost, while U.S. and allied leaders dither. This type of scenario would lead to considerable damage to international norms, U.S. alliances, and American national security.

Even more simulations rapidly escalate into full-scale conflict, bringing China and the United States to the doorstep of nuclear war over stakes that no rational observer would consider worth it. The U.S. national security community tends to view the ability to defeat China (or Russia) in combat wherever an ally might be attacked as an essential goal. Direct defense or prompt reversal of any aggression, no matter how small, are the foundational principles of current strategy. Article 5 of the NATO treaty and similar mutual defense commitments to Japan and the Philippines treat all aggression as an equally existential threat. So in a scenario involving a Chinese landing on the Japanese-administered Senkakus or a threat to the Sierra Madre—a derelict Philippine navy ship intentionally ran aground at Second Thomas Shoal in the Spratlys and now housing a dozen soldiers—American strategic culture most often leads to the conclusion that kinetic action to retake a seized feature or outpost is justified to avoid abandoning an ally and damaging U.S. credibility.

But such an escalation, while it should be kept as an option, would be fraught. It might end quickly, amounting to little more than a skirmish, or large-scale conflict between nuclear-armed superpowers could ensue. Both sides would have powerful political incentives to escalate further. Military warning and communications systems might be targeted through cyberattack or other means in a way that sowed confusion. Escalation control could not be guaranteed—history and military scholarship strongly suggest as much, and many war games corroborate it.

#### Cyber-weapons are the only usable ASATs---U.S. dependence on satellite infrastructure incentivizes attacks that risk nuclear war

Abhijeet Singh Baghel 19, M.S. in Cybersecurity, Utica College, December 2019, “Cyber Warfare in Outer Space,” ProQuest Dissertations Publishing, document ID: 27670535

A future war in space includes the possibility of one or more anti-satellite (ASAT) attacks which could destroy one or several important satellites and quickly escalate to a nuclear conflict. In 2014, the Obama administration initiated the need to develop new ASAT defense strategies and technology to counter China after its second ASAT test the year before (Kulacki, 2016). Attacking any U.S. intelligence, surveillance, and reconnaissance (ISR) satellite, Global Positioning System (GPS) or communication satellites using missiles such as long-range missiles or Co-Orbital ASATS is expensive, time-consuming, and is hard to keep a secret (Hitchens, 2019d & Wright, 2012). It could be used to deter initial U.S. involvement in conflict but would have devastating impacts on its loss (Please see Appendix A & B for more information).

It is no secret that the U.S.’s major vulnerabilities lie with modernizing the National Airspace System (NAS) and using only one source for timing, navigation, and communication (aka GPS) whereas Russia, Europe, China, and others utilize additional forms of satellite navigation systems (Livingstone & Lewis, 2016). Therefore, only the U.S. would suffer losses with the disruption or destruction of the GPS constellation. To achieve enough damage to the GPS constellation and other space-based assets would require several satellites to be disabled to successfully disrupt the network and disable the U.S. This would have to be done in quick succession before the U.S. could retaliate which is also hard to do and the adversary would have to covertly launch its missiles from several locations or maneuver ASATs currently in orbit to attack its targets. On the other hand, hostile cyber operations are a much bigger threat to the operation of satellites such as GPS (Findler, 2019). As both cyberspace and space assets increasingly rely on each other it is imperative to implement flexible, proactive cybersecurity measures as new threat actors, companies, and technologies are always expanding and evolving space activities (Findler, 2019).

Space and cyberspace share several similarities. Both, along with international waters and airspace, are a global common[s] for the international competition which in turn determines the global distribution of power (Heftye, 2017). Both have applications that affect the everyday lives of many people and economies worldwide (Asbek, 2014). Although cyberspace is a man-made domain, it produces virtual results used for military operations and, along with space, provides adversaries a viable platform for exploitation.

In the last decade the integration of internet-based infrastructure into space systems, such as communications satellites has become an integral part of how satellites operate (Mather, 2018). Along with ASATS, other technologies are being developed to “deny, degrade, deceive, disrupt, or destroy space assets,” thus rendering space infrastructure useless (DOD & DNI, 2011). This includes lasers capable of blinding and knocking down space assets, jamming signals from space, and cyberattacks on satellites which are often considered electronic attacks that are reversable in comparison to orbital threats or nuclear explosions which are irreversible as shown in Figure 1 (Harrison, Johnson, & Roberts, 2019).

The major difference between physical weapons and cyber-attacks is the cost and time associated with an attack. Space assets are vulnerable to cyber threats and the growing dependence on them for commercial and military purposes alike could pose a serious national security threat. There was a time that critical infrastructure was supported by its proprietary technologies of which many have been replaced with internet-based technologies. As a result, nearly anything can be attacked through the internet, especially the interconnected space-assets which will inevitably be a primary target in the case of significant conflict.

#### Satellites key to overall critical infrastructure---attacks risk blackouts and collapse crisis response and deterrence

Patricia Lewis 16, research director for international security at Chatham House; and David Livingstone, associate fellow for international security at Chatham House, 11/21/16, “The cyber threat in outer space,” https://thebulletin.org/2016/11/the-cyber-threat-in-outer-space/

Satellites that orbit the Earth form the exoskeleton of the world’s critical infrastructure. Global communications, air transport, maritime trade, financial services, weather and environmental monitoring, and defense systems all depend on an expansive network of satellites in space. As the September 2014 cyber attack on the US weather system starkly demonstrated, the strategic space-based assets of America and other nations have serious cyber vulnerabilities. In the maritime arena too, space-based monitoring systems are regularly being jammed or spoofed by vessel operators entering false information in order to disguise their illicit activities.

The vulnerability of satellites, their ground stations, and other space assets to cyber attack is often overlooked in wider discussions of cyber threats to critical national infrastructure. Yet just as with other digital networked systems, satellites are vulnerable to cyber attacks that include data theft, jamming, spoofing, and satellite hijacking. All of these present serious risks for societies and critical infrastructures, and analyzing the intersection between cyber security and space security is essential to understanding this evolving problem. So too is the need for an ogranized global effort to confront these threats. Despite some progress at the United Nations and elsewhere, there is currently no international body dedicated to the issue of cyber security in space. Establishing such a multi-stakeholder regime, with the aim of assessing risks and promoting best practices, would begin to close this critical gap.

The nature of the threat. Cyber risks for space-based systems take many forms. While one attack might involve the jamming, spoofing, or hacking of communications or navigational networks, another might target or hijack control systems or specific electronics for missions, shutting down satellites, altering their orbits, or “grilling” their solar cells through deliberate exposure to damaging radiation. Still another might strike at satellite control centers on the ground.

As in other areas of cyber conflict, players and motivations abound. States or non-state armed groups could use such attacks to create military advantages in space prior to or during a war. Government agencies or corporations with sufficient computing power to crack encryption codes could use cyber attacks on satellite systems to steal strategic quantities of intellectual property. Well-resourced criminal organizations could steal significant amounts of cash. Groups or even governments could initiate catastrophic levels of satellite run-ins with space debris, perhaps even causing a cascade of collisions—called the Kessler Effect—that could deny everyone the use of space for the foreseeable future. Even individual hackers who simply want to show off their skills could create inadvertent mayhem.

Perhaps the most worrying vulnerabilities involve satellite-enabled navigational systems. Many such systems have been developed, from Europe (notably the new Galileo system) to Asia, but the most ubiquitous is the US global-positioning system commonly known as GPS. Much of the world’s infrastructure relies on this system, yet it was not originally intended for civilian use, and therefore not designed with security in mind. A successful spoofing cyber attack could introduce erroneous timing signals, which are used for determining precise locations. Aimed at a power grid, this type of manipulation could potentially trigger catastrophic overloads, leading to cascading equipment failures and even major blackouts. Spoofers could also target banks and stock exchanges by manipulating automated time-stamps on transactions. Earlier this year, when 15 satellites accidentally broadcast signals that were inaccurate by 13 microseconds, telecom companies using Chronos GPS services were hit with 12 hours of thousands of system errors.

The threat to military technology looms large as well. Not enough attention has been paid, at least not in the open literature, to the increasing vulnerability of space-based assets, ground stations, and associated command-and-control systems. Cyber attacks on satellites have the potential to undermine the integrity of strategic-weapons systems and destabilize deterrence relationships. And in the event of a military crisis, the potential for cyber attacks could cast doubt on intelligence and increase the risk of misperception, not to mention threaten missile systems, both strategic and tactical, which rely on satellites and the space infrastructure for navigation and targeting, command and control, operational monitoring, and other functions. Because cyber technologies are within the grasp of most states and non-state actors, they level the strategic field and create hitherto unparalleled opportunities for small belligerent governments or terrorist groups to instigate high-impact attacks.

Your smart fridge isn’t helping. As satellites and satellite constellations continue to grow in number—a very good thing in terms of human connectedness, scientific research, and space exploration—so do entry points and communications pathways for cyber attacks, the so-called Internet of Things (or, as we now like to think of it, Gadgnet) that has sprung up due to our love of digital devices. Yet cyber defenses have failed to keep up with this growth, mostly due to the high cost of (optional) built-in security in a world of smaller and cheaper satellites, even though this is ultimately the most cost-effective and sustainable approach to cyber safety in space.

The international supply chain of satellite components, with the associated uncertainties about provenance and standards of production, along with back-door holes in encryption, is increasingly hard to regulate. The costs associated with cyber security, in both software and hardware, are rising, and in low-cost space missions where the commercial price of implementing security measures rivals the value of the mission, the temptation to neglect them and hope for the best is high. In the rush to get products to market, designers and manufacturers often skip or pay only passing attention to important security controls. This is already causing immense concern for machine designers, manufacturers, and insurance companies. Indeed, the October 2016 Dyn attack that resulted in denial-of-service strikes on major websites such as Twitter, Spotify, and Reddit appears to have harnessed botnets on personal computers through poorly secured home devices connected to each other and the outside world through wireless routers.

Reducing risks, building resilience. The 2011 US International Strategy for Cyberspace stressed that international approaches and cooperation are needed in order to address and mitigate the full range of cyber threats to military systems, and indeed international cooperation will be crucial in any response to space-based cyber threats, both military and civilian.

#### NC3 and infrastructure attacks cause extinction

Michael T. Klare 19, professor emeritus of peace and world security studies at Hampshire College and senior visiting fellow at the Arms Control Association, November 2019, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation,” <https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation>

In January 2018, details of the Trump administration’s Nuclear Posture Review (NPR) were posted online by the Huffington Post, provoking widespread alarm over what were viewed as dangerous shifts in U.S. nuclear policy. Arousing most concern was a call for the acquisition of several types of low-yield nuclear weapons, a proposal viewed by many analysts as increasing the risk of nuclear weapons use.

Another initiative incorporated in the strategy document also aroused concern: the claim that an enemy cyberattack on U.S. nuclear command, control, and communications (NC3) facilities would constitute a “non-nuclear strategic attack” of sufficient magnitude to justify the use of nuclear weapons in response.

Under the Obama administration’s NPR report, released in April 2010, the circumstances under which the United States would consider responding to non-nuclear attacks with nuclear weapons were said to be few. “The United States will continue to…reduce the role of nuclear weapons in deterring non-nuclear attacks,” the report stated. Although little was said about what sort of non-nuclear attacks might be deemed severe enough to justify a nuclear response, cyberstrikes were not identified as one of these. The 2018 NPR report, however, portrayed a very different environment, one in which nuclear combat is seen as increasingly possible and in which non-nuclear strategic threats, especially in cyberspace, were viewed as sufficiently menacing to justify a nuclear response. Speaking of Russian technological progress, for example, the draft version of the Trump administration’s NPR report stated, “To…correct any Russian misperceptions of advantage, the president will have an expanding range of limited and graduated [nuclear] options to credibly deter Russian nuclear or non-nuclear strategic attacks, which could now include attacks against U.S. NC3, in space and cyberspace.”1

The notion that a cyberattack on U.S. digital systems, even those used for nuclear weapons, would constitute sufficient grounds to launch a nuclear attack was seen by many observers as a dangerous shift in policy, greatly increasing the risk of accidental or inadvertent nuclear escalation in a crisis. “The entire broadening of the landscape for nuclear deterrence is a very fundamental step in the wrong direction,” said former Secretary of Energy Ernest Moniz. “I think the idea of nuclear deterrence of cyberattacks, broadly, certainly does not make any sense.”2

Despite such admonitions, the Pentagon reaffirmed its views on the links between cyberattacks and nuclear weapons use when it released the final version of the NPR report in February 2018. The official text now states that the president must possess a spectrum of nuclear weapons with which to respond to “attacks against U.S. NC3,” and it identifies cyberattacks as one form of non-nuclear strategic warfare that could trigger a nuclear response.

That cyberwarfare had risen to this level of threat, the 2018 NPR report indicated, was a product of the enhanced cybercapabilities of potential adversaries and of the creeping obsolescence of many existing U.S. NC3 systems. To overcome these vulnerabilities, it called for substantial investment in an upgraded NC3 infrastructure. Not mentioned, however, were extensive U.S. efforts to employ cybertools to infiltrate and potentially incapacitate the NC3 systems of likely adversaries, including Russia, China, and North Korea.

For the past several years, the U.S. Department of Defense has been exploring how it could employ its own very robust cyberattack capabilities to compromise or destroy enemy missiles from such states as North Korea before they can be fired, a strategy sometimes called “left of launch.”3 Russia and China can assume, on this basis, that their own launch facilities are being probed for such vulnerabilities, presumably leading them to adopt escalatory policies such as those espoused in the 2018 NPR report. Wherever one looks, therefore, the links between cyberwar and nuclear war are growing.

The Nuclear-Cyber Connection

These links exist because the NC3 systems of the United States and other nuclear-armed states are heavily dependent on computers and other digital processors for virtually every aspect of their operation and because those systems are highly vulnerable to cyberattack. Every nuclear force is composed, most basically, of weapons, early-warning radars, launch facilities, and the top officials, usually presidents or prime ministers, empowered to initiate a nuclear exchange. Connecting them all, however, is an extended network of communications and data-processing systems, all reliant on cyberspace. Warning systems, ground- and space-based, must constantly watch for and analyze possible enemy missile launches. Data on actual threats must rapidly be communicated to decision-makers, who must then weigh possible responses and communicate chosen outcomes to launch facilities, which in turn must provide attack vectors to delivery systems. All of this involves operations in cyberspace, and it is in this domain that great power rivals seek vulnerabilities to exploit in a constant struggle for advantage.

The use of cyberspace to gain an advantage over adversaries takes many forms and is not always aimed at nuclear systems. China has been accused of engaging in widespread cyberespionage to steal technical secrets from U.S. firms for economic and military advantages. Russia has been accused, most extensively in the Robert Mueller report, of exploiting cyberspace to interfere in the 2016 U.S. presidential election. Nonstate actors, including terrorist groups such as al Qaeda and the Islamic State group, have used the internet for recruiting combatants and spreading fear. Criminal groups, including some thought to be allied with state actors, such as North Korea, have used cyberspace to extort money from banks, municipalities, and individuals.4 Attacks such as these occupy most of the time and attention of civilian and military cybersecurity organizations that attempt to thwart such attacks. Yet for those who worry about strategic stability and the risks of nuclear escalation, it is the threat of cyberattacks on NC3 systems that provokes the greatest concern.

This concern stems from the fact that, despite the immense effort devoted to protecting NC3 systems from cyberattack, no enterprise that relies so extensively on computers and cyberspace can be made 100 percent invulnerable to attack. This is so because such systems employ many devices and operating systems of various origins and vintages, most incorporating numerous software updates and “patches” over time, offering multiple vectors for attack. Electronic components can also be modified by hostile actors during production, transit, or insertion; and the whole system itself is dependent to a considerable degree on the electrical grid, which itself is vulnerable to cyberattack and is far less protected. Experienced “cyberwarriors” of every major power have been working for years to probe for weaknesses in these systems and in many cases have devised cyberweapons, typically, malicious software (malware) and computer viruses, to exploit those weaknesses for military advantage.5

Although activity in cyberspace is much more difficult to detect and track than conventional military operations, enough information has become public to indicate that the major nuclear powers, notably China, Russia, and the United States, along with such secondary powers as Iran and North Korea, have established extensive cyberwarfare capabilities and engage in offensive cyberoperations on a regular basis, often aimed at critical military infrastructure. “Cyberspace is a contested environment where we are in constant contact with adversaries,” General Paul M. Nakasone, commander of the U.S. Cyber Command (Cybercom), told the Senate Armed Services Committee in February 2019. “We see near-peer competitors [China and Russia] conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage.”

Although eager to speak of adversary threats to U.S. interests, Nakasone was noticeably but not surprisingly reluctant to say much about U.S. offensive operations in cyberspace. He acknowledged, however, that Cybercom took such action to disrupt possible Russian interference in the 2018 midterm elections. “We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts,” he testified in February. According to press accounts, this included a cyberattack aimed at paralyzing the Internet Research Agency, a “troll farm” in St. Petersburg said to have been deeply involved in generating disruptive propaganda during the 2016 presidential elections.6

Other press investigations have disclosed two other offensive operations undertaken by the United States. One called “Olympic Games” was intended to disrupt Iran’s drive to increase its uranium-enrichment capacity by sabotaging the centrifuges used in the process by infecting them with the so-called Stuxnet virus. Another left of launch effort was intended to cause malfunctions in North Korean missile tests.7 Although not aimed at either of the U.S. principal nuclear adversaries, those two attacks demonstrated a willingness and capacity to conduct cyberattacks on the nuclear infrastructure of other states.

Efforts by strategic rivals of the United States to infiltrate and eventually degrade U.S. nuclear infrastructure are far less documented but thought to be no less prevalent. Russia, for example, is believed to have planted malware in the U.S. electrical utility grid, possibly with the intent of cutting off the flow of electricity to critical NC3 facilities in the event of a major crisis.8 Indeed, every major power, including the United States, is believed to have crafted cyberweapons aimed at critical NC3 components and to have implanted malware in enemy systems for potential use in some future confrontation.

Pathways to Escalation

Knowing that the NC3 systems of the major powers are constantly being probed for weaknesses and probably infested with malware designed to be activated in a crisis, what does this say about the risks of escalation from a nonkinetic battle, that is, one fought without traditional weaponry, to a kinetic one, at first using conventional weapons and then, potentially, nuclear ones? None of this can be predicted in advance, but those analysts who have studied the subject worry about the emergence of dangerous new pathways for escalation. Indeed, several such scenarios have been identified.9

The first and possibly most dangerous path to escalation would arise from the early use of cyberweapons in a great power crisis to paralyze the vital command, control, and communications capabilities of an adversary, many of which serve nuclear and conventional forces. In the “fog of war” that would naturally ensue from such an encounter, the recipient of such an attack might fear more punishing follow-up kinetic attacks, possibly including the use of nuclear weapons, and, fearing the loss of its own arsenal, launch its weapons immediately. This might occur, for example, in a confrontation between NATO and Russian forces in east and central Europe or between U.S. and Chinese forces in the Asia-Pacific region.

Speaking of a possible confrontation in Europe, for example, James N. Miller Jr. and Richard Fontaine wrote that “both sides would have overwhelming incentives to go early with offensive cyber and counter-space capabilities to negate the other side’s military capabilities or advantages.” If these early attacks succeeded, “it could result in huge military and coercive advantage for the attacker.” This might induce the recipient of such attacks to back down, affording its rival a major victory at very low cost. Alternatively, however, the recipient might view the attacks on its critical command, control, and communications infrastructure as the prelude to a full-scale attack aimed at neutralizing its nuclear capabilities and choose to strike first. “It is worth considering,” Miller and Fontaine concluded, “how even a very limited attack or incident could set both sides on a slippery slope to rapid escalation.”10

What makes the insertion of latent malware in an adversary’s NC3 systems so dangerous is that it may not even need to be activated to increase the risk of nuclear escalation. If a nuclear-armed state comes to believe that its critical systems are infested with enemy malware, its leaders might not trust the information provided by its early-warning systems in a crisis and might misconstrue the nature of an enemy attack, leading them to overreact and possibly launch their nuclear weapons out of fear they are at risk of a preemptive strike.

“The uncertainty caused by the unique character of a cyber threat could jeopardize the credibility of the nuclear deterrent and undermine strategic stability in ways that advances in nuclear and conventional weapons do not,” Page O. Stoutland and Samantha Pitts-Kiefer wrote in 2018 paper for the Nuclear Threat Initiative. “[T]he introduction of a flaw or malicious code into nuclear weapons through the supply chain that compromises the effectiveness of those weapons could lead to a lack of confidence in the nuclear deterrent,” undermining strategic stability.11 Without confidence in the reliability of its nuclear weapons infrastructure, a nuclear-armed state may misinterpret confusing signals from its early-warning systems and, fearing the worst, launch its own nuclear weapons rather than lose them to an enemy’s first strike. This makes the scenario proffered in the 2018 NPR report, of a nuclear response to an enemy cyberattack, that much more alarming.

Yet another pathway to escalation could arise from a cascading series of cyberstrikes and counterstrikes against vital national infrastructure rather than on military targets. All major powers, along with Iran and North Korea, have developed and deployed cyberweapons designed to disrupt and destroy major elements of an adversary’s key economic systems, such as power grids, financial systems, and transportation networks. As noted, Russia has infiltrated the U.S. electrical grid, and it is widely believed that the United States has done the same in Russia.12 The Pentagon has also devised a plan known as “Nitro Zeus,” intended to immobilize the entire Iranian economy and so force it to capitulate to U.S. demands or, if that approach failed, to pave the way for a crippling air and missile attack.13

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread chaos and harm and eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, such attacks “could lead to major conflict and possibly nuclear war.”14

These are by no means the only pathways to escalation resulting from the offensive use of cyberweapons. Others include efforts by third parties, such as proxy states or terrorist organizations, to provoke a global nuclear crisis by causing early-warning systems to generate false readings (“spoofing”) of missile launches. Yet, they do provide a clear indication of the severity of the threat. As states’ reliance on cyberspace grows and cyberweapons become more powerful, the dangers of unintended or accidental escalation can only grow more severe.

‘Defending Forward’

Under these circumstances, one would think the major powers would seek to place restrictions on the use of offensive cyberweapons, especially those aimed at critical NC3 systems. This approach, however, is not being pursued by the United States and the other major powers.

Under the Obama administration, the Department of Defense was empowered to conduct offensive cyberstrikes on foreign states and entities in response to like attacks on the United States, but any such moves required high-level review by the White House and were rarely approved. This approach was embedded in Presidential Policy Directive 20 (PPD-20), adopted in October 2012, which states that any cyberaction that might result in “significant consequences,” such as loss of life or adverse foreign policy impacts, required “specific presidential approval.”

Officials in the Trump administration found this requirement unduly restrictive and so persuaded the president to rescind PPD-20 and replace it with a more permissive measure. The resulting document, National Security Presidential Memorandum 13 (NSPM-13), was approved in September 2018 but has not been made public. From what is known of NSPM-13, senior military commanders, such as Nakasone, enjoy preapproval to undertake offensive strikes against foreign entities under certain specified conditions without further White House clearance. In accordance with the new policy, military planners can prepare for offensive cyberattacks by seeking vulnerabilities in adversarial computer networks and by implanting malware in these weak spots for potential utilization if a retaliatory strike is initiated.15

As translated into formal military doctrine, this approach is described as “defending forward,” or seeking out the originators of cyberattacks aimed at this country and neutralizing them through counterstrikes and the insertion of malware for future activation. “Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries’ weaknesses, learn their intentions and capabilities, and counter attacks close to their origins.”16

In embracing this strategy, Nakasone and other senior officials insist that their intention is defensive: to protect U.S. cyberspace against attack and deter future assaults by letting opponents know their own systems will be crippled if they persist in malicious behavior. “For any nation that’s taking cyber activity against the United States,” said National Security Advisor John Bolton when announcing the adoption of NSPM-13, “they should expect…we will respond offensively as well as defensively.”17 For any potential adversary following these developments, defending forward will certainly be interpreted as preparation for offensive strikes in the event of a crisis, inviting stepped up defensive and offensive moves on their part.

#### Yes miscalc---their authors are overly optimistic

Alexander Klimburg 20, non-resident senior fellow at the Atlantic Council, February-March 2020, “Mixed Signals: A Flawed Approach to Cyber Deterrence,” Survival, Vol. 62, No. 1, p. 107-130

The empirical justification of CYBERCOM’s new offensive vision has been shaky from the start. The academic underpinnings of persistent engagement were presented in a 2017 article by Richard Harknett and Michael Fischerkeller, which was released just as the former was concluding his stint as CYBERCOM’s first resident scholar.9 The very title of the article, ‘Deterrence Is Not a Credible Strategy for Cyberspace’, indicates that the authors thought it was possible (and desirable) to frame the strategy as one of ‘non-deterrence’. Their analysis rests on the belief that, as part of an ‘agreed competition’ concept, it would be possible to completely contain cyber conflict within its own domain. This would be non-escalatory due to the invisible hand of ‘tacit bargaining’, through which adversaries would feel out the borders of allowable conflict and come to a stable conflict scenario. According to this logic, not only is there less chance of inadvertent escalation over the threshold of armed conflict when engaging in the cyber domain, but this kind of engagement would also avoid retaliation in other domains, such as diplomacy and trade, or even in physical conflict zones, such as Syria and the Persian Gulf. The authors also seem to suggest that cyber could effectively function as a ‘pressure valve’ for international tensions, concentrating the inevitable tit for tat (the tacit bargaining) of international security to a more controllable and less dangerous environment.10

The many suppositions of Harknett and Fischerkeller’s article have been roundly criticised.11 Although the idea of agreed competition is presented as deriving from Herman Kahn’s idea of ‘agreed battle’, the article never answers the basic question of why an adversary would allow itself to be constrained in a way that clearly favours the United States. Cyber experts Brandon Valeriano and Benjamin Jensen have drawn on a comprehensive historical dataset of cyber operations to argue instead that such operations on their own seldom produce concessions. Normally, they need to be accompanied by other actions, such as diplomatic overtures, to work – an approach which the authors contend the US has employed to great effect in the past, despite Nakasone’s assessment that cyber deterrence has failed.12 Overall, few observers would agree that outcomes in cyberspace are as easy to predict as advocates of persistent engagement seem to believe. On the contrary, the basic assumption of diplomacy over at least the last decade is that cyberspace is the domain most prone to misinterpretation and miscalculation.13 Finally, there is no clear theory of victory in persistent engagement and no strategic endgame, only the purpose of creating operational advantages in cyberspace. There is no agreement as to what the basic strategic game is, or what constitutes its winning and losing factors.

### 1AC – Plan

#### The United States federal government should seek to create with the People’s Republic of China jointly agreed-upon restraints on interference with space assets via cyberspace, including defining thresholds for harmful interference and armed attack.

### 1AC – Solvency

#### Legally-binding cyber TCBMs solve

Dr. Rajeswari Pillai Rajagopalan 19, Distinguished Fellow and Head of the Nuclear and Space Policy Initiative at the Observer Research Foundation, the Technical Advisor for a UN Group of Governmental Experts on Prevention of Arms Race in Outer Space, May 2019, “Electronic and Cyber Warfare in Outer Space,” https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf

This paper suggests that, as the development of counter-space technologies accelerates, there is a growing need to develop more effective and viable global instruments that limit the potentially dangerous consequences of these new capabilities. Nevertheless, the global debate has not gone far, with broadly two perspectives. One perspective is that legally binding measures are necessary, while the other argues that such legal treaties are difficult to conclude, suggesting instead that the international community should pursue voluntary transparency and confidence-building measures (TCBMs). This dialogue played out most recently in the Group of Governmental Experts on further practical measures for the prevention of an arms race in outer space, which met in Geneva for its final session in March 2019. This Group was unable to reach consensus on a report or to make any further recommendations in part because some States do not think that adopting an effective treaty is possible at this time and that voluntary measures should be pursued. Building consensus between these two camps is critical. But several factors, including the changing balance of global and regional power dynamics, have hampered the process of building an agreement between them. Given that this is a long-term challenge, there are those who articulate a middle path in the form of legally binding TCBMs.

Irrespective of the form and type of new efforts, the need for definitional clarity on a range of concepts is clear. Terms such as ‘space weapon’, ‘weaponization of space’ and ‘peaceful uses of space’ need to be defined clearly if the challenges of counter-space technologies—especially electronic and cyber warfare technologies—are to be dealt with in an effective manner. The existing legal regime has been insufficient to address these electronic and cyber warfare challenges. Given that literally any object in space can be used in a nefarious manner, to be prudent States could focus on behaviour and activities that an object in space is used for. Indeed, this was a conclusion of the 2013 Group of Governmental Experts report on Transparency and Confidence-Building Measures in Outer Space Activities.55

In the coming years, the international community will need to consider which electronic and cyber activities in outer space it will focus on to ensure outer space remains safe, secure and accessible. This requires tackling some difficult questions with a view to achieving some kind of common understanding. What, for example, should be the criteria for deciding that an electronic or cyber attack has taken place? Building a consensus among States on this question will not be easy. It is likely that most States will agree that an attack has taken place if it leads to physical destruction of space assets or causes fatalities. But it is likely more difficult to reach an agreement on this question when a State or a private corporation has used electronic or cyber measures for tampering with or stealing data or interference that does not lead to destruction of physical assets. Though unauthorized access would usually be considered a crime, whether it would amount to international aggression is not clear cut. Reaching some agreement—at the least—on what is clearly prohibited and potential casus belli should be considered a priority. There should also be discussion on where to set the bar. Should it be set so low that only the most egregious offensive act is deemed illegitimate? What would be the broader implications for the rule of law and relations between States?

Any new international measure that is developed, whether it is a legally binding treaty on the prevention of arms race in outer space or a new Code of Conduct, will need to consider whether to make a distinction between electronic and cyber technologies on the one hand and kinetic means on the other. It is not necessary that both of these types of capabilities be dealt with in the same instrument: they could be addressed through distinct measures. It is likely that some States will wish to retain the option to use electronic and cyber measures, for reasons explained earlier, even if they are reluctant to use kinetic means. One way forward might be to focus on the effects of an attack, irrespective of the means used. Also, given the interlinkages between these technologies, electronic and cyber warfare issues may be brought into discussions in information and communication technology forums as well. This will require more cross-cutting conversations that transcend existing policy and technical discourses, which are frequently siloed.

Another related concern is that of adjudicating complaints about electronic and cyber attacks. By their very nature, use of such means is not easy to detect or trace even after an attack has taken place. Ideally, accusations of such attacks need to be arbitrated neutrally. While mechanisms exist for such neutral arbitration in some areas, this remains the exception rather than the norm. One possibility would be an agency with a UN mandate in order to promote global participation that will have international legitimacy.

Developing consensus on some of these pragmatic aspects of addressing electronic and cyber warfare will not be easy. Yet the importance of outer space to the entire global community means that outlining the rules of the road is necessary in order to limit their negative consequences. An initial step could be to work jointly on a simple working definition of what constitutes armed attack in space. Important questions that arise in this regard include whether electronic and cyber attacks such as hacking, jamming, or spoofing a satellite can be considered as an armed attack and how and whether such actions become a threat to international peace and security. Issues such as the threshold for the use of force under such a scenario, as well as what might be a proportionate response to such attacks against space objects, could also be tackled in these discussions. Of course, these questions could become even more complicated especially when third parties such as commercial actors are involved. It would be advisable to stay aligned with the current dominant legal opinion that scale and effects of an attack should determine whether the armed attack has taken place. While this may not be entirely satisfactory, it is consistent with current legal standards. The next step would be to assess States’ responsibility—especially due to the increasing prevalence of non-State actors in outer space activities. Security Council resolution 1540 provides a potential solution because it mandates each State to control the actions of citizens and individuals within its borders.56 With regard to cyber and electronic warfare in outer space, following the resolution 1540 example, it could be made clearer that States are responsible for ensuring attacks are prevented from within their territory.

Discussing these issues in the UN Disarmament Commission could be an appropriate way to begin this process of moving toward future regulation, and it would contribute to greater understanding and, hopefully, policy convergence. The Commission could choose from a number of tracks, from a broad approach discussing electronic and cyber warfare in outer space in a general sense, to a narrower approach in which specific issues are taken up. In view of what has been explored in this paper, some specific issues for consideration could be: defining what an armed attack against an outer space object is; the requirements for verification and monitoring mechanisms in any future mechanism; and a mapping exercise laying out the national technical means to undertake verification and monitoring. The outcomes of these discussions could subsequently be directed to the General Assembly First Committee and Security Council for further action.

#### Bilateral dialogue key---spills up

David Livingstone 16, associate fellow at Chatham House, was policy lead on Military Aid to the Civil Powers at the UK Ministry of Defence between 1994 and 1999; and Patricia M. Lewis is the research director of the International Security Department at Chatham House, September 2016, “Space, the Final Frontier for Cybersecurity?” <https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf>

An international response is required to the cybersecurity challenges of space, but there are no relevant international organizations or agreed mechanisms that could conceivably constitute the basis for that response. A framework needs to be developed quickly to harmonize the space supply chain and its offerings, which are now being market-led. However, government-to-government dialogue in international security matters works slowly, particularly through UN and ITU structures, as does the academic discourse. In the international structures, there are a number of frameworks and international agreements for addressing international peace and security in space, including the Committee on the Peaceful Uses of Outer Space (COPUOS); the UN Office for Outer Space Affairs; the Disarmament Commission; the Conference on Disarmament and the UN Office of Disarmament Affairs; the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (the Outer Space Treaty); the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space; the Convention on International Liability for Damage Caused by Space Objects; the Convention on Registration of Objects Launched into Outer Space; the Constitution and the Convention of the International Telecommunication Union and its Radio Regulations (amended).

Recent progress has been made in the Wassenaar Arrangement53 and two UN processes: the Group of Governmental Experts on Transparency and Confidence-building Measures in Outer Space Activities (GGE-Space);54 and the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE-Cyber). In addition, space and cyber guidelines are currently being discussed within COPUOS,55 including, for example, Guideline 9 (formerly guideline 43) to ‘implement policy aimed at precluding interference with the operation of foreign space objects through unauthorized access to their on-board hardware and software’ and Guideline 18 (formerly guideline 35) to ‘ensure the safety and security of terrestrial infrastructure that supports the operation of orbital systems and respect the security of foreign space-related terrestrial and information infrastructures’.

[BOX 1 OMITTED]

[BOX 2 OMITTED]

The new dialogue on cybersecurity at senior official levels between the United States and China could be the start of a process that will operationalize the GGE-Cyber’s call to establish ‘dialogue on security and common understandings on the application of international law and norms, rules and principles for responsible behaviour’. The 2015 US–China cyber agreement was part of a wider group of measures to strengthen bilateral relations and build trust and confidence between the two countries. The agreement includes: i) timely responses to requests for information and assistance concerning malicious cyber activities; ii) cooperation in the investigation of cybercrimes, including the collection of electronic evidence, and mitigation of malicious cyber activity emanating from the territories of either party; iii) agreement not to conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information; iv) identifying and promoting appropriate norms of state behaviour in cyberspace within the international community; v) a high-level joint dialogue mechanism on cybercrime and related issues; and vi) a hotline for the escalation of issues that may arise in the course of responding to such requests.58

Any proposed organization to address cybersecurity in space needs to reflect the multi-stakeholder character of the cyber and space communities.59 Its structure would need to be fundamentally nonregulatory and sensitive to national perspectives in cybersecurity policies, accepting the need for regulation where necessary, and yet being nimble and responsive – in other words, everything that most governmental organizations are not. To begin with, and to ensure sensibilities are protected, the regime should set out simply to instil a culture of ‘getting the basics right’ – which, according to experts in the field, constitutes 80 per cent of the strategic response.60

All participants and stakeholders in this regime need to understand this objective. The essence of the regime is that it works from all perspectives – organizational, business change and obsolescence management – to give it competitive advantage over its adversaries. The regime must be agile and act with initiative; actor-neutral; risk-based; and able to understand that a system level of response (i.e. based on technology alone) is not the answer. Not only that, but its core deliverable is to increase collaboration and cooperation in this highly dynamic environment in order to enhance knowledge. The outputs it generates will be hard to measure, as its success depends on a reduction in the number of attacks, in a domain where these have not been reported widely, making it hard to ascertain their absence.

The response to space cyber insecurity should be based on soft power, rather than controls underpinned by an international diplomatic community moving at glacial pace with a series of ‘sticks’ wielded by national regulators. The approach required must be from an international community of the willing responding to ‘carrots’, who have a shared awareness of the problem and a shared goal. Such an approach offers the most appropriate basis for an international space cybersecurity strategy that includes – rather than mandates – a wide variety of stakeholders with the necessary agility and flexibility. The regime would develop the essential ‘top-down’ approach needed to complement the ‘bottom-up’ security measures being developed by technological experts and state organizations assisting with intelligence and threat information and with highly complex forensics work.

The regime needs to be a platform for communication and collaboration rather than taking any operational steps, or even overseeing tactical procedures, to increase security. From the outset, those functions would be left to national regulation and law enforcement authorities that may already be able to work with other states via existing bilateral and multilateral instruments designed to tackle other risks to society. However, research in other cybersecurity domains suggests that there is little history of successful institutional sharing, and this is perhaps the most critical failure of all. The regime’s philosophy should therefore be based on a sharing economy. This may not suit some national authorities, however, given their traditional concern with security, which is principally directed at threats to the state and terrorist attacks.

Nevertheless, some states that already work in multilateral risk-reduction and multi-stakeholder enterprises may be more relaxed about participating in an international community of the willing. Such a regime would focus on cooperation and information-sharing in its early phases, if only to explore and set up systems for joint working and collaboration that can be expanded incrementally over time, and include more stakeholders as confidence increases. The regime would, however, have to recognize that any analysis it undertakes of cyberspace and related security threats is a problem that concerns all of society; not the exclusive concern of governments, commercial enterprises or international organizations. As noted above, in cyberspace security, different interests and constituencies are challenged by a variety of interconnected actors and actions. And if society – for all its diversity – cannot respond in a similarly interconnected way, then the sum of security diminishes overall and becomes dangerous.

This prospective multi-stakeholder alliance should initially be made up of those states and non-state entities that already have a relatively high national-level awareness of cyber risks and commensurately mature countervailing strategies, and that also accept the need for a decentralized approach. Such a group will be able to swiftly and collectively identify sets of core capabilities, particularly in best practices within each of their national strategies, and to produce those as industry-led standards for the benefit of an expectant community of interest. This will constitute the beginnings of a space cybersecurity regime.

#### Dialogue over cyber-norms enables complex learning that transforms states’ perceptions of their interests---that overcomes definitional and verification challenges---nuclear arms control proves

Mischa Hansel 18, Assistant Professor at the Institute for Political Science and European Affairs at the University of Cologne; Max M. Mutschler, Researcher at the German Institute for International and Security Affairs; and Marcel Dickow, deputy head of the International Security Division of the German Institute for International and Security Affairs, 2018, “Taming cyber warfare: lessons from preventive arms control,” Journal of Cyber Policy, <https://doi.org/10.1080/23738871.2018.1462394>

While nuclear weapons and cyber weapons differ in numerous ways, there is a stunning similarity regarding their perception as revolutionary technologies and the way they challenged strategic wisdom and provoked learning processes (Nye 2011). In this paper, we argue that such learning processes can lead to redefinitions of strategic interests, and that these changes of preferences are perhaps more important to the success or failure of arms control efforts than definitional or verification challenges. In this view, the history of nuclear weapons – more than other technological histories and despite all technological dissimilarities – is indeed highly relevant for the issue of preventive arms control in cyberspace.

Therefore, we look back at a particular episode of nuclear competition, namely strategic missile defence and the ambiguities surrounding the technologies behind it. More specifically, we offer an analysis of the establishment of the AMB Treaty, an achievement that was regarded highly unlikely by strategists only a few years before it came into existence. The case of the ABM Treaty is instructive because it shows that neither definitional vagueness nor unequal relative gains proved to be insurmountable obstacles for cooperation. Rather, the transformation of strategic interests through complex learning was key to the achievement of the ABM Treaty. Recent developments in cybersecurity negotiations show that similar learning processes are underway, although progress and setbacks are going hand in hand. This is not to say that definitional and verification problems can be easily solved and that a treaty prohibiting cyber weapons is possible. But there is reason to believe that complex learning can transform perceived interest, just like it did during the Cold War, and that international norms against certain cyber attacks can be established.

# Fun 2AC Stuff

### 2AC -- President Key

#### President key---rhetoric gaps wreck solvency

Jason Healey 19, Senior Research Scholar in the Faculty of International and Public Affairs and Adjunct Professor of International and Public Affairs at Columbia University, was the founding director of the Cyber Statecraft Initiative of the Atlantic Council where he remains a Senior Fellow, president of the Cyber Conflict Studies Association, August 2019, “The implications of persistent (and permanent) engagement in cyberspace,” Journal of Cybersecurity, Vol. 5, No. 1, p. 1-15

Persistent engagement will place military and intelligence forces in close contact, actively contending with each other. If this dynamic isn’t to spiral out of control, there must be military-to-military hotlines and diplomatic mechanisms to reduce the chances of miscalculation. The current gap between subtle strategies and fiery rhetoric threatens the process of “tacit bargaining” and could lead to the failure of the strategy. Which strategy is Putin and Xi likely to believe, the cautious one advanced by the operational commander, or the more aggressive one being pushed from the White House?

### 2AC -- Xi Good

#### Plan’s a huge win for Xi

Adam Segal 18, Ira A. Lipman Chair in Emerging Technologies and National Security at the Council on Foreign Relations, September/October 2018, “When China Rules the Web Technology in Service of the State,” https://www.foreignaffairs.com/sites/default/files/sepoct18-issue-partner-form-97500.pdf

Almost from the moment he took power in 2012, Xi made it clear just how big a role the Internet played in his vision for China. After years of inertia, during which cyber-policy was fragmented among a wide array of government departments, Xi announced that he would chair a so-called central leading group on Internet security and informatization and drive policy from the top. He established a new agency, the Cyberspace Administration of China, and gave it responsibility for controlling online content, bolstering cybersecurity, and developing the digital economy.

Cyberpower sits at the intersection of four Chinese national priorities. First, Chinese leaders want to ensure a harmonious Internet. That means one that guides public opinion, supports good governance, and fosters economic growth but also is tightly controlled so as to stymie political mobilization and prevent the flow of information that could undermine the regime.

### 2AC – CCP Collapse

#### Model clash inevitable now---US will try to digitally disrupt China’s domestic censorship---that’s Hoffman

#### Perception alone makes leadership fear party instability---escalates---that’s Wright

#### Turns and solves their impact

Samantha Hoffman 19, PhD in Politics and International Relations from the University of Nottingham, 2019, "Managing the State: Social Credit, Surveillance, and the Chinese Communist Party's Plan for China," https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B\_0161\_WRIGHT\_ARTIFICIAL\_INTELLIGENCE\_CHINA\_RUSSIA\_AND\_THE\_GLOBAL\_ORDER.PDF

Chinese information technology research and development, including the priorities outlined in the 2017 AI development plan, are interesting on their own because they mark advances in important research areas. But, as the language of the AI development plan indicates, these advances cannot be separated from Beijing’s social management and state security policy. Applied to the social management process, they are aimed at improving governance capacity—automating the carrot-and-stick processes that ensure the partystate’s power. Senior CCP leadership hopes that through automation the Party will be able to more effectively anticipate and react to emerging problems, preempting crises before they become serious threats to stability.

### 2AC – Diversion

#### US attacks on China’s internet firewall cause mass instability and diversion

Chen Pokong 16, China analyst, former assistant professor of economics at Sun Yat-sen University in Guangzhou, leader in China Democracy Movement, 5/28/16, “This is How a Bloody U.S.-China War Could Start,” https://nationalinterest.org/feature/how-bloody-us-china-war-could-start-16383

The chapter sketches the hypothetical beginnings of a conflict scenario between the United States and China. In it, the U.S. responds to provocative Chinese cyberattacks by launching one of its own, tearing down the Great Firewall. In response, Chinese authorities clamp down Internet access completely, which America quickly responds to. Ultimately, regime-organized street violence endangers the lives of American consular staff, and U.S.-China relations quickly descend from the current modus vivendi to outright hostilities.

While both the United States and China can be expected to avoid going to war, it’s by no means difficult to imagine a scenario in which such a war might break out. Let’s consider such a development from the perspective of a young Chinese computer technician named Xiaolu:

After returning home from work one Friday evening, Xiaolu follows his usual practice of turning on his home computer and preparing to access his favorite overseas websites through proxies that will help him break through the Chinese government’s internet firewall. To his great surprise, he finds himself able to freely browse the Voice of America website without a proxy. He tries the BBC Chinese-language website, and then Radio Free Asia, Epoch Times, Boxun, the Chinese-language websites of the New York Times and the Wall Street Journal. . . surfing all of them with ease, he wonders if there’s some bizarre fluke in the system. He quickly telephones a friend and tells him to give it a try, and the friend reports the same experience. Overjoyed, Xiaolu contacts all of his friends and tells them to log onto the internet as fast as they can.

The situation continues the next day, and China’s streets and microblogs are abuzz with the news. People wonder if the Chinese government has suddenly decided to lift its internet blockade, and if this means political reform has also been launched.

Xiaolu stays glued to the internet all the next day and evening, too excited to sleep until he finally drifts off near dawn. By the time he awakens, the sun is high and the clock shows that noon is approaching. Luckily it’s still the weekend, and Xiaolu doesn’t need to be at work. Rolling groggily out of bed, he slouches over to his computer and goes online again, only to see a blank wall. Not only the foreign websites, but even China-based websites have disappeared and have been replaced with a uniform message of “Page not found.” Shocked, disheartened and angry, Xiaolu wonders what happened. He turns on his television just in time to hear a CCTV presenter read out this news bulletin:

“The United States has used the pretext of alleged Chinese hacker attacks on American websites to blame on the Chinese government and People’s Liberation Army. These baseless accusations originate from the pathological fantasies of certain individuals in the United States, and we have always categorically refuted them. The United States is now using the pretext of ‘freedom of information’ to interfere with China’s normal internet operations and oversight. This is a genuine cyberattack and a blatant cyberinvasion. It is a plot to overturn the Chinese government.

Interfering with and sabotaging China’s internet is a brazen violation of Chinese sovereignty and dignity. It is a last-ditch effort by American hegemonism to obstruct China’s rise following its failure to impose ‘peaceful evolution.’”

Xiaolu now understands that his earlier access to overseas websites was due to the United States playing a technological wild card that destroyed China’s internet blockade. His current inability to go online is due to the Chinese government taking the drastic step of cutting off all internet access after losing its “Great Firewall” to America’s technical superiority.

Through his shortwave radio, Xiaolu hears an announcement by the U.S. government:

“Safeguarding freedom of expression and freedom of information is a universal value. The United States of America firmly upholds the Chinese people’s freedom of information, the deprivation of which is an infringement of fundamental human rights. . . .”

Related reports and discussion show that the cyber operation, codenamed “Airborne Freedom” and launched by the United States, is in fact retaliation for a cyberattack by China. China has for some time been carrying out cyberattacks and cyberespionage against U.S.-based websites, and repeated warnings from Washington to end the attacks have met with only temporary pullbacks by Beijing, followed by renewed onslaughts. Reaching the end of its patience, the United States has finally decided to take action, and a full-scale cyberwar has been launched between China and the United States.

With internet access cut off, Chinese netizens begin taking to the street to express their indignation, their eyes directed straight forward or upward to signify their silent protest. The Chinese government issues an announcement: “The relevant departments have cut off internet access only as a temporary measure and as the only option. The United States, which launched a cyberattack to interfere with and sabotage normal internet operations in China, must take full responsibility.”

On the third night, internet access is miraculously restored. Strangely, however, unlike before, only overseas websites can be accessed, and almost no China-based websites. Xiaolu is initially baffled, but after surfing overseas websites, he gains an understanding of how the situation has developed.

It turns out that after the Chinese government cut off all internet access, the United States used satellite technology to provide wireless internet service to China. Operation Airborne Freedom has entered its second phase. The U.S. government explains its rationale: “We first of all need to ensure that American organizations in China as well as the U.S. Embassy and consulates can continue to access the internet. . . . At the same time, we are helping the Chinese people to freely access information. . . .”

The Sina and Sohu microblogging websites that Chinese netizens normally use have ceased operation, and have been replaced by internationally dominant social media such as Facebook and Twitter. The Chinese Baidu search engine has stopped working, but Google is available as a substitute, and Chinese netizens rejoice.

The next day, the Chinese government plays a new card. The State Council issues a “Notice Regarding the Suspension of Internet Access”:

“Malicious interference and sabotage by hostile overseas forces resulting in severe chaos in the arrangements for our country’s internet management has aroused mass outrage among the people. In order to ensure state security and normal information access, from this day forward the relevant departments will carry out comprehensive inspection, maintenance and rehabilitation of the internet. During this time, internet access will be suspended throughout the country.

Specific provisions are as follows:

1. Any work unit or individual who without authorization accesses the internet will be subject to confiscation of his computer, a fine, dismissal from employment or other penalties.

2. Any individual who uses the internet to create or spread rumors or to transmit reactionary information, and in particular any individual who incites opposition or subversion of the government, will be held criminally liable.

3. All internet cafes will be temporarily closed until further notice.

4. Sales of computers must be registered under the purchaser’s name. . . .”

Over the next few days, China’s netizens continue to enjoy access to overseas websites, and there is an explosive increase in satirical comments about the Chinese government on Facebook, Twitter and overseas Chinese internet forums. Rumors spread of police in some localities going door-to-door to examine internet browsing histories. Official media begin reporting on some people being investigated and having their computers confiscated. Overseas media report that rights defenders are being summoned and warned by the police, while some dissidents have been placed in criminal detention on allegations of using the internet to create or spread rumors to incite subversion of the government.

Mobilized by netizens through Facebook and Twitter, increasing numbers of people begin standing in the streets with their eyes directed forward or upward in what come to be known as “stand-ins.” Internet posting proclaim: “The Chinese people have stood up!” As another day passes, police are mobilized in a massive operation during which they physically push people away from “stand-ins.” Some protesters who resist are arrested. Four police officers grab Xiaolu by his arms and legs and carry him off as he struggles and yells out, “The Chinese people have the right to stand up!”

China’s PLA Daily publishes a commentary entitled “Cyberinvasion is a War of Aggression,” which states:

“We must point out that cyberinvasion is a war of aggression. We sternly warn the American hegemonists that today’s China is not the China of 1840; today’s China is not a China that can be bullied or trampled upon. Under the leadership of the great Chinese Communist Party, we have achieved economic liftoff and military modernization that will bring about the great revival of the Chinese people. Our country and our people have the capacity to defend our homeland. In the face of serious provocation, the full force of the Chinese People’s Liberation Army will resolutely follow the Party’s command and is prepared to go to war at any time in retaliation against any who dare aggressive action against our country’s sovereign rights and interests. We are prepared at all times to fight and to emerge victorious in repelling a frontal assault by the invaders. . . .”

In contrast to this hard line, the tone of some official scholars is more temperate. In an Associated Press interview, a professor of international relations at Renmin University of China appeals for calm on both sides. He urges the Chinese and U.S. governments to sit down for a face-to-face exchange of views on the mutual accusations of cyberattacks, and to resolve the conflict through dialog and negotiation to prevent the conflict from escalating out of control.

Prohibitions on internet access are implemented in government organizations, state-owned enterprises and all schools, libraries and other public bodies. Even so, how can the authorities control 500 million netizens and 300 million bloggers? Most netizens ignore the prohibitions and continue to access the internet at home. Internet access is unstable and intermittent, but the wireless internet service that the United States is providing to China has not been cut off.

After “stand-in” protests against the Chinese government have been suppressed for two days, anti-American protests suddenly break out in Beijing, with hundreds of people gathering around the U.S. embassy, shouting out anti-American slogans, denouncing the United States for sabotaging China’s internet and demanding an end to the U.S. cyberinvasion. Similar protests quickly follow in Shanghai, Guangzhou, Chengdu, Wuhan and Shenyang, where people gather around U.S. consulates and yell out slogans while waving the five-starred red flag of the People’s Republic of China. “Down with American hegemonism!” “We vehemently denounce American sabotage of China’s internet!” “Resolutely beat back the U.S. cyberinvasion!” “Creating chaos in China has ulterior motives!” Given the uniformity of the slogans and banners throughout the country, outsiders quickly realize that these protests have been orchestrated by the Chinese government.

### 2AC – Japan Link (Cyber)

#### Cyberattack definitions solve assurance crisis

Mina Pollman 19, PhD student in MIT's Department of Political Science, 6/7/19, “Learning to Embrace an Unequal Alliance,” https://www.tokyoreview.net/2019/06/us-japan-embrace-unequal-alliance/

The same pattern of overpromising manifested itself more recently, at the Japan-U.S. Security Consultative Committee (SCC) meeting held in April. Particularly problematic is how the Joint Statement deals with cyber issues. There is an acknowledgement that in the realm of cyber, each state should prioritize developing capabilities to protect their own national networks and critical infrastructure. However, the U.S. assurance that “a cyber attack could, in certain circumstances, constitute an armed attack under Article V” is vague and does more harm than good. The caveat that each cyber attack would be handled on a case-by-case basis does not necessarily distinguish it from any other type of attack. However, there is no standardized definition of a cyber attack under international law, and the second to last thing that the alliance needs, should Japan face a cyber attack, is bickering within the alliance over whether it counted as an armed attack under Article V or not. The last thing that the alliance needs is Japanese complacency or reliance on this shaky promise. Cyber is uncharted territory for alliances. Both the United States and Japan need to be particularly wary of the damage that overpromising in this realm can have on other realms of cooperation.

#### Japan wants the plan

Giulio Pugliese 19, lecturer in war studies at King's College in London, 5/29/19, “Four Scenarios for U.S.-China Relations and What They Mean for Japan,” https://www.tokyoreview.net/2019/05/four-scenarios-us-china-relations/

Japan would have to navigate between two deeply unpalatable options in such a scenario. Japanese multinationals and small & medium enterprises rely heavily on Chinese demand and regional supply chains. Policymakers in Tokyo would thus need to square the circle between a strong U.S.-Japan alliance and the preservation of deep economic ties with its wealthy neighbor. China’s rise presents opportunities and risks that need to be managed, in some cases with the help of the United States – but Japan will hopefully not get dragged into needless confrontations that entail economic pain and self-fulfilling prophecies that turn China into an enemy. Tokyo must resist a U.S.-China decoupling and brave the stormy Trump seas while teaming up with like-minded European partners to preserve the open global economy in the face of “might makes right” approaches from both sides of the Pacific Ocean. The expected unwillingness of U.S. allies, possibly including Japan, to pick sides in this hypothetical Cold War 2.0 makes this scenario unlikely.

The second scenario, and the optimum scenario for Japan, would be sustained U.S. regional engagement, with renewed American commitments to the global commons, including preservation of the multilateral free trade system. In this scenario, the United States would maintain its forward military presence and deter a more assertive China with the help of its allies. In addition, the United States would join the revived Trans-Pacific Partnership and coordinate with Japan, the European Union, and like-minded parties to shape the rules of twenty-first century economic practice, and work together towards the realization of connectivity projects through government financing (rather than rhetoric and MoUs). The aim would not be a zero-sum containment of China, but rather the preservation of a favorable regional balance coupled by joint efforts towards shaping Chinese political and economic behavior in a constructive direction through sticks, carrots, and international norms. One concrete example of such an attitude is Japan’s constructive ambivalence towards the Belt and Road Initiative (BRI), as Tokyo aims at shaping Chinese government financing towards international standards gearing up to the G-20 Summit.

### 1AR – Japan LT

#### Credibly applying article V to cyber key to deterrence and assurance---but, it’s case by case now---Pollman says that guarantees fights---the plan solves by 1) stopping attacks and 2) clearly delineating what counts as armed attack---overpromising and failing collapses US-Japan Coop

Daniel Hurst 19, freelance journalist based in Tokyo, 4/26/19, “Japan, US Beef up Their Cyber Alliance,” https://thediplomat.com/2019/04/japan-us-beef-up-their-cyber-alliance/

Both sides agreed to enhance cooperation on cyberspace issues, including deterrence and response capabilities, according to the joint statement, “but as a matter of priority, emphasized that each nation is responsible for developing the relevant capabilities to protect their national networks and critical infrastructure.”

The meeting considered how the existing provisions of the security treaty between the United States and Japan could be applied to emerging threats. Article Five of their Treaty of Mutual Cooperation and Security, signed in 1960, said that Japan and the United States each recognized “that an armed attack against either Party in the territories under the administration of Japan would be dangerous to its own peace and safety.” In the same article of that treaty, each side declared “that it would act to meet the common danger in accordance with its constitutional provisions and processes.”

During the April 19 meeting, the ministers “affirmed that international law applies in cyberspace and that a cyber attack could, in certain circumstances, constitute an armed attack for the purposes of Article V of the U.S.-Japan Security Treaty.” A decision as to whether a particular cyberattack rose to that level of seriousness would be made on a case-by-case basis.

Iwaya, the Japanese defense minister, told reporters that the agreement on Article Five coverage was “significant from the perspective of deterrence.”

The focus on cybersecurity reflects growing concerns among policymakers about the potentially devastating impact of attacks on critical infrastructure or communication networks, at a time when businesses, utilities, government entities, and the general public are increasingly reliant on digital technology.

Japan’s latest annual defense white paper said state-sponsored cyberattacks had been on the rise in recent years and were becoming more sophisticated. The white paper, published last August, said cyberattacks on telecommunication networks of government and military forces, or on critical infrastructure, “could have a serious effect on the security of states.”

As a result, the issue was a key focus in Japan’s revised National Defense Program Guidelines, published last December. The Guidelines indicated that Japan’s Self-Defense Forces (SDF) would maintain a cyberspace defense unit “in order to conduct persistent monitoring of SDF’s information and communications networks as well as to fundamentally strengthen cyber defense capability, including capability to disrupt, during [an] attack against Japan, [an] opponent’s use of cyberspace for the attack.”

#### Legal framework key

Sonoko Kuhara 20, Research Intern with the Japan Program at the Stimson Center, 2/25/20, “Can the US-Japan Alliance Handle Cyberattacks?” https://thediplomat.com/2020/02/can-the-us-japan-alliance-handle-cyberattacks/

Japan, which suffers the third most targeted cyberattacks in the world, has caught up with this trend. In April 2019, the United States and Japan agreed that their mutual security treaty will also cover serious cyberattacks against both countries, and this agreement is expected to deepen their cooperation significantly. However, three major challenges remain for the U.S. and Japan to effectively protect themselves against cyber threats.

The first is the lack of a legal framework to address cyberattacks and the issues related to countermeasures. The Tallinn Manual is the first step toward applying international law to cyber operations. However, even among NATO states there are different thresholds to activate self-defense and collective defense against cyber threats, a discrepancy that also exists between the United States and Japan. Moreover, this manual is not yet accepted as an international norm. This makes cyber defense particularly challenging for Japan. So far, the Japanese government has said the activation of self-defense should be considered case by case; however, decision-making on cases with the support of the public will be difficult without international consensus, including with the United States.

### 2AC – Allies AO

#### Cyber agression wrecks ally trust

Jason Healey 19, Senior Research Scholar in the Faculty of International and Public Affairs and Adjunct Professor of International and Public Affairs at Columbia University, was the founding director of the Cyber Statecraft Initiative of the Atlantic Council where he remains a Senior Fellow, president of the Cyber Conflict Studies Association, August 2019, “The implications of persistent (and permanent) engagement in cyberspace,” Journal of Cybersecurity, Vol. 5, No. 1, p. 1-15

The third and last set of feedback loops are the impact of persistent engagement on the larger system of cybersecurity and cyberspace. Persistent presence may be incompatible with the overarching US policy to “promote an open, interoperable, reliable, and secure Internet that fosters efficiency, innovation, communication, and economic prosperity” [35]. The competing goals of stability and superiority may prove to be mutually exclusive. Lin and Smeets have conducted a simple but very effective scenario-based analysis to examine these trade-offs [93]. The USA has been here before when, prompted by the Snowden revelations US allies moved to create stronger European borders in cyberspace [94]. Engaging in hot pursuit of Russians into European infrastructure may not garner the thanks of grateful allies for liberating their systems from occupation. As Lisa Monaco, former White House advisor for homeland security, cautioned, “other countries may not see U.S. activity on their network as ‘defensive’” [95]. According to one DoD official, the new strategy will require the trust of US allies to permit (and hopefully support) such activities.16 Given the Trump administration’s willingness to challenge even the closest allies, this trust will be hard won. In a particularly striking phrase, Smeets has written that “U.S. Cyber Command’s mission to cause friction in adversaries’ freedom of maneuver in cyberspace may end up causing significant friction in allies’ trust and confidence.” [69].

### 2AC – BMD AO

#### Cyber insecurity collapses BMD which solves missile threats, and is key to assurance

Lauren Borja 19, post-doctoral fellow in the School of Public Policy and Global Affairs at the University of British Columbia, 2/22/219, “Missing from the 2019 Missile Defense Review: Cybersecurity,” https://thebulletin.org/2019/02/missing-from-the-2019-missile-defense-review-cybersecurity/

The 2019 Missile Defense Review promises to create US “missile defense programs to counter the expanding missile threats posed by rogue states and revisionist powers to us, our allies, and partners, including ballistic and cruise missiles, and hypersonic vehicles.” It expands the role of current defense systems that defend against global threats, while pursuing unproven technology. But one important criterion for US missile defenses is entirely absent from the Missile Defense Review: cybersecurity.

The protection of critical computer systems, networks, and data can be achieved through both technical and social means. Good cybersecurity includes robust computer software and hardware, prudent engineering standards, and vigilant cyber hygiene—the procedures and practices required of network users to keep information and data on the network secure. Sometimes people assume that the security of a network is based entirely on the way it has been constructed; however, it is also important to consider how individuals interact with the network when assessing its security. Best practices usually include regularly installing system updates, using multi-factor authentication, enforcing compartmentalized [“need to know”] user permissions, establishing strong password rules and multi-authorization procedures, ensuring that firewalls are properly installed, updating both “white lists” and “black lists,” and not connecting unknown data storage devices—such as CDs and thumb drives—to a network.

These activities may sound mundane, but poor cyber hygiene has compromised many secure networks, including some classified US military networks, In 2008, the National Security Administration detected a rapidly-spreading computer virus on computers inside the Pentagon. William Lynn, who was the Deputy Defense Secretary at the time, wrote in Foreign Affairs that the virus was inserted “when an infected flash drive was inserted into a US military laptop at a base in the Middle East.” This lapse in cyber hygiene took the US Defense Department 14 months to fix.

After this incident, one would expect cybersecurity to be at the top of the list of concerns of the 2019 Missile Defense Review. But in fact, the review does not discuss how to address cyber vulnerabilities in existing missile defense systems, or how to prevent cyberattacks from occurring in these systems in the future.

By ignoring cybersecurity concerns, the Trump administration’s plans will contribute to the problems that currently plague US missile defense systems: Such systems are often overpromised, overbudget, and behind schedule. The history of missile defense systems accidents shows that these systems are often rushed into the field before errors in their software and hardware have been fixed. And subsequent poor cyber hygiene in US missile defense systems leaves them increasingly vulnerable to cyberattack. In other words, expanding US missile defense systems while ignoring cybersecurity will likely lead to increased—not decreased—security concerns.

Software problems in US missile defense. Even in the absence of cyberattacks, software problems exist within US missile defense systems. In 2003, the Patriot missile defense system, employed to defend against missiles during the Iraq War, was responsible for the death of three airmen in three separate friendly-fire incidents. The first incident involved a Patriot missile mistakenly targeting and destroying a British Tornado fighter plane. Its two crew members were killed instantly. In the second incident, a US F-16 fighter plane fired on a Patriot missile system after it erroneously targeted his aircraft. The third fatality occurred when a Patriot system shot down a US F/A-18 fighter plane, killing the pilot.

The summary of the ensuing official fact-finding report identified some of the problems that led to these incidents. Chief among them: the Patriot missile system had trouble distinguishing between friendly and enemy aircraft, a defect which had been previously observed in training exercises.

Documentation from operational tests of the Patriot missile system around the same time as the accident revealed a history of false identifications. Records from as late as 2001—a mere two years before the system was used in combat during the Second Persian Gulf War—described problems with target identification in the missile defense system. In 2002, the same researchers recommended more operational testing, even while noting the army’s immediate need for hundreds more missiles for the already-deployed Patriot systems.

Evidently these priorities—making the system available quickly, and building a system that is safe to operate—were in conflict for the Patriot missile defense system. As later accidents revealed, availability was prioritized over safety, and systems were sent into the field with significant software and hardware problems.

Current systems within missile defense, such as their command and control networks, continue to be deployed with significant known vulnerabilities, according to a 2018 Government Accounting Office (GAO) report. (Command and control networks link decision makers, sensors, and weapons systems; they enable the planning, management, and operations of various missile defense systems.)

According to the report, many of the computers used to coordinate missile defense operations use Windows XP, an outdated and vulnerable operating system for which Microsoft no longer releases updates. (It was originally launched in 2001, an eternity in the world of computing, where six months is considered an entire generation.) Computers running outdated operating systems have provided easy targets for hackers. For example, the WannaCry ransomware attack in May 2017 specifically targeted computers running unpatched Microsoft operating systems. The United Kingdom’s National Health Service was among the hardest hit; a report published contemporaneously criticized the organization’s continued reliance on Windows XP.

While the US Missile Defense Agency (the organization responsible for overseeing all of the US’ missile defense system) says that no cyberattacks have been detected as of 2017, vulnerabilities in the operating system have been exploited by the opposing team in internal cybersecurity exercises. The agency acknowledges that if “known deficiencies are exploited, mission capabilities like [missile defense] planning, radar control, track reporting, and situational awareness may be significantly degraded.”

The same GAO report says that these cyber vulnerabilities will be fixed in the next planned upgrade of the command and control infrastructure, which is scheduled to occur in all global command centers by sometime in 2019. The GAO notes, however, that the updated version faces technical challenges and cost increases which could lead to delays in scheduled deliveries. Fixing the cybersecurity issues before this planned upgrade has been deemed “cost prohibitive,” although the Missile Defense Agency had not specified the exact amount to the GAO at the time of the report.

In the 2019 Missile Defense Review, software is mentioned only once, and then merely as a way to add new capabilities to existing missile defense systems, such as countering hypersonic missiles.

Poor cyber hygiene in US missile defense. But bad as they are, the problems with faulty software and poor hardware in missile defense technology pale in comparison with the larger systemic problems within the missile defense development program. A report by the Defense Department’s Inspector General, released in late 2018, found that many of the facilities that support US missile defense systems lacked basic cyber hygiene practices, proper security controls, and rudimentary data safeguards. These “exploitable weaknesses” could allow “US adversaries to circumvent [ballistic missile defense system] capabilities, leaving the United States vulnerable to deadly missile attacks.”

### 1AR -- T/Japan

#### Turns Japan---space cybersecurity key

Yuki Watai 18, Ph.D. Candidate in the Department of Politics and International Studies at the University of Warwick, 11/28/18, “Is Japan’s Ballistic Missile Defense Too Integrated With the US?” https://thediplomat.com/2018/11/is-japans-ballistic-missile-defense-too-integrated-with-the-us/

Japan was among the first countries to participate in the U.S.-led Ballistic Missile Defense (BMD) project and decided to introduce its own BMD system in 2003. BMD is a highly integrated system with satellite radars to detect a missile and address it using a multilayered anti-ballistic missile system. However, so far Japan’s BMD cannot possibly function without U.S. technological and military capabilities, and most of Japan’s BMD developments are predicated on the assumption that the U.S. military will remain a key partner. Over the course of 15 years since the system’s introduction, not only has BMD been an effective tool to strengthen the U.S. alliance and internal defensive capabilities, but also it has created a platform resulting in a highly complex integration of the two militaries. Japan can no longer say no to the United States — not just because of the broader alliance relationship but because of overreliance on and integration with the U.S. military when it comes to defending Japan against ballistic missiles.

BMD has served Japan’s strategy very conveniently, enabling Japan to join the regional offense-defense arms race despite its pacifist constitution. The nature of BMD as a defensive system is a perfect fit for Japan’s strategy of “exclusively defense-oriented defense,” under which Japan has focused on defensive capabilities while relying on the U.S. nuclear umbrella. In a similar vein, BMD also strengthens the architecture of the U.S.-Japan security alliance – known as the “Sword and Shield System.” Along with Japan’s long-standing emphasis on the alliance as a crucial part of its security policy, BMD serves not only maintain the alliance but also strengthen it.

This is all the more crucial because, since the 1990s, Japanese policymakers have been concerned about potential “abandonment” by the United States after the end of the Cold War and the seeming decline in the U.S. geopolitical interests in the Asia-Pacific. As Daniel C. Sneider, an associate director of research for Stanford University’s Walter H. Shorenstein Asia-Pacific Research Center, told Asia Times, “the Japanese have this fear of abandonment. It’s deep-seated in Japanese strategic thinking.”

Given this fear, it’s interesting to note that BMD in Japan cannot function without U.S. military capabilities. The United States possesses Early Warning Satellites with the Space-Based Infrared System (SBRIS), operating in earth orbit, which cost more than $11 billion. The SBIRS allows the United States to constantly monitor the Asia-Pacific region, including North Korea, and detect any sign of potential launches. Japan does not yet possess such capabilities and hence receives information from the United States. Japan thus far has developed only ground-based radars, Aegis Destroyers’ radar, and Airborne Early Warning, which are helpful only in tracking missiles after a missile is launched. Thanks to the very short action time after a missile launch, a swift exchange of information to detect and track the missile is crucial, which necessitates both the use of U.S. satellites and enhanced interoperability to a substantial degree.

### 1AR -- T/NoKo + Iran

#### BMD solves North Korea/Iran

Lukas Mikelionis 20, Journalist for Fox News, citing the MDA, 3/26/20, “US shoots down dummy ICBM in groundbreaking military exercise,” https://www.foxnews.com/us/us-shot-down-icbm-missile-in-groundbreaking-military-exercise

The U.S. Missile Defense Agency on Monday successfully shot down a dummy Intercontinental Ballistic Missile (ICBM) in space during a highly complex test of the U.S. military’s capabilities to counter incoming missiles from foreign adversaries.

Two interceptor missiles, launched from an Air Force base in California, shot down the ballistic missile – launched from the Marshall Islands in the Pacific 4,000 miles away – supposedly meant to resemble missiles used by North Korean or Iranian militaries.

The first interceptor hit and destroyed the re-entry vehicle. The second interceptor hit a secondary object.

The agency said that during the test, ground and sea-based Ballistic Missile Defense System (BMDS) sensors successfully provided data to the Command, Control, Battle Management and Communication (C2BMC) system, which then prompted the launch of two interceptor missiles.

“This was the first GBI salvo intercept of a complex, threat-representative ICBM target, and it was a critical milestone,” MDA Director Air Force Lt. Gen. Samuel A. Greaves said in a statement.

“The system worked exactly as it was designed to do, and the results of this test provide evidence of the practicable use of the salvo doctrine within missile defense. The Ground-based Midcourse Defense system is vitally important to the defense of our homeland, and this test demonstrates that we have a capable, credible deterrent against a very real threat.”

# Thing we didn’t finish that would’ve been cool

### Core Solvency cards

#### The plan’s grid of directed-energy satellites eliminates all missiles and ASAT projectiles that enter space---transcends mutually-assured destruction AND generates spin-off tech like global wifi and PNT

Michael Nayak 17, staff scientist at the Maui High Performance Computing Center, Captain in the US Air Force, was a National Defense Science and Engineering Graduate Fellow, previously worked for NASA at the Kennedy, Goddard and Ames Centers, Ph.D. Earth and Planetary Science, et al., 2/23/17, “Changing the Deterrence Paradigm: Leveraging Space to Mitigate Nuclear Risks,” https://www.airuniversity.af.edu/Portals/10/SOS/documents/Think-Tank/FY17/17D/17D\_Eagles\_Think\_Tank\_Final\_Paper.pdf?ver=2017-02-23-132635-350

Strategic deterrence and nuclear capability are at the forefront of America’s national security and a high priorities to the new Presidential Administration. President Trump has tweeted the following: “The United States must greatly strengthen and expand its nuclear capability until such time as the world comes to its senses regarding nukes”1. While this frames the associated concept of deterrence to nuclear weapons, it can be linked to the future of the subject in a broader sense as well. The question becomes: do we march forward with revitalizing our time tested model of nuclear deterrence through the nuclear triad, or do we consider alternate methods of accomplishing strategic deterrence in the interest of the United States and its allies? Nuclear modernization and maintenance is already built into the Department of Defense (DOD) budget and nuclear weapons have been the cornerstone of deterrence for nearly 60 years.

However, should it continue to be our only strategic deterrence option?

With emerging technologies and scientific breakthroughs, space offers a unique and valuable frontier that the United States can advantageously explore for defense and deterrence. These technologies open up an entirely new realm of possibilities for national defense, industry, and the overall geopolitical environment in which we live. Space defense can change deterrence at the national and global levels. Moreover, current and future space capabilities are key terrain to war fighters and policy makers alike - assuring the ultimate high ground for our national objectives is truly critical.

In order to maintain a strong deterrence posture, the US should invest in a global, defensive, space-based, additive directed energy grid to co-target nuclear and ASAT threats. Executing this course of action (COA) will maintain the US’s Strategic advantage while changing the deterrence paradigm. This piece advocates for this initiative and will cover topic background, a thorough discussion of the COA, second and third order effects of it, constraints, and concluding remarks.

Background

Deterrence and Geo-political Climate

Since the days of the Cold War, nuclear warfare with other nuclear nations has been a significant threat to the United States. The United States and the Union of Soviet Socialist Republics (USSR) were the first two nations to develop nuclear weapons and immediately recognized that there is essentially no defense for these weapons of mass destruction (WMDs). This led to the ongoing challenge of keeping the other side from using them.

In the 1960s, an analyst at Hudson Institute coined the acronym “MAD”, which stands for mutually assured destruction, in describing the outcome of two nations engaging in nuclear warfare.2 Since that time, we have relied on our own nuclear weapons in order to dissuade other nuclear nations from using their WMDs against the United States. If an adversary launched a nuclear weapon at the United States, we would respond by reciprocating in kind. This would result in two severely demolished nations—a devastating scenario so awful that no near-peer nation would even make threats of launching a nuclear weapon. This has been our nuclear deterrence paradigm up until today. It centers on the doctrine of proportional response and retaliation with a second-strike capability.

We as the United States think that the MAD deterrence model has worked so far, but can never know for sure until it fails. We have even less confidence that this paradigm would stand up against rogue nations. It also fails to protect anyone from an accidental launch or unauthorized launch by a renegade operator. Furthermore, if a terrorist organization ever came into possession of a nuclear weapon, it would not hesitate to use this capability. Extremists would happily die as martyrs if they could launch a nuclear weapon at the United States. For these reasons, mutually assured destruction proves to be both outdated and ineffective. It cannot remain the sole, permanent model for nuclear deterrence.

The geo-political situation has evolved over the past 30 years to include other countries with a nuclear capability. US allies sought and gained the technology as well as other countries that the US is not allies with, such as China. More importantly, other nations, namely North Korea and Iran, are aggressively seeking nuclear Intercontinental Ballistic Missile (ICBM) technology. Whereas once the system of nuclear deterrence and mutually assured destruction applied to two actors, now multiple countries in different regions are involved. Mutually assured destruction is still the main deterrent; however, the predictability of other nations cannot be calculated. Nations such as Iran and North Korea have already proven a disregard for the United Nations and will present a clear and present danger to the US once they are successful in their endeavors. Furthermore, regional instability between Pakistan and India can lead to nuclear weapon use that could draw other nations into a war. In such a geo-political environment, the United States must further evolve in order to ensure its national security rather than leave it to a complacent perception of deterrence by mutually assured destruction.

Aging Nuclear Assets

This nuclear deterrence, MAD, paradigm relies upon an adequate and reliable nuclear arsenal. Unfortunately, this is in question as every leg of the US' nuclear triad is aging. The ground based leg of the triad, the Minuteman III ICBM, was fielded in 1970. There are approximately 416 deployed Minuteman III ICBMs which cost an estimated $2.6 billion annually to maintain. The Minuteman III is expected to be phased out and replaced beginning in 2030. The 14 Ohio-class ballistic missile submarines represent the sea leg of the nuclear triad. The first of these was fielded in 1981, and is expected to be phased out starting in 2027. The air leg of the triad, the B-52H Stratofortress and B-2 Spirit strategic bombers, need replacement as well. The B-52H was fielded in 1961 with a current end-of-service date in the 2040s. The B-2 stealth bomber was fielded in 1997 but is expected to retire in 2058. All three legs of the triad have modernization plans. The Ground Based Strategic Deterrent will replace the Minuteman III; the Columbia-class ballistic missile submarine will replace the Ohio-class; and the B-21 Raider will replace the B-52H as a dual-use long range strike bomber. All told, the cost of this modernization is estimated by to be around $1T over 30 years. The cost breakdown of this modernization is outlined in the graphic below3.

Space Law

While space provides an attractive alternative to policy makers as a domain in which to field a strategic deterrent, the US must consider current space agreements and international norms. The 1967 Outer Space Treaty is the foundational document for international attitudes and postures toward space. Article IV of the Outer Space Treaty specifically bans placing nuclear, or other WMDs in orbit around Earth. Additionally, this article prohibits military bases, fortifications, and weapons testing on celestial bodies. Aside from banning WMDs and militarization of celestial bodies, the primary result of the 1967 Outer Space Treaty is the establishment of outer space as a global commons for the open use and benefit of all mankind. Global commons are the domains that no one person or nation controls but which all individuals and nations can utilize. Because of this global commons status, and the ban on nuclear weapons, the prevention of any weaponization of space has become an international norm4. This sentiment stems from the massive benefits of the space industry, as well as the potential catastrophe of its destruction. For example, the Global Positioning System (GPS), is used across the globe as a public good for everything from navigation, to banking, cellular phone operations, and much more5. Destroying the GPS system would destroy the US economy. Despite the understood benefits of space, and sentiment to keep it conflict free, nations are pursuing weapons for use in the domain because these capabilities represent a clear and present danger.

Antisatellite Weapons (ASATs)

Another key consideration for policy makers is the role of the most common weapon being developed for the space domain, ASATs. ASAT development has a long history dating back to the 1950s with the USSR and the US. However, more interesting are the recent developments. Recognizing that space is the “soft ribs” of the US due to the US’ dependence on space assets, China began pursuing ASAT technology. In 2007, China successfully destroyed one of their own aging satellites in low Earth orbit with a kinetic kill vehicle launched from the ground. This stunned the international community, including the US, but since then China has conducted multiple tests including a 2014 test of a “non-destructive” ASAT6. Russia has also demonstrated a renewed interest in ASAT technology. In 2016, Russia successfully tested its Nudol ASAT for the fifth time7.

These tests have all used direct ascent ASAT technology where the ASAT is launched from a ballistic missile to place the kill-vehicle on an intercept trajectory with the orbital target. However, co-orbital ASAT systems have also been tested where the ASAT is placed into orbit and maneuvers toward a target to intercept/destroy or within range to disable the target through other means. Co-orbital ASATs are generally more expensive and sophisticated, but a potential future co-orbital ASAT threat is the miniaturization of satellites and the emergence of cubesatellites (cubesats). Cubesats are small, cheap, and simple satellites that can be easily designed, built, and launched. High-schools and universities have placed cubesats in orbit. Due to their size, these cubesats are incredibly difficult to track in space. And due to their price, even rogue nations such as North Korea could weaponize cubesats technology to impose their will on others8. Indeed, ASATs are not only a threat to US assets, but the global commons of space as well.

Course of Action

The course of action recommended by this work incorporates both space miniaturization and distributed systems design. We propose a global, distributed multi-node satellite grid, situated in a variety of orbits, each capable of hosting a low-power directed energy beam payload, for global space-domain superiority. The power of each beam will be such that, by itself, it will be incapable of producing a kinetic effect, suitable for a smaller spacecraft platform. However, the co-targeting of multiple such beams, on the same object, would raise the incident power to a destructive level, allowing the total system to exert destructive effects.

In less than a decade, space miniaturization technology has come so far that students at a high-school level of education are today capable of designing, integrating, launching, and operating cubesat systems9. Some university-designed systems boast sophisticated maneuvering and navigation capabilities10 and are capable of advanced military-relevant mission sets11. Though systems centered on smaller spacecraft may not be as reliable, these development efforts prove that the technology is both mature and accessible.

This additive directed energy system would target any projectile that breaks into the space domain around the world, whether an ICBM, standoff submarine launched ballistic missile (SLBM) or direct-ascent ASAT weapon. It would therefore directly target the ICBM leg of the nuclear triad, and would be proportionally less effective against either a close-range SLBM or the bomber aircraft-released nuclear weapon.

By nature, this system would be highly distributed. It is anticipated that several dozen spacecraft will be required to achieve system global reach, particularly since co-targeting by multiple spacecraft will be required to achieve kinetic effects. However, distributed or disaggregated systems are intrinsically less vulnerable. Defined as “the dispersion of space-based missions, functions or sensors across multiple systems spanning one or more orbital plane, platform, host or domain”12, a disaggregated system offers a natural resiliency and survivability. Since the capability is exerted through a larger number of redundant component parts, multiple component satellites can be lost before total system failure. There are many challenges to consider in the move toward small-satellite disaggregation, including architecture integration, ground system operations, mission assurance and others. However, these are dwarfed by the benefits: such systems are resilient by nature. A distributed systems architecture serves to eliminate the United States’ dependence on finite centers of gravity (COGs) of space power; with multiple systems in play, the payoff for an attack against the overall system lessens.

Such a platform would, by nature, be multi-purpose as well. The push toward multisensor space platforms is well under way; a global small spacecraft system in Low Earth Orbit (LEO), such as that proposed here, could also carry sensors for global Wi-Fi, protected communications, LEO position-navigation-timing (PNT) or global missile launch detection. Such combined mission sets would help to reduce the overall cost of the system, which is currently estimated to be of the same order as the modernization of the ICBM leg of America’s nuclear triad. Fielding such a system would render ICBMs and other nuclear launch systems that require space as a medium within which to transit highly susceptible to failure, redirecting worldwide nuclear spending from a “triad” concept to a “diad” concept, consisting of SLBMs and aircraft-based nuclear weapons. For several countries around the world, e.g. Pakistan, Iran and North Korea, this negates their nuclear delivery capability completely.

Finally, the theory of graduated deterrence is centered on “active” defensive measures complementing the threat of force. One of the key factors for successful deterrence is the criteria of “proportionality, reciprocity and coercive credibility”. The more superior a nation’s available instruments to inflict harm, the larger costs for non-compliance it may credibly impose13. Dissuasion of enemy escalation is accomplished through the threat of progressive retaliation, ultimately discouraging the enemy from an initial action14. Nuclear deterrence theory makes good use of graduated deterrence, dating back to Robert McNamara and the Cold War15 and attacks against this space system would follow a similar principle16. Though each directed energy platform is not capable of an offensive strike against the ground or even a target in flight, it is able to defend itself against either ASAT attacks or space-to-space attacks by leveraging that directed energy capability. Combined with the fact that US space policy makes clear that any hostile act in space will be considered an act of war,17 this allows for a credible defense and dissuasion of enemy aggression against this system.

#### Great solvency ev but lol old

-- Russia says yes

-- Changes global perception of BMD to be seen as stabilizing

-- Key to check rogues with missile programs and respond to accidental/unauthorized launch risks

-- Normal means includes consultation with allies which solves any assurance DA

-- Doesn’t turn over the decision to intercept to the world community

-- Includes any interested country

-- For T: does SSA sharing and launch notification

-- Both sides get what they want: Russia gets early warning coop, US gets coop on deployment of defenses

Stephen Hadley 93, at the time was 3rd Assistant Secretary of Defense for Global Strategic Affairs, 1993, “Global protection system: Concept and progress,” Comparative Strategy, Vol. 12, No. 1, p. 2-6

The story begins with the restructuring of the Strategic Defense Initiative Organization (SDIO) program, which was ordered by President George Bush in January 1991. This changed the focus of SDI to a program called Global Protection Against Limited Strikes, or GPALS, which is an effort to defend against limited attacks, whatever their source, focusing in particular on third-country attacks and also on the possibility of accidental or unauthorized launch from a nuclear power. In a nationally-televised speech on September 27, 1991, President Bush called upon the leadership of the then Soviet Union to take immediate concrete steps to permit the deployment of defenses against limited ballistic missile attack. Less than two weeks later, President Mikhail Gorbachev said that the Soviet Union was ready to consider U.S. proposals for non-nuclear defense against ballistic missiles. There was a hiatus in the process as the Soviet Union descended into crisis and ultimately dissolution. There was the coup attempt in August 1991, its failure, the struggle and jockeying between the forces of reform and status quo, and finally in December 1991 the emergence of the reformers in the form of the first democratically elected president of Russia, Boris Yeltsin. Within one month of that development, on his first visit to the United States, President Yeltsin announced to the United Nations that Russia was ready to jointly develop and subsequently create and jointly operate a global system of defense against ballistic missiles. At the summit meeting between President Yeltsin and President Bush that followed in June 1992 in Washington, the two presidents agreed to work together with allies and other interested states to develop a concept for a Global Protection System against limited ballistic missile attack.

GPS Provides Vehicle for Change

The U.S. approach to President Yeltsin's concept of a Global Protection System has been to embrace it and make it a focus of our own efforts. We did so for three reasons: First, we saw in GPS a possibility of changing the thinking of the international community about ballistic missile defense. I think it is fair to say that the Anti-Ballistic Missile (ABM) Treaty got the international community to think of ballistic missile defense as something bad, as something destabilizing. We found that the focus on a Global Protection System would be potentially a vehicle to change that thinking. In our view, the world community learned from Iraq that it can be threatened by rogue states with ballistic missile capability. I think the instability surrounding the Soviet coup attempt in August 1991 also reminded the world community of the risk of accidental and unauthorized attack with ballistic missiles. We have tried to stress that the reality of this threat is a threat to the entire global community, and that a Global Protection System can be a vehicle by which the world community can address this threat.

Second, we thought that focusing on the GPS concept could help change thinking in Russia. President Yeltsin's call for cooperation on a Global Protection System is nothing short of a breakthrough in the attitude of the former Soviet Union on these issues. We believe that cooperation in a Global Protection System can provide a context in which Russia could accept our deployment of defenses against ballistic missiles and the changes in the ABM Treaty required to permit those deployments. Separately, GPS is also an area of potential defense cooperation between the United States and a new democratic Russia. In our view, it can help put the relationship between the United States and Russia on a new basis to reflect our aspirations for Russian democracy and reform.

Third, the focus on a Global Protection System concept could help change thinking in the United States, as well. If the world community in general and Russia in particular are ready to work on defenses against limited ballistic missile attacks, then even the most skeptical critics in the United States would have to give way. It would, we hope, break the log jam on the ABM Treaty, the constraints of which prevent us from deploying defenses and from pursuing a Global Protection System concept.

Since January, we have concentrated on four areas: First, we have worked to develop a concept for a Global Protection System. Second, we have had frequent consultations with our allies and other states on the GPS concept, and we have kept them fully informed of our discussions with the Russians. These consultations are beginning to lay a foundation for cooperation between the United States and our allies and a large segment of the world community on a Global Protection System. Third, we have worked with Congress on implementing the historic Missile Defense Act of 1991, which established a consensus between Congress and the Executive Branch on the role of missile defense in protecting the United States, its friends and allies, and our forces abroad against limited ballistic missile attacks. We believe the Missile Defense Act will continue to serve as the foundation for our national program and that a Global Protection System is a way to implement the objectives that are set out in the Act. Finally, we have pursued discussions on a GPS concept in some detail and with great intensity with the Russians, which I will discuss later in my comments.

Regarding our concept for a Global Protection System, let me specify what we think it is not. GPS is not a system whereby we would participate with the global community and turn over a system of ballistic missile defense to the United Nations or some other group, which would have the sole key to control of that system. We think that does not reflect the reality of politics in the world, or the concern of nations legitimately to have under sovereign control the means of their own defense. Therefore, we have taken a different view and approach. We view GPS as an association of sovereign states that would commit to assisting one another to meet a challenge to their national security and international stability posed by the proliferation of ballistic missiles and weapons of mass destruction. Participation in GPS would be open to all interested states that are members in good standing of the community of nations and that have embraced the objectives of stemming proliferation of advanced technology.

Participants in GPS also would establish and operate a global protection center, which would serve several purposes: Participants would share information on sources of proliferation and the uses of proliferated technology. They would register pre-launch notifications of launches of ballistic missiles and space vehicles. They would share certain specified information on all launches of missiles detected by national sensors such as time of launch, location of launch, number of missiles launched, direction of flight, and the like. They would assist each other to develop their own national technical means of warning and defense against limited ballistic missile attacks. Center participants could undertake planning activities, engage in exercises, and develop models to support cooperative defensive operations against such attacks. The center would be a forum in which individual states could work out cooperative agreements by which the assets of one nation might be used to defend the territory of another against limited ballistic missile attacks. At the same time, participants would retain control of the national assets they committed to a Global Protection System.

Under the GPS center approach, the United States would be willing to make available the benefits of its GPALS deployment to participants in the Global Protection System. For example, we would be prepared to make available processed early-warning information from our existing and planned early-warning systems for use with ballistic missile interceptors of all types. We also would be ready to cooperate with other participants for coordinated missile defense operations, as our capabilities for ballistic missile defense (such as Brilliant Pebbles, for example) develop along with the capabilities of other nations. Additionally, we would be prepared to assist, through technical cooperation and other activities, the development by other participants of the means to defend their own homelands and forces.

I do not want to suggest that this concept of GPS is set in stone, or that we have tied a ribbon around it and are marketing it in the world community. What I have tried to convey is our thinking on a concept that we think makes sense, recognizing that our thinking is undergoing change every day. We have consulted with the Russians and with our allies and friends, and we are beginning to modify our own thinking to reflect those deliberations and consultations. We think there is something important involved, a concept that can be a useful element for defending against these threats in the 1990s, and we are committed to pursue it.

GPS Discussions with the Russians

We are pursuing the GPS issue diligently in our discussions with the Russians. At the June 1992 summit in Washington, Presidents Bush and Yeltsin established a senior high-level group to explore on a priority basis practical steps that could be taken toward developing a concept for a Global Protection System. To that end, the high-level group was challenged to explore the potential for sharing of early-warning information through the establishment of an early-warning center; for cooperating with participating states in developing ballistic missile defense capabilities and technologies; and for developing a legal basis for cooperation, including new treaties and agreements and also changes to existing treaties and agreements necessary to implement a Global Protection System.

The first meeting of the high-level group was held in Moscow July 13 and 14, 1992. It was headed by Assistant to the President Dennis Ross on the U.S. side and Deputy Foreign Minister Georgiy Mamedov on the Russian side. The group agreed to establish three working groups: one to develop thinking about the GPS concept itself, a second group to explore areas for possible technology cooperation, and a third to explore common efforts on non-proliferation. The senior group will retain responsibility for discussing legal issues associated with a Global Protection System.

The second meeting of the high-level group was held in Washington September 21 and 22, 1992. Four topics were discussed: (1) technology cooperation, (2) nonproliferation activities, (3) further elaboration of the GPS concept, and (4) further discussion about issues associated with the legal basis for GPS. Talks will continue by the working groups during October, and the senior group is expected to meet again and review the results.

This is a long, hard road. On balance, I am cautiously optimistic. I think there is agreement between the U.S. and the Russian sides that there is a real threat, and that it is more clear and present to Russia than it is to the United States. In our threat briefing, we have a chart which shows countries that potentially could have ballistic missiles through the end of this decade. We run range arcs on what we think the range of those missiles might be, and put them on a world map. It is a very convincing portrait, because a lot of those circles hit Russia. Very few hit the United States in terms of what we expect in the next five to seven years.

We have gotten the Russians' attention and I think they are aware of the threat. I believe the Russian military definitely would like to deal with us in a cooperative way to try and meet the threat, and I think we have a potential constituency in the scientific community, which wants to participate in these efforts, both to employ their scientists and also potentially to sell hardware to GPS participants.

Our priorities, however, are somewhat different. The Russians are very interested in early-warning capabilities and the possible sharing of early-warning information to fix some very real problems in their early-warning network. The United States has an early warning network that we are comfortable with. For us, the priority is getting on with deployment of defenses.

Secondly, the Russians are very interested in anti-theater ballistic missile systems. Given the location of the threat, that probably makes sense to them. On the other hand, we have to pay much more attention to ABM capability, given our geographic location. Again, this is somewhat of a different priority. The solution, I think, is to use the GPS concept as a framework for collaboration, where both sides can get what they need to manage this problem. We have made it very clear in our conversations with the Russians that we cannot just deal with early warning, we have to deal with deployment of defenses. We cannot just deal with ATBM, we have to deal also with ABM. And we also have made it clear that, if we are going to cooperate on a Global Protection System, we will have to have relief from the ABM Treaty. Otherwise, we simply cannot do the things we need to do to meet the threats that exist. We have made it clear to the Russians that we would like to revise the ABM Treaty consensually. We also have made it clear that this is a national priority, something we feel committed to do, so that they have no doubt.

#### Solvency---more recent

-- Russia says yes---they were interested until the U.S. bailed on initial talks

-- Should include space-based interceptors

-- Should start with U.S.-Russia bilateral discussion and then expand to include other nations

-- Facilitates global disarm

Barry M. Blechman 16, Distinguished Fellow at the Stimson Center; and Jonas Vaicikonis, Intern at the Stimson Center, 11/3/16, “Unblocking the road to zero: US-Russian cooperation on missile defenses,” Bulletin of the Atomic Scientists, https://doi.org/10.1177/0096340210387041

When President Barack Obama took office the following year and indicated a desire to “reset” US-Russian relations, beginning with the negotiation of a new START agreement limiting offensive forces, the Russians also made clear their desire to limit defenses. This issue was one of several which delayed completion of the START talks. In the end, however, recognizing that incorporating limits on defenses in the START agreement would not be feasible politically for President Obama, the Russians contented themselves with language in the preamble stating that a relationship existed between defenses and offenses. They also issued a unilateral statement to the effect that they retained the right to withdraw from the treaty if the US deployed significantly improved defensive capabilities. Both sides understand that further steps toward negotiated reductions in offensive forces will not be possible until they have a meeting of minds about missile defenses.2

Previous efforts to develop cooperative missile defenses

One way to address the recurring conflict over missile defense would be for the two sides to negotiate a new treaty limiting strategic defenses. Given the continuing proliferation of nuclear weapons and missile technologies to small nations with aggressive agendas, such a limitation might not be in either country’s interest, however. Iran, for example, might be in a position to threaten both Russia and US allies with nuclear-armed missiles within a few years (Senate Select Committee on Intelligence, 2010). Negotiating a new missile defense treaty would be extremely difficult for any US administration, moreover, as missile defense is such a polarizing issue in American politics. American public opinion strongly supports missile defenses and there are many powerful proponents of missile defense in Congress (Aheran, 2008). For example, the statement in the preamble about a relationship between offenses and defenses and Russia’s unilateral assertion of its right to withdraw because of US defense improvements were the primary reasons cited in the Senate debate during the summer of 2010 for opposing the New START agreement.3

There is also a technical reason why a new missile defense treaty might not be feasible: It is not evident how limitations on strategic defenses could be defined. Neither country would be willing to place limits on its tactical missile defenses—the systems that protect warships, air bases, and deployed ground forces from both cruise and ballistic missiles. Discriminating between strategic and tactical defenses was difficult enough in 1972 when the ABM Treaty was written. Forty years later, both tactical and strategic defenses can utilize common early warning, targeting, and command and control systems, and the two sides are moving toward interceptors, as well as new types of weapons like lasers, that could conceivably be used in either tactical or strategic roles. A new ABM Treaty is simply a non-starter.

The idea that the US and Russia could cooperate on missile defenses as a way to circumvent these difficult political and technical issues has been around since the 1980s. As noted, President Reagan proposed such cooperation in conjunction with Premier Gorbachev’s proposal to eliminate all nuclear weapons. During the George H. W. Bush administration, the two nations held talks on the possibility of such cooperation and, by all accounts, made surprising progress. Russian participants, particularly, speak almost nostalgically about the rapid progress that was made in those talks.

The talks were initiated by Russian President Boris Yeltsin in January 1992, when he proposed bilateral cooperation on a jointly operated global missile defense system to replace the unilateral American SDI, saying, “We are ready to develop, then create, and jointly operate a global defense system, instead of the SDI system” (Bunn, 1992). Seeing such cooperation as a key element in the emerging friendly relationship with the newly non-communist Russia, the Bush administration developed the proposal into a concept called the Global Protection System (GPS), which was later known as Global Protection Against Limited Strikes (GPALS). Overall, the idea was to begin by providing an opportunity for interested states to cooperate to enhance the capabilities of their own systems and then to move on to more ambitious joint programs (Hadley, 2010). In principle, as discussed by the two sides, the system would have several components: (i) a jointly manned center that would be fed early warning data from each nation’s systems; (ii) nationally controlled interceptors on each country’s territory; and, even, (iii) a jointly built system of space-based interceptors to deal with shorter range threats, such as the Iraqi Scud missiles fired at Israel and Saudi Arabia the year before, in 1991.

Presidents Bush and Yeltsin agreed to establish a bilateral High-Level Working Group to develop the idea further in June 1992. This group met three times and established three working committees: a committee that discussed the GPS concept overall, a committee that investigated avenues for possible technological cooperation, and a committee that focused on non-proliferation.

The High-Level Working Group established that both the US and Russia had a level of interest in developing functional missile defense capabilities and that there certainly were opportunities for cooperation. However, the Russian side was more interested in cooperating on early warning and on theater missile defenses (TMD), which could be deployed to protect specific areas deemed at risk from short-range missile attack. The US already had an effective early warning and tracking system and was more interested in cooperating on the actual deployment of active strategic interceptors. Also, while the US showed interest in TMD systems, it believed it was a greater priority to develop countermeasures against intercontinental ballistic missiles (ICBMs), simply because geography dictates that the US is more vulnerable to ICBM attacks than to shorter range missiles (Hadley, 2010).

A major sticking point became evident when discussions turned to the ABM Treaty. The talks took place at a time when the US was unwilling to withdraw unilaterally from the Treaty (as it did 10 years later), as it was hoping to develop cordial relations with the newly independent Russia. Instead, the American side proposed amending the Treaty to (i) lift constraints on the testing of ABM systems, and (ii) grant each country the right to deploy national missile defenses at six sites with up to150 interceptors each—a huge increase to the limits in the existing treaty (Arms Control Today, 1992). The Russian side rejected this proposal, but signaled that they might be open to interpreting the existing ABM Treaty as allowing for a truly internationally controlled missile defense system (Arms Control Today, 1992). Shortly thereafter, when President Clinton came to office and the US administration turned against defenses again, the working group talks faltered, although discussions of some sort of joint or shared warning system persisted for a time.

The possibility of cooperation on missile defenses was reborn during the final years of the Clinton administration. In September 1998, Presidents Clinton and Yeltsin announced a new effort to ease fears of accidental missile launches by creating a Joint Data Exchange Center (JDEC). This was to be a center in Moscow that would be staffed by American and Russian personnel and would receive data feeds from Russian and American sources on worldwide missile launches (New York Times, 1998). The JDEC was said to have the potential to reduce the likelihood of an event like that in 1995, when a scientific rocket, launched over Norway to study the Northern Lights, was interpreted by some in Moscow as an American nuclear attack requiring a Russian nuclear response. Despite years of discussion during the ensuing George W. Bush administration, the JDEC was never established, ostensibly because of disputes over taxes and liabilities (Baker, 2001; Boese, 2006). In truth, it appears that the tense Russian-American relationship during much of this period and the Russian’s perception that the US was offering the JDEC as a fig leaf to cover an unwillingness to discuss more serious forms of cooperation were the true culprits.

Despite the failure to close the JDEC deal, the Russians renewed proposals for cooperation in missile defenses. In response to the NATO proposal to deploy missile interceptors in Eastern Europe in 2006, then-President Putin offered to cooperate with the US to work toward a joint missile defense system (White House, 2008). Putin even went so far as to say that cooperation on a missile defense system would take bilateral relations to “an entirely new level” (Rutenberg, 2007). However, the US saw the proposal as a ploy to undermine the NATO missile defense system and never took it seriously, just as the Russians understood the proposed NATO system as a first step toward more robust defenses that could threaten their retaliatory capabilities.

Greater progress has been possible within the NATO-Russia Council (NRC)—and more accurately, by its Theatre Missile Defence Ad Hoc Working Group, which, since its creation in 2004, has embraced the task of working out the technical details of a cooperative missile defense system (NATO-Russia Council, 2010). It has fleshed out a feasibility study for the interoperability of forces and equipment and held several joint exercises between 2004 and 2008, when NATO cancelled them in response to the Russia-Georgia conflict. Progress has been made on the development of common terminology, joint TMD training, and the completion of interoperability studies. The NRC resumed its meetings in March 2009 and has commenced work on a joint air traffic coordination system that many European countries, as well as the US and Canada, are participating in.

Since 2008, the notion of bilateral US-Russia cooperative missile defenses also has been resuscitated. President Obama cancelled the Bush plan for a European missile defense system in Poland and the Czech Republic, replacing it with a phased approach to the defense of Europe against missiles originating in the Middle East. Russian leaders say they find this system less threatening, at least in its early phases. Moscow has even suggested that two of its early warning radars, which are well positioned to cover the Middle East from stations in Azerbaijan and southern Russia, might be integrated into this NATO defense system (Chivers, 2007).

Also, an Arms Control and International Security Working Group of the US-Russian Bilateral Presidential Working Group was created by Presidents Obama and Medvedev in July 2009. One of the issues this group has been tasked with discussing is the possibility of cooperating on missile defense capability and establishing a JDEC. While this working group has met several times at high levels, it has yet to achieve notable results (US-Russia Presidential Commission, 2010; White House, 2009). The lack of progress is probably the result of both sides’ wish to avoid complicating the New START ratification process by raising the possibility of changes in US missile defense plans that could provide fodder to opponents of New START. Serious discussions have yet to begin.

Cooperative missile defenses: An agenda

Once New START is ratified, the US and Russia will turn their attention to the possibility of deeper cuts in nuclear arsenals. Coming to a mutual understanding on defenses will not be the only obstacle to such an agreement, but it is certainly a prerequisite. For this reason alone, discussions of ways to cooperate on missile defenses should be given a high priority by both countries’ leaders.

A recurring hurdle to cooperative missile defense is that new missile defense systems are on the cutting edge of military technology. Some elements of defense systems also involve advanced intelligence and surveillance systems. If only for these reasons, it is difficult to develop multilateral approaches, even among allies. Discussing these technologies will be even harder between two nations that are no longer enemies, but not yet friends. The discussions, therefore, should begin with baby steps, building confidence before tackling more ambitious forms of cooperation. It might also simplify matters if the US and Russia discussed early measures of cooperation bilaterally and then broadened them to include other nations. An illustrative agenda might look something like the following:

Common missile database

The two nations already know a great deal about their respective missiles as a result of the cooperative verification measures incorporated in the START agreement. These data could form the beginning of a shared information system, which could then be extended to the characteristics of other nations’ missiles, such as their range and payload. Given that missiles become highly visible when they are tested, a great deal is known about the characteristics of the world’s missiles in unclassified sources. In its early phases, the common database would be based on such information, as the two nations review the various sources available and reach agreement on which data are most accurate. As new missiles are tested by nations, the two countries could update the database to incorporate additional descriptors of their trajectories, etc.

Shared early warning information

Both nations maintain space-based systems capable of detecting missile launches, although the Russian system provided incomplete coverage in recent years. Identical command centers could be established in Russia and the US and be staffed by officers and technicians of both countries. These centers would receive feeds from the two countries’ early warning systems so that they would have a common picture of missile launches around the globe. They could also receive data from the two nations’ early warning radars; in this regard, Russia might contribute more with its radar than its satellite systems. Alternatively, a single center could be established in one city, as was envisioned for the JDEC. In either case, these shared systems would have no response commitment or capability. Those capabilities would be retained by each country’s own command centers. The cooperative warning center or centers would be intended strictly to ensure that each side had the best information available, so as to avoid miscalculations and unnecessary responses. Presidents Obama and Medvedev have already agreed to establish a center of this type, in effect reviving the stalled JDEC project from the Clinton and Bush years. It is long past time to break the 12-year logjam on this issue.

Common warning systems

In 1997, the US and Russia discussed building and operating two joint warning satellites, called the Russian American Observation Satellite (RAMOS), and signed an agreement to create two satellites to share warnings of missile attacks. The hope was that the system would increase transparency and thus lessen the chance of a catastrophic misunderstanding. The two satellites would be placed in low Earth orbit and observe with infrared, visible, and ultraviolet sensors. The proposed system would also have the capability of observing hurricanes and predicting their paths (Samson, 2007). This concept might be explored again in the future, as a first step toward a common defense from missiles originating in the Middle East—a common threat. This satellite could be placed in an orbit that would help patch the deteriorated Russian early launch warning satellite network. The US would benefit, as the satellite would give the Russians greater confidence in their ability to monitor all missile approaches to their territory continuously and would help reduce the risk of a misinterpreted missile launch. Satellite technology is some of the most highly classified information the US holds, but since the idea of a joint satellite was proposed almost two decades ago, the idea may prove feasible, especially if the cooperative satellite is of rudimentary design.

Complementary defense of Europe and European Russia from missiles originating in the Middle East

These discussions should be held in a working group under the auspices of the NATO-Russia Council. They need not include all NATO members, but should not exclude any that wish to be included. This working group would discuss the Russian proposal to provide data from its early warning radars in Azerbaijan and southern Russia for use by NATO’s planned defenses. Russia would not gain a voice in the operations of the NATO system, but would benefit if missiles originating in the Middle East were aimed at, or strayed toward, Russian territory, and yet were vulnerable to interceptors on US Aegis warships deployed in the Black Sea. NATO would gain additional confidence that it would have timely warning of potentially hostile missile launches. The deployment of US warships in the Black Sea on a continuous or nearly continuous basis would represent a change in Russian policy and signify its seriousness about cooperation in missile defenses.

Coordinated or even common defense from missiles originating in the Middle East

Following achievement of the complementary defense outlined above, the working group should design the architecture of a coordinated, or even common, defense system, and then work to implement it. These talks should be expanded to include other nations, like Ukraine, whose geographic position might prove useful for the location of interceptors or radars. The system could be a modification of NATO’s current plans for the later phases of its adaptive defense to incorporate Russian components, or envision a completely different system, such as the drone interceptors proposed by MIT professor Theodore Postol (2009). It would be possible to design and build such a system only if political relations between NATO and Russia improve significantly; in such a case, it would be reasonable to expect Russia to play a role in the operation of the system as well.

Global defense

At this point, thought should be given to erecting a worldwide missile defense system with the cooperation of all technologically advanced nations wishing to participate. The system would be designed to complement negotiated reductions and eventual elimination of all nuclear-armed missiles (and other nuclear weapons), providing a fail-safe hedge against cheating on such an agreement. Such a system could only be established if it included emerging powers like China and India. Otherwise, it might be perceived as if NATO and Russia were establishing a sort of global condominium. The establishment of such a system would realize Reagan and Gorbachev’s shared dream from 1986: a world free of nuclear weapons along with a reduced threat of missile attacks by rogue states.

Conclusion

The fifth and sixth items on this agenda seem far-fetched at present, but, not so long ago, so did the possibility of the dissolution of the USSR and the end of the Cold War. Nuclear weapons pose unacceptable dangers to people in all nations. The longstanding political conflict over missile defenses, a relic of the Cold War, cannot be permitted to hinder progress toward the reduction and eventual elimination of nuclear arsenals. The US and Russia should begin immediately to discuss small and practical steps toward cooperation in defending against nuclear-armed missiles, setting the stage for the more ambitious common efforts that are necessary components of a nuclear weapon-free world.

#### All obstacles can be overcome once the U.S. and Russia decide to do the plan---and it’s key to check the impact of accidental launches and inevitable global prolif

Alexei G. Arbatov 10, Head of the Center for International Security, Institute of World Economy and International Relations of Russian Academy of Sciences, Corresponding Member of the Russian Academy of Sciences; Vladimir Z. Dvorkin, Major-General (rtd.), Chief Researcher, Center for International Security, Institute of World Economy and International Relations of Russian Academy of Sciences; and Sergey K. Oznobishchev, Head of Sector, Center for International Security, Institute of World Economy and International Relations of Russian Academy of Sciences, 6/22/10, “NON-NUCLEAR FACTORS OF NUCLEAR DISARMAMENT (Ballistic Missile Defense, High-Precision Conventional Weapons, Space Arms),” https://www.files.ethz.ch/isn/144178/10002.pdf

1. Cooperation of Russia, the US and NATO in developing a joint BMD is presently the key to further progress in nuclear arms reduction and limitation (deep nuclear disarmament), and shaping political partnership. Despite two decades of official and academic promotion of this idea, up to now it has not been implemented in practice in any tangible way (except a series of joint command exercises). Recent two years of “resetting” US-Russian relations have produced some changes which might open new prospects for cooperation on BMD.

President Obama's Administration has sent a clear enough message of intention to cooperate with Russia in this field. NATO leadership also agreed with the necessity to work together with Russia in developing and building joint defense against ballistic missiles. Russian leadership gives positive signals regarding the possibility of such cooperation.

2. The US is presently an absolute leader in the development of nonstrategic and strategic ballistic missile defense systems. Nevertheless, Russia is still capable of making a considerable contribution by providing its early warning and interception capabilities to the joint BMD system. Apparently, joint development of TMD, let alone strategic BMD, is a long-term program that requires the parties to solve many complicated political, military and technical, economic and legal issues. It is simply impossible to address or even foresee all of such problems in advance.

Yet, once the milestone decision is made and strategic course towards cooperation is defined, it is possible to start with relatively simple and indisputable measures and plan at solving future issues in due time . Very important that practical progress in this pivotal security sphere would by itself have a profound beneficial effect on the relations between the parties and facilitate resolution of issues that now appear to be insoluble. (Probably, it is for this particular reason why the strongest opponents of cooperation between Russia and the West campaign so zealously against any, even minor, practical measures of cooperation in this area.)

The participants in the conference held on June 22, 2010 and the authors of this booklet have no doubt that it is imperative that the parties promptly engage in such cooperation, and first of all restore the elements of cooperation that have been abandoned over the recent years.

First steps could be decisions to revive at a new level the efforts to integrate information components of missile launches early warning systems by reviving the project of a Joint Data Exchange Center and resuming the interrupted series of TMD exercises that should now reach beyond the limits of the theatre of operations There is no point in convincing the Europeans that they may only be threatened by short-range ballistic missiles. Furthermore, as technologies advance, the boundary between tactical and strategic BMD diffuses. Former intentions to cooperate only in developing non-strategic BMD appear an anachronism, although such cooperation format may become a first step of a long-term cooperation program.

The revival of the idea of virtual JDEC might facilitate its implementation and help avoid unnecessary expenses and organizational difficulties. Still, considering the strengths and weaknesses of a virtual JDEC, and taking in account political importance of this project, reviving the idea of a real (physical) joint Center retrofitted to gather real-time information appears to be a better option.

3. Although Russia does not presently view Iran's and North Korea's missile capabilities as a threat, in the longer term Iran possessing missiles and nuclear weapons can seriously destabilize the situation in the region and across the world, and this would pose a new threat to Russia. In addition to countering possible Iranian threat, there are several reasons that make the cooperation of Russia with the US and NATO desirable.

First, such cooperation may play a crucial part in promoting positive strategic partnership of the two nuclear superpowers and the leading NATO countries. This cooperation would also embrace other areas of security and help flesh out the new Euro-Atlantic security architecture proposed by the president of Russia with concrete programs.

Second, in case of unilateral implementation of the new plan on building BMD in Europe as proposed by the Barack Obama Administration, the absence of such cooperation will inevitably cause another BMD crisis between Russia and the West as the weapons of the BMD acquire strategic potential. Notably, a new crisis after “resetting” might have more acute and devastating character.

Third, despite robust measures taken by the members of the nuclear club to prevent unauthorized or accidental missile launches, there is no hundred percent guarantee that such launches will never happen. This is even more relevant for other existing and potential nuclear missile states. Therefore, it does make sense to protect against such cases.

Fourth, history shows that the relations between states may deteriorate quite drastically (especially in case of unstable, radical regimes), turning non-hostile nuclear missile capabilities into a key national security threat. This was the case with the USSR-China relations in the 1960s-1970s and with the US-Iranian relations in the 1980s.

Finally, even if Iran and the DPRK do not turn into Russia’s enemies, Iran with its nuclear missiles and DPRK enhancing its capabilities may potentially destabilize the situation both regionally and globally, causing a chain reaction of proliferation (in Saudi Arabia, Syria, Turkey, Egypt, Libya, Japan, South Korea, Taiwan) and creating a threat for Russia as well.

#### Great solvency/AT: unilat

Alexander A. Dynkin 10, Director, Institute of World Economy and International Relations of the Russian Academy of Sciences, 6/22/10, “FOREWORD,” in NON-NUCLEAR FACTORS OF NUCLEAR DISARMAMENT (Ballistic Missile Defense, High-Precision Conventional Weapons, Space Arms), https://www.files.ethz.ch/isn/144178/10002.pdf

Though I am by no means trying to predetermine the course of the conference, I would like to stress that the influence of BMD systems on nuclear disarmament and non-proliferation depends not only on specifications of the defense systems – in no smaller extent it is determined by the military-political format of their development. Developing BMD systems on the basis of NATO/US-Russia cooperation will, among other things, practically contribute to further reduction and non-proliferation of nuclear weapons. A recent evidence of this is the unified position of the great powers on the UN Security Council resolution on Iran concurrent with the cancellation of US plan to deploy a strategic BMD system in Europe and with the signing of a new START Treaty.

However, developing and expanding BMD on a unilateral basis or only within the framework of the existing alliances, is most likely to hinder further nuclear disarmament and disrupt the cooperation of the great powers in the sphere of non-proliferation with all the consequences that come with it, including the extension of the nuclear club and the possibility of terrorists' gaining access to nuclear weapons.

Yet, just to say that the great powers should cooperate on BMD would be far from sufficient. Indeed, despite the fact that in the 1990s and in the current decade the United States and Russia have made quite a number of unilateral proposals and even had a series of joint computer-assisted exercises and signed several joint documents, things have not got off the ground.

The truth is that joint development of BMD requires addressing a whole range of most complicated issues. In addition to technical and financial matters (such as secrecy, intellectual property protection, operational compatibility as well as the sharing of costs, research and development and, subsequently, the allocation of operational functions) there are serious strategic and political issues to tackle.

It is assumed that a joint tactical missile defense system (TMD) designed to protect the US, its allies and Russia against sub-strategic rockets would not cause major strategic frictions, since the two powers do not possess intermediate- and shorter range missiles. However, the dividing line between tactical and strategic ballistic missile defense is presently rather vague and will only be further dissolved as technologies advance.

Most or all of the missile capabilities of other nuclear states (China, India, Pakistan, Israel and the Democratic People’s Republic of Korea (DPRK)) and non-nuclear-weapon states possessing missile capabilities (Iran, Saudi Arabia, Turkey, Egypt, Syria, Libya and Yemen) consist of shorter- or medium-range weapons. Hence, these states will surely assume that a joint US-Russia BMD is aimed against them.

Are the United States, Russia and their allies prepared for the reaction of the said states to their joint TMD, and are the great powers on the same page as to which of these states should be regarded a priority threat?

As to strategic BMD, things are even more complicated. For the time, the strategic relations between the US and Russia (plus the forces of the UK and France) are based on mutual nuclear deterrence, which in its turn relies on mutual ability to inflict unacceptable damage with intercontinental ballistic missiles (ICBMs) and sea-launched ballistic missiles (SLBMs); this model of relations was once again sealed by the new START Treaty. Then how will the parties be able to simultaneously build a joint BMD for intercepting the missiles of this particular class? Is it possible to draw distinction between a joint BMD designed for ensuring defense against third countries and a system destabilizing mutual nuclear deterrence?

Will a joint BMD imply abandoning strategic relations based on mutual nuclear deterrence? What will replace mutual nuclear deterrence until total nuclear disarmament is achieved? Are we talking about a fullscale military alliance between the Collective Security Treaty Organization (CSTO) and NATO, and if so, are the two parties ready for it (such an alliance exists between the US, the United Kingdom and France whose nuclear forces are not postured for mutual nuclear deterrence )?

Such an alliance, if it is ever feasible, would be regarded by China – the 21st century superpower – as an alliance against itself. Therefore, China should be engaged in the alliance and the creation of joint BMD, shouldn’t it? Will the US and its partners on joint BMD in the Far East accept this? Will Beijing, as a state claiming leadership in the Third World, welcome such an alliance? What is then to be done with respect to India – a partner of both the US and Russia – whose nuclear forces are aimed against China and Pakistan? If India is embraced by the ballistic missile defense, what is to be done with Pakistan? Is it possible (similarly to the NATO-Russia alliance, which is still only a theoretical proposition) to renounce mutual deterrence and create a military alliance in the China-India-Pakistan triangle as well?

The implementation of the new START Treaty is indirectly associated with the preservation of BMD systems roughly within their current scope, which is underlined in the Treaty’s Preamble. Hence the question: what changes to these parameters will undermine the Treaty? At what stage and in what forms should the development of ballistic missile defense systems become a joint task for the sake of preserving the Treaty? What are the limits of further reduction of strategic offensive arms under the next treaty in case of unilateral ballistic missile defense development or in the context of potential US-Russia cooperation on BMD?

Without at least basic answers to all the abovementioned, as well as to other questions, we may hardly count in earnest on the US-Russia cooperation, even if we call for such cooperation for another hundred times.

Further, how will the development of conventionally armed high-precision ballistic and cruise missiles by the US and NATO affects the outlook for the next stage of strategic offensive arms reduction and cooperation on BMD? As is well known, Russia’s new Military Doctrine prioritizes the threat of an air-space attack, and, consequently, the building of airspace defense1 system for Russia. One could hardly imagine Russia taking part in the development of a joint BMD with the US (NATO) while simultaneously building its own air-space defense system against the same states.

There is yet another question: what impact may the development of space arms have on strategic offensive arms reduction and the development of a joint BMD? Are any agreements and rules of conduct possible in the military space sphere?

Finally, what impact the developments in the areas related to strategic offensive arms, BMD, high-precision conventional weapons and space weapons systems may have in terms of nuclear weapons and missile technology proliferation on the global scale?

Untangling a most complicated knot of the said issues and processes or even outlining basic principles and criteria of, as well as paths towards solutions is one of the major objectives of the military and political expert community in Russia and the West at the current stage. The turning point that has been reached in the recent months must be consolidated and enhanced in every possible way lest the commencing constructive cooperation of the two powers be suffocated by the obstacles and conflicts that are characteristic of their relations. Thus, this session within the framework of the joint IMEMO-NTI project is of great importance and relevance.

Given the profile of the project and high professionalism of the participants, we may expect that the discussion will result in a profound analysis of the problems and will enable us to arrive at meaningful and applicable conclusions and proposals contributing to mutual understanding and practical cooperation between the parties on the complicated issues outlined above.

#### Solvency card that connects really well to the advantage---only multilaterally-deployed global missile defenses transcend mutually assured destruction---that solves long-term inevitable nuclear wars because of deterrence failures, miscalc, accidental launches, etc

Jerome Slater 2K, University Research Scholar at the University at Buffalo, 7/15/2000, “The Best Defense is Mutual: Rescuing Missile Defense from Both its Supporters and Opponents,” https://buffalonews.com/2000/07/16/the-best-defense-is-mutual-rescuing-missile-defense-from-both-its-supporters-and-opponents/

Critics of a missile defense system make two principal arguments. The first is that it can never work. The second is that it would be a bad idea to deploy defenses even if they worked, for defenses would inevitably lead other states to greatly expand their numbers and types of offensive weapons in order to overcome the defenses. In the jargon of the nuclear age, the nuclear balance of terror -- also known, aptly, as the system of mutually assured destruction, or MAD -- would be "destabilized."

In the context of the Cold War, this argument was generally persuasive. If the United States had deployed defenses against Soviet missiles, Moscow would have feared that its nuclear deterrent would be rendered useless, tempting Washington to initiate a nuclear strike against the Soviet Union.

To prevent such a scenario, a unilateral U.S. defense system would have precipitated a Soviet decision to build up its offensive forces to a level that could overwhelm the defenses. In the end, each side would have spent billions of dollars to create useless defenses against an ever-expanding offensive threat. The greater numbers of nuclear weapons in turn would undercut efforts at arms control, increase the risks of nuclear war and make war, if it should occur, even more devastating.

During the 1960s, both the American and Soviet governments came to accept this gloomy prognosis and agreed to forgo missile defenses in the ABM Treaty of 1969. In the mid-1980s President Reagan sought to revive the issue of missile defense, but the failure of the "Star Wars" technology (laser beams to shoot down missiles) led to a quiet death of that idea.

In the last few years, however, the Republican Party has decided to make missile defense a national priority, leading Clinton to pre-empt the Republican issue by announcing his general support of a national missile defense system, if and when the technology was shown to be workable.

The Clinton missile defense program has two announced purposes and two unacknowledged ones. Officially, it would provide defense against "rogue states," in particular against the kind of modest missile force that North Korea is expected to have by 2005 and Iran and Iraq by about 2010. In addition, the system would provide protection against an accidental or unauthorized Russian or Chinese missile launch. Seeking to avoid offense to China, the administration vigorously denies that it is seeking to nullify the Chinese nuclear deterrent force, but who's kidding who? The Chinese are not fooled and have already made it clear that they will take a variety of countermeasures if Washington decides to deploy defenses.

In reality, the driving force behind the current U.S. missile defense program is not the need to defend against an out-of-the-blue nuclear attack, for even "rogue states" would have no doubt that such an attack would be followed by an overwhelming U.S. response that would destroy their countries.

What really concerns American defense officials is that the Chinese missile force today and the projected forces of North Korea, Iraq and Iran will make it too risky for the United States to use its overwhelming conventional military superiority to intervene in overseas conflicts, say, to help defend Taiwan against a Chinese attack, or to resist rogue state expansionism.

In other words, it's not so much that we fear being the victim of an unprovoked deliberate attack as that we fear nuclear retaliation if we use our overwhelming conventional military force to intervene in Korea, the Taiwan Straits or the Middle East.

It is not only our adversaries that fear a unilateral U.S. missile defense system; most of the rest of the world, including our closest allies, also vigorously oppose such a step. Generally, the Europeans share the view that defenses are destabilizing -- why tamper with the balance of terror that so far has prevented the use (since 1945) of any nuclear weapons anywhere?

Despite the end of both the Cold War and the Soviet Union, Russia has made it clear that it would be forced to resume an offensive arms race against a missile defense system. It fears that what would begin as a small defensive system would inevitably be expanded, perhaps to the point that it might render useless its own nuclear deterrent against the United States.

Are the critics of a national missile defense system right that defenses would be destabilizing?

Even in the context of the Cold War, the argument was always overstated. Moreover, it would be even more unpersuasive if defensive systems were properly structured and deployed not unilaterally but rather as part of an overall, globally negotiated arms control and war-avoidance system.

The almost automatic assumption of critics that nuclear defenses must always be dangerous is based on a double fallacy. It seriously exaggerates the risk to nuclear stability of defensive systems while seriously underestimating the prospects that the current balance of terror will sooner or later break down, guaranteeing unimaginable catastrophe in a defenseless world when it does.

The balance of terror could lead to nuclear war in two very different ways: a deliberate decision by a major nuclear power to attack another state, or an inadvertent war that comes about because of an accidental or unauthorized attack by some crazy general, a la Dr. Strangelove. Those who worry that defenses would be destabilizing are focusing only on the first scenario, which is the least likely way war could occur.

The argument against a missile defense system holds that a state deploying an effective defense against missiles could use it to support aggression. It might decide to unleash its offensive missiles against the nuclear retaliatory force of its enemy, destroying most of it on the ground, and then shooting down the greatly weakened return strike with its defensive missiles.

But in light of the catastrophic destructiveness of nuclear weapons -- and maybe of biological weapons as well -- this scenario is bizarre. A single retaliatory nuclear weapon getting through the defenses would wipe out a major city, killing millions of people.

Therefore, even a slightly rational government would be forced to make conservative estimates. That is, it would have to assume that a significant proportion of its enemy's retaliatory force would survive a surprise attack and then penetrate defenses to strike cities. It wouldn't take too many prospective lost cities to deter a first strike -- one should be enough.

In order for a state with a missile defense system to use it for aggressive purposes, it would have to assume that both its offensive and defensive systems would work with near-perfection.

The offensive strike would have to destroy nearly all the enemy's weapons of mass destruction, and the defensive forces would have to knock out the entire retaliatory strike, including a man with a suitcase carrying miniaturized nuclear or biological weapons into a major city. But in all of human history, there has never been anything close to a perfect offensive or defensive system.

Nonetheless, it does not follow that we should permanently give up the idea of defending against weapons of mass destruction. Rational governments will always be deterred from starting a nuclear war, but by definition, you can't deter accidents, unauthorized actions, miscalculations or madmen. And as long as defenses are banned, all states will be completely vulnerable to that kind of attack.

There is an obvious solution to this apparent dilemma: Defenses can be deployed only on a cooperative, negotiated, multilateral basis. Put differently, the paradox of defense in the nuclear age is that you can defend yourself only if your opponent agrees to let you do so.

A unilateral system is certain to provoke others to defeat it, and they always will succeed in doing so, either by overwhelming force or circumventing the defenses. Long-range ballistic missiles are not necessary. As someone once said, an enemy could always smuggle nuclear weapons into the United States in bales of marijuana, because they know we can't stop that.

On the other hand, cooperative defense deployments, building on the common interest in removing the specter of mass destruction that hangs over everyone, would be different. States that had their own defensive systems would have no rational incentive to make defense impossible.

Multilateral deployment of defensive systems would defend against small-scale accidental and unauthorized missile launches, as well as attacks from a madman.

It is possible that multilateral deployment would be so expensive -- over time, hundreds of billions of dollars -- and with such uncertain prospects for success that it simply wouldn't be worth the cost.

What would justify the costs, though, is that the multilateral deployment of defenses would be the necessary first step toward the replacement of a global mutually assured destruction with Mutual Defense Emphasis.

By one route or another, a defense based on mutually assured destruction will eventually fail -- unless you believe that deterrence can last, as one observer has put it, for "an eternity of rational leaders and stable societies, free from accident and miscalculation."

Short of global disarmament, then, a mutual defense emphasis may be our only real hope of transcending mutual destruction.

What would a mutual-defense-emphasis system consist of? It would be a central component in a global arms-control system, whose main features would be the following:

Vast reductions in numbers of weapons of mass destruction, particularly nuclear weapons. For example, a multilaterally negotiated agreement might allow all states no more than 100 to 200 nuclear weapons, sufficient to deter deliberately initiated nuclear war.

These nuclear weapons would be deployed in invulnerable retaliatory systems, for example: submarines or small, easily hidden and mobile land ICBMs. Thus, a deliberate offensive attack is doubly deterred: not only by the prospect of catastrophic retaliation, but also because the attacker can't hit the targets of a first strike, which must be the weapons of retaliation. Indeed, against all but literally insane potential enemies, deterrence could hardly be more "stable" -- a first strike would accomplish nothing except the destruction of the attacker.

All states would be allowed to deploy extensive defensive systems. Indeed, the United States, which can best bear the costs and is most likely to lead in the technology, would have to agree to provide defensive systems to the rest of the world.

#### Space-based lasers are vital to effective overall missile defense, and international coop creates global deterrence against rogues and revisionist states

Lorinda A. Frederick 9, Lt. Col., U.S. Air Force, flight commander and instructor in intercontinental ballistic missile and missile warning squadrons, has deployed to the combined air operations center, combat operations division, space cell, in support of Operation Iraqi Freedom and Operation Enduring Freedom, Master of Military Operational Art and Science, Air Command and Staff College; Master of Airpower Art and Science, School of Advanced Air and Space Studies, Fall 2009, “Deterrence and Space-Based Missile Defense,” Air and Space Power Journal, Vol. 23, No. 3, p. 107-118

During the Cold War, the United States relied on the nuclear triad to deter ballistic missile threats emanating from the Soviet Union. Today, the threat is expanding to include rogue elements and proliferators of missile technologies undeterred by Cold War methods. Missile technology is growing despite political attempts to stop it. The United States and other nations are fielding advanced missile defenses to counter the threat posed by proliferating ballistic missiles. However, this air-, land-, and sea-based missile defense architecture lacks redundancy and depends on the proper positioning of assets to intercept missiles in their midcourse and terminal phases of flight. This architecture also lacks a reliable capability to intercept missiles during the boost phase—a capability perhaps best provided from space.

Deterrence before Ballistic Missile Defense

The Department of Defense (DOD) defines deterrence as a "state of mind brought about by the existence of a credible threat of unacceptable counteraction."1 "Counteraction” conjures up Cold War images of massive retaliation and vulnerability when the adversary could threaten not only vital interests but also national survival. In the absence of ballistic missile defense (BMD), the US military could not negate or counter the missile threat facing the nation without retaliating in kind. Effective deterrence denies an adversary the benefits of his actions, imposes costs, and/or encourages restraint.2

The United States refined its deterrence strategy during the Cold War from massive retaliation to mutual vulnerability to assured destruction. Massive retaliation, a policy adopted by the North Atlantic Treaty Organization in 1954, threatened an overwhelming nuclear response to any Soviet aggression. ' Limited options forced the United States into a position of fighting fire with more fire or, more precisely, fighting threats with more threats.

Massive retaliation evolved into mutual vulnerability in the late 1950s, when the Soviet Union appeared to match US nuclear capabilities: “With each side vulnerable to a nuclear strike by the other, nuclear weapons no longer conferred a simple military advantage, and their use could not be threatened unilaterally to deter general aggression by a nuclear-capable opponent.”'1 Mutual vulnerability made sense in a time when BMD could not negate or even reduce the threat.

As the Soviet Union and United States continued to increase their nuclear arsenals, mutual vulnerability was bolstered with assured destruction. In the 1960s, the strategy of assured destruction "required each side to possess a guaranteed second-strike capability, one which could survive the opponent's massive, and possibly unanticipated, first strike."5 This strategy did not eliminate mutual vulnerability because one side’s ability to defend against an attack might weaken deterrence by tempting it to strike its adversary first.

To reinforce the stability provided by assured destruction, both sides agreed to limit BMD severely, as set out in the Anti-Ballistic Missile (ABM) Treaty. Such defenses were considered destabilizing during the Cold War because strategists predicted that a defended nation might strike first, confident that it was protected from the limited retaliatory strikes of its adversary's surviving nuclear forces. In truth, these newly emerging BMD technologies had not matured to the point where nations could trust their performance.

Deterrence and Ballistic Missile Defense

After the Cold War, deterring ballistic missile threats became more complicated due not only to the increasing numbers of nuclear-capable states but also to the rise of hostile rogue elements within a state as well as the proliferation of weapons of mass destruction (WMD), along with missile technology and expertise. 6 According to joint doctrine, “the predominant threat is not from a competing superpower, but more likely from the deliberate launch of a ballistic missile from a 'rogue state,' failed state, or terrorist group.”7 Yet, the United States has difficulty tracking ballistic missiles due to the shortage of accurate and reliable intelligence, having “been surprised in the past by an opponent’s earlier-than-expected military technology, including the testing of the Soviet hydrogen bomb, the testing of missiles by Iraq and North Korea, and the acquisition of Chinese missiles by Saudi Arabia."8 Consequently, the "proliferation of advanced technologies for missiles, guidance systems, and WMD warheads has increased the potential missile threat to the homeland” (emphasis in original).9 Today, the United States must attempt to deter both state and nonstate actors.

Nonstate actors and rogue elements complicate deterrence for a number of reasons.10 First, rogue elements' decision makers are harder to identify and locate, let alone deter, than their state counterparts. Without the ability to attribute the use of WMDs to a rogue-element actor, or even its state sponsor, the United States may have difficulty deterring an attack. Leaders of rogue elements and proliferators threaten US, regional, and global security interests because they defy international laws or norms of international behavior and use asymmetric means to attack law-abiding nations.

Second, the fact that states operate more in the open allows the United States to gauge their perceptions, based on their actions: "The objective of deterrence is to convince potential adversaries that courses of action that threaten U.S. national interests will result in outcomes that are decisively worse than they could achieve through alternative courses of action.”11 Because rogue elements do not operate in the open, the United States cannot accurately gauge their perceptions of capability and will.

Third, the United States cannot threaten to inflict substantial costs on rogue elements that have few high-value assets, minimal territorial claims, and small populations, compared to their state counterparts.:J An adversary's hidden calculation of cost, benefits, and risks complicates the US approach to deterrence.

Fourth, it may prove difficult to discern what is important to rogue elements. The United States could easily assume that they share its goals and values—but this is a dangerous assumption.

Fifth, the United States has neither established nor exercised communication channels with rogue elements to the same extent that it has with state actors. Communication is a necessary component of deterrence strategy with regard to relaying the United States' intent to respond to aggression. Even after receiving a clear message, rogue elements may not be deterred. BMD could help the United States deter aggression and respond should deterrence fail.

The Role of Ballistic Missile Defense in Deterrence

BMD should primarily be considered a vital part of a deterrent strategy and secondarily an effective tool to protect against ballistic missile attacks. BMD is an integral part of deterrence because it makes escalation less likely. Confidence in BMD technology may allow US decision makers to accept an increased risk of attack and allow time for other instruments of power to defuse the situation. Adversaries must consider US defensive capabilities in relation to their offensive capabilities. Confident that inbound ballistic missiles will not reach the homeland, the United States could choose not to respond in kind to such provocation.

Extending BMD to friendly states bolsters deterrence because it effectively conveys to potential aggressors the US commitment to defense. Extended deterrence can keep other states out of the conflict. For example, the United States provided Israel with theater missile defense (TMD) during Operations Desert Shield and Desert Storm to protect the Israelis and keep them out of the broader conflict. Extended deterrence may encourage allies to "forgo indigenous development or procurement of duplicative military capabilities, thereby enhancing US counterproliferation efforts.” BMD is more than just a defensive measure that the United States possesses to knock down threatening missiles. Decision makers should think of it as a vital part of deterrence to help restrain rogue elements and proliferators.

Presidential Perspectives on Missile Defense

Key political decisions made during the presidential administrations of Ronald Reagan, George H. W. Bush, Bill Clinton, and George W. Bush highlight the progress (or lack thereof) made towards developing potential missile defense capabilities.

Pres. Ronald Reagan

When he entered office in 1981, President Reagan inherited a deterrence strategy based on assured destruction, which relied on the unmistakable ability to inflict an unacceptable degree of damage upon any aggressor or combination of aggressors— even after absorbing a surprise first strike. Frustrated with this strategy, he announced the Strategic Defense Initiative (SDI) in 1983, beginning the United States’ pursuit of an active national missile defense (NMD). Thus began a research and development (R&D) effort to protect the United States against a full-scale missile attack from the Soviet Union.M The envisioned system would consist of air-, land-, sea-, and space-based sensors and interceptors. Space-based elements included "constellations of Earth-orbiting battle stations” that would destroy ballistic missiles during their boost and midcourse phases.15 Technologies developed under SDI would allow deterrence policies to rely on defending the United States instead of destroying the enemy.

The concept of using space-based hit-to-kill interceptors emerged from Project Defender, founded in 1958 by the Defense Advanced Research Projects Agency (DARPA), which recognized the promise of advanced weapons and initiated the development of laser technology scalable to the power levels required for BMD.16 In 1980 DARPA began exploiting newly emerging laser and particle-beam technologies for BMD applications, including space-based laser defense against ballistic missiles and aircraft.17 DARPA programs brought the United States closer to deterring and responding to ballistic missile attacks from space.

Technologies pursued under SDI could be restricted, depending on the administration's interpretation of the ABM Treaty. According to Article 5 of the treaty, "each Party undertakes not to develop, test, or deploy ABM systems or components which are sea-based, air-based, space-based, or mobile land-based.’’18 The administration reinterpreted the ABM Treaty to allow for the testing of space-based missile defense (SBMD) technologies.19 Although members of Congress largely supported increased R&D, they rejected this broad interpretation of the treaty. It was one thing to explore the potential of SBMD on paper and develop technology; it was quite another to test and demonstrate the capability.

SDI challenged the traditional treatment of space as a sanctuary.20 Believing that the benefits of missile defense outweighed the costs, President Reagan stood up new organizations and attempted to break down barriers, allowing these organizations to explore space capabilities for defense. This display of will to deploy SBMD technologies did not go unnoticed by the rest o f the world, the Soviet Union in particular. At a summit meeting in 1986, Soviet president Mikhail Gorbachev pressed President Reagan to "accept limitations to the SDI program as a pre-condition for other agreements restricting offensive arms."21 The Soviet Union opposed SDI because the new capabilities could weaken its power and security; however, President Reagan refused to accept any restrictions.

In order to win the Cold War, President Reagan was willing to challenge old paradigms about deterrence and rethink treaty obligations, asking, "Wouldn’t it be better to save lives rather than to avenge them?”22 According to Henry Kissinger, former national security adviser and secretary of state, "Soviet leaders were not impressed by Reagan's moral appeals, but they were obliged to take seriously America’s technological potential and the strategic impact of even an imperfect defense."23 President Reagan was looking for a technological alternative to assured destruction. The bipolar world in existence at the start of his presidency would radically change in the next administration.

Pres. George H. W. Bush

President Bush faced the daunting task of shifting the United States from bipolar to multipolar threats. The Warsaw Pact dissolved in 1989, as did the Soviet Union two years later." Regional threats, such as those from Iraq and Iran, as well as continued missile proliferation, became more apparent. Iraq’s invasion of Kuwait in 1990 and the global response in the form of Desert Storm charted a course for multilateral relationships. During the Cold War. space systems had focused on the strategic threat posed by the Soviet Union, but as the strategic environment shifted, they began to support multiple regional threats.

President Bush's administration reviewed SDI as part o f a broader examination of US strategic requirements for an emerging "New World Order” in which assured destruction no longer formed the basis of deterrence.25 The review concluded that the most important threat to the United States would come from unauthorized or terrorist attacks by limited numbers of missiles. Additionally, deployed US forces would face increasing threats from shorter-ranged theater missiles due to the proliferation of ballistic missile technology.

Responding to this change in threat, President Bush announced that the DOD was refocusing the SDI program away from defending against a massive Soviet missile attack towards implementing a system known as Global Protection Against Limited Strikes (GPALS), designed to protect US forces overseas, US friends and allies, and the United States itself from accidental, unauthorized, and/or limited ballistic missile strikes.-5 GPALS had three components, only one of which —Brilliant Pebbles—relied on space. Space capabilities played a supporting role in the other two components—TMD and limited NMD. A constellation of small, autonomous, kinetic-energy interceptors, Brilliant Pebbles would detect and destroy ballistic missiles in their boost, post-boost, and early midcourse phases of flight. A March 1992 report to Congress highlighted the potential of Brilliant Pebbles for intercepting every Iraqi Scud missile launched against Israel and Saudi Arabia during the Gulf War." This insight was based on simulations of actual Defense Support Program data collected on Scud launches.

The space-based laser (SBL), another program that showed potential for missile defense, sought to detect, track, engage, and destroy theater and strategic ballistic missiles in their boost, post-boost, and midcourse phases29 The program examined the capability of directed-energy weapons, such as lasers, to destroy targets on or above Earth’s surface. 30 Energy delivered by a laser would propagate at the speed of light and stay on target until that energy accumulated to a destructive level.31 After destroying the missile, the laser could quickly target the next missile and continue this process until it ran out of either fuel or targets. 32 Multiple SBLs could increase the probability of the missile defense architecture's successfully intercepting incoming missiles.

Reassured because the deterrent effect of its missile arsenal would remain intact for the time being, the Soviet Union (now Russia) welcomed the Bush administration’s shift from SDI, which emphasized defense against large-scale attacks, to GPALS, which emphasized defense against limited attacks. But rogue elements and other states now had cause for concern since the United States was on a fast track to acquiring BMD capabilities that could negate missile technology they might acquire. President Bush appreciated the value of missile defenses and had the will to field them.

Pres. Bill Clinton

President Clinton continued the shift in focus of missile defense programs from national to theater applications during his administration. This shift became apparent in his narrow interpretation of the ABM Treaty’s prohibition o f the development, testing, and deployment of sea-, air-, space-, and mobile land-based ABM systems and components.33 Showing its support for missile defense, Congress continued to fund SBMD development programs. However, because President Clinton preferred land-based missile defense programs over space-based programs, he ended Brilliant Pebbles. 44 The Advanced Technology Kill Vehicle program, which used technology developed through Brilliant Pebbles to produce small, lightweight kill vehicles for use in surface-based interceptors, died as well.

President Clinton also cancelled the Clementine II space probe due to concerns about violating the ABM Treaty.35 By bring small projectiles at asteroids, it would test technologies for use in missile defense applications.36 Clementine II would have demonstrated SBMD-relevant technologies to quell political concerns about the potential o f Brilliant Pebbles technology.r The best Clementine technology demonstration program also attempted to space-qualify first-generation Brilliant Pebbles miniature, self-contained hardware and software.38 “This Clementine mission achieved many of its technology objectives during its flight to the Moon in early 1994 but, because of a software error, was unable to test the autonomous tracking o f a cold target."39 Fluctuating political concerns and differing interpretations of the ABM Treaty reflected changes in the US will to deploy SBMD.

These cancellations might have been an instinctive reaction to the end of the Cold War and the perceived lack of a credible ballistic missile threat. However, the world became more dangerous following the Cold War because, instead of the threat emanating from one country, now it came from many smaller countries. Not realizing that the ballistic missile threat was increasing, the United States cut funds for missile defense, and teams of technologists either moved on to other projects or disbanded.

The world remained a dangerous place, so the nation still needed the benefits that missile defenses could offer. In 1998 the Iranians flight-tested their medium-ranged Shahab-3 missile, quickly followed by a North Korean Taepodong-1 missile launch demonstrating their capability to extend the missile’s range by using a third stage.4" Reacting to these two events, the United States began development of TMD, a light, mobile, land-based BMD system that would thwart very limited nuclear attacks.41

Russia took the US pursuit of missile defenses seriously. After a summit meeting, President Clinton and Russian president Boris Yeltsin expressed interest in pursuing cooperative TMD activities and issued guidance concerning the TMD capabilities not permitted under their new agreement. Both sides agreed not to “develop, test, or deploy space-based TMD interceptor missiles or components based on other physical principles capable of substituting for interceptors.”42 Even though previous presidents had argued that the ABM Treaty did not ban space-based TMD components, President Clinton committed the United States to refrain from deploying them, thereby reinforcing his views of space as a sanctuary.

With the emphasis now on TMD, the Clinton administration still needed to determine what should happen with NMD. The ”3 + 3" program, created in June 2000, accelerated research and testing for the next three years to build up information needed to assist the president in deciding whether or not to deploy an NMD system. Furthermore, the system would then be fielded within three years of the decision to deploy. Although President Clinton had the opportunity to make a deployment decision before leaving office, he did not do so.

Concerns about the costs of missile defense started to override the benefits during President Clinton’s administration. The elimination of Brilliant Pebbles and Clementine, as well as the decision to continue studying NMD rather than make a deployment decision, indicates that President Clinton had doubts about the benefits o f NMD. His willingness to negotiate with President Yeltsin on TMD criteria showed that he valued missile defense. President Clinton calculated the strategic threat and potential benefits differently than previous presidents. The threats remained, and missile defenses were still viable—but those defenses, particularly space-based components, were too expensive to develop and field.

Pres. George W. Bush

President Bush's administration took an active interest in missile defense. His secretary' o f defense, Donald Rumsfeld, chaired the 1997 Commission to Assess the Ballistic Missile Threat to the United States, which concluded that the United States would have little or no warning o f threatening ballistic missile deployments and argued that America should develop the means both to deter and defend against hostile acts.41

In late 2001, President Bush announced the United States’ withdrawal from the ABM Treaty with the former Soviet Union: "I have concluded the ABM Treaty hinders our government’s ability to develop ways to protect our people from future terrorist or rogue state missile attacks."44 While abiding by the ABM TVeaty, the United States could not pursue the deployment of land-based missile defenses. Its withdrawal from the treaty made clear to Russia and the world that the United States was committed to developing missile defenses to counter an attack. As long as the ABM Treaty remained in place, it blocked prospects of an effective missile defense for the United States and limited options for defending military forces, allies, and coalition partners stationed overseas.4'

For President Bush, the benefits of missile defense once again overrode the costs of both TMD and NMD. Like President Reagan, President Bush sought to remove the restriction on deploying such a defense. The United States was willing to seek unilateral options for deterring ballistic missile attacks by creating a credible defense. The full range o f missile defense options (including SBMD) became available when the United States withdrew from the ABM Tfeaty.

The Current Ballistic Missile Defense Architecture

The United States must maintain the technological capability to respond if deterrence tails. Multiple opportunities to intercept an incoming ballistic missile increase the probability of a successful interception. BMD "must provide an active, layered defense that allows multiple engagement opportunities throughout the boost, midcourse, and terminal phases of a missile’s flight to negate or defeat an attack as far from the Homeland as possible."46 Throughout these phases, a BMD could incorporate land-, sea-, air-, and space-based elements, using both kinetic and nonkinetic means to destroy hostile missiles.47

The nation’s current BMD architecture relies on space components to sense and cue terrestrial interceptors. Space-based sensors can detect the heat of the burning booster during its boost phase and transmit trajectory information to ground stations. Once the booster extinguishes and infrared-sensing satellites lose track of the missile, radars can track it throughout the remaining flight time. These radars cue terrestrially based BMD elements so they can attempt to intercept the missile. Commanders on the ground, in turn, can launch interceptors to destroy it. Currently, the United States possesses land- and sea-based kinetic-kill intercept capabilities but no space-based intercept capability.

The level of support for SBMD capabilities has waned since President Reagan first started SDI, but support for land-and sea-based missile defense has remained stable and even grown. President Reagan supported R&D for missile defense in all mediums (air, land, sea, and space) and provided the funding to back his SD1 program. Pres. George H. W. Bush continued President Reagan’s initiatives but at a reduced level due to the changing threat environment and declining defense budget. President Clinton favored missile defense, with the exception of SBMD; however, he did not provide enough funding for it, thus limiting the scope of BMD to TMD. Pres. George W. Bush reinvigorated missile defense by extending BMD to incorporate NMD in all mediums except space, where he opened the door, enabling future presidents to cross this threshold.

Benefits of Space-Based Missile Defense

Many characteristics of SBMD could create uncertainty in the minds of potential adversaries about whether or not they could achieve their aims.48 Space provides access to threats in areas that terrestrial, maritime, and airborne defenses cannot reach. SBMD is capable of destroying ballistic missiles over the enemy’s territory before they release multiple reentry vehicles or countermeasures designed to thwart defenses.

The constant forward presence of SBMD could allow the United States to limit its military footprint on foreign soil and support many military operations simultaneously. Land- and sea-based interceptors have to be placed in areas where they can provide credible protection from ballistic missile attacks. Prepositioning infrastructure, supplies, and equipment may shorten response times when hostilities erupt, but they are costly and difficult to sustain. SBMD allows a nonintrusive forward presence because it does not require the prepositioning of assets on other territories.

Furthermore, employing SBMD is not contingent on approval from another nation. The continued presence of US assets on foreign soil depends on the host nation’s accepting or approving the mission that those assets support. If defenses are not in position, deterrence is reduced. Stationed in the right orbits in the right quantities, SBMD could deter or defend against attacks around-the-clock, especially if used in concert with other sea- and land-based missile defenses.

Responding to Countermeasures

Potential adversaries may develop countermeasures in response to the US fielding of an SBMD because the latter would make their capabilities ineffective. R&D of countermeasures, which takes time and money, may result in reduced payload and/or range of the missile. These monetary and performance costs may be enough to deter an adversary from attempting countermeasures.

One countermeasure against nonkinetic SBMD capabilities—hardened missiles—could have a reduced payload due to the added weight of the hardening material and additional fuel needed to reach the required distances. The adversary could also field more missiles to saturate the missile defense architecture. 49 The saturation point depends upon the numbers of both space-based and terrestrially based interceptors deployed. Because decoys and countermeasures are deployed after boost phase, SBMD could lighten the load for midcourse and terminal-phase defenses.

The adversary could also shift from ballistic missiles to cruise missiles but would pay a penalty in terms of speed, reach, and destructive potential. These penalties, in combination with existing cruise missile defenses, could make an attack less likely to succeed. Space sensors designed to trigger SBMD could also trigger TMD to intercept cruise missiles. SBMD could increase the effectiveness of the current BMD architecture even if the adversary employs countermeasures. Credible capabilities have the potential to deny an adversary’s objectives and therefore may deter him from employing ballistic missiles altogether. Key political decisions help explain the progress (or lack thereof) made towards exploring and developing the potential of SBMD.

The Way Ahead

SBMD progressed through various programs, such as GPALS, Brilliant Pebbles, Clementine, and SBL, despite dwindling support from presidential administrations following President Reagan’s. Pres. George W. Bush paved the way for the next administration to put SBMD on the international agenda. According to The National Security Strategy of the United States of America (2006), the United States may need new approaches to deter state and nonstate actors and deny them the objectives of their attacks.50 Additionally, the National Strategy to Combat Weapons of Mass Destruction (2002) states that "today's threats are far more diverse and less predictable than those of the past. States hostile to the United States and to our friends and allies have demonstrated their willingness to take high risks to achieve their goals, and are aggressively pursuing WMD and their means of delivery as critical tools in this effort. As a consequence, we require new methods of deterrence.”51

Cooperation on missile defense initiatives could increase global stability. By banding together in coalitions, countries can deter war by repelling an attack against any member.52 States and rogue elements will not be able to strike surreptitiously if they know that the international community could quickly discern the origin of any launch and compute potential impact points. Attempts by a rogue element to destabilize the region through the attribution of attacks to a state may initially promote the rogue elements own agenda. However, data provided by missile defense and other sensors can refute such claims. The shared international ability to identify launch and impact points might deter states and rogue elements from launching in the first place. The more nations cooperate with each other, the more stable the world becomes.

Policy makers need to invest in the development of many different capabilities, including SBMD, to negate missiles in their boost phase and use the information gleaned from these developments to inform decisions. One approach involves bringing a system to the prototype stage for testing and accurately gauging its performance. This approach could let the United States invest in only a limited number of prototypes, thus deferring large-scale production to allow further research, development, and testing. These efforts could decrease the risk of failure during production and deployment. 5' When the need arises, the United States should capitalize on preexisting prototypes as long as the industrial base could support rapid production.

By funding R&D for SBMD, the United States would ensure the viability of these technologies. The DOD cannot expect developments in commercial industry to be available for national security purposes. Competitive pressures force industry to fund near-term R&D programs and choose near-term survival over longterm possibilities.54 Applied research into SBMD technologies would allow the United States to gain more knowledge about boost-phase defenses. America will get as much R&D in SBMD technologies as it is willing to fund.

The United States may need to examine the standards it applies to the fielding of other BMD systems and adjust expectations for an initial SBMD capability. Henry Kissinger has commented on the standard of perfection applied to missile defense:

The experts had all the technical arguments on their side, but Reagan had got hold of an elemental political truth: in a world of nuclear weapons, leaders who make no effort to protect their peoples against accident, mad opponents, nuclear proliferation, and a whole host of other foreseeable dangers, invite the opprobrium of posterity if disaster ever does occur. That it was not possible at the beginning of a complicated research program to demonstrate SDI’s maximum effectiveness was inherent in the complexity of the problem; no weapon would ever have been developed if it first had had to submit to so perfectionist a criterion.55

Fielding even imperfect elements of the architecture may deter an adversary, as occurred in Desert Storm when imperfect TMD helped keep Israel out of the war.

The fact that senior leaders and policy makers tend to focus on current issues because they are more tangible puts the United States at risk of not funding research critical to its future defense. America may need to avoid pressures to sacrifice long-term research for the sake of short-term procurement by moving away from having policy determine the technologies pursued and letting feasible technologies inform policies necessary to deter threats.

Conclusion

Credible deterrence depends on technological capability and political will. During the Cold War, the United States relied on the nuclear triad to deter ballistic missile threats emanating from the Soviet Union. These capabilities reinforced the political will expressed through policies such as massive retaliation and assured destruction. We had no defense against ballistic missile attacks. Today, the nuclear triad still deters threats from Russia and China; however, the threat has expanded to include rogue elements and proliferators undeterred by Cold War methods. The current land- and sea-based missile defense architecture provides a limited defense against these threats, but it lacks redundancy and depends on the proper positioning of assets to intercept missiles in their midcourse and terminal phases of flight.

Attaching a monetary figure to SBMD is difficult. A cost/benefit assessment should include potential cost savings in other parts of the missile defense architecture in relation to the benefits, including rapid responsiveness, global power projection, and constant presence. The United States must also consider the cost of expanding current missile defense layers to achieve the added deterrent and protective effect that SBMD could provide. Putting a monetary value on deterrence represents the main difficulty of a comprehensive assessment.

The continued proliferation of ballistic missile technology to states and rogue elements warrants increased research into SBMD. The United States should continue to demonstrate the international will necessary to help deter the proliferation of ballistic missiles while providing the capability to defend against rogue elements should deterrence fail.

#### The plan is the perfect middle ground---starting with bilateral U.S.-Russia coop that’s open to other states creates global agreement on cooperative space BMD

Charles Shotwell 94, assistant professor of political science at the US Air Force Academy and formerly a USAF National Defense Fellow with the International Security Studies Program at the Fletcher School of Law and Diplomacy, Tufts University, served as chief of the Legislative Affairs Section for the Deputy Under Secretary of the Air Force, International Affairs, Lt. Col., U.S. Air Force, et al., 1994, “Ballistic Missile Defense for the Twenty-First Century: At The Crossroads of Global Security,” <https://www.bits.de/NRANEU/BMD/documents/shotwell94.htm>

There are options available other than the maximalist or minimalist approaches. The alternative presented here represents a recognition that something more than minimal cooperation is needed between states to combat the dangers of weapon proliferation, but that full integration of global defense systems may be undesirable or unworkable, It is a recognition that national sovereignty and independence of action need not be sacrificed in order to bring about some level of global cooperation for purposes of ensuring international peace and security.

The reality is a complex network of bilateral, multilateral, and multi-bilateral relationships. The treaty must be amended by bilateral US-Russian effort, but with bilateral consultations with each signatory's defense partners. The amendment could provide the basic structure for a follow-on multilateral arrangement. Structuring the discussions this way provides for maximum US and Russian leverage over defense partners, while still including them sufficiently for meaningful cooperation in the later multilateral forum.

The basic objectives of the regimes would be to provide defense against ballistic missiles and to address the causes of proliferation. A viable variation would be a combination of regional and global arrangements for the exchange of early warning information. This parallels the early debates prior to the end of World War II about whether power should be given to a global body, such as the United Nations, or to regional organizations. The answer was a compromise, as now appears in the UN Charter. Although the Security Council has the preponderance of authority, regional organizations are given considerable power in the settlement of regional disputes.

Under this scheme, arrangements would be negotiated for regional early warning and defense centers and would be adapted to regional needs and conditions. These arrangements would allow for flexibility in local arrangements and make the job for negotiators easier by reducing the number of nations required to agree to the arrangement. NATO's structure is well suited for integration into such a framework.

Conclusion

We are at a Crossroads, where decisions must be made for the future course of policy. Policymakers must recognize the dramatic changes in the security environment undermining the validity of previous planning assumptions and the extraordinary challenges that lie ahead.35 New threats and new technologies require adjustments of strategy and policy.36 The failure to adapt to changed conditions is a key peril for decision makers.37 The costs in doing so are quite substantial.

It is clear that many states are preparing to use space to gain military advantage. The facade of compliance with the sanctuary doctrine has fostered a growing cynicism among several states. The changes in the reality of the use of space dictate that the diplomatic reality catch up with the security reality. Even the Senate Armed Services Committee noticed a "gap" between defense planning and the diplomatic reality:

The committee is concerned by the apparent gap between SDIO planning assumptions with regard to programs that raise ABM Treaty compliance problems and the progress to date in US and Russian efforts to negotiate amendments of the ABM Treaty. The committee urges the President to pursue vigorous changes to and clarifications of the ABM Treaty.38

The treaty will not go away of its own accord. It requires affirmative bilateral action to amend it to meet our new security needs. This provides some unique opportunities, particularly while we enjoy unprecedented favorable relations with Russia. It is an opportunity to mold the future and, perhaps, counter the emerging threat of proliferation. Such opportunities usually do not last for long and the opportunity costs for failing to act could be significant.

Placing the issue of the use of space for defensive purposes on the world agenda in the context of the global protection system could serve to force all players to "lay their cards on the table." The issue recognizes the reality of state actions in the use of space but channels those activities into an open, constructive, and cooperative mode. Rather than allowing space to be subverted to aggressive purposes, we may bring the militarization of space under control by addressing the issue publicly.

It is clear that some actions must be taken unilaterally by the US for defense. There is no global system that can be solely relied upon for our security. It is also true that the causes of the major threats to national security (i.e., the proliferation of weapons of mass destruction and their delivery means) can be dealt with most effectively in a regime of greatly increased global cooperation.

Once again, states around the world are looking to the US for leadership. Therefore, a primary concern should be that of developing all aspects of US security policy in a coordinated effort. The technology involves long lead times and is dependent upon political direction. The threat posed by ballistic missiles requires a methodical, long-term strategy. The prerequisite for a coherent strategy is reconciliation of the national security imperative with the political imperative.

### Solvency---Russian Tech

#### Russian technical contributions are absolutely vital to effective space-based missile defense

Alexei G. Arbatov 10, Head of the Center for International Security, Institute of World Economy and International Relations of Russian Academy of Sciences, Corresponding Member of the Russian Academy of Sciences; Vladimir Z. Dvorkin, Major-General (rtd.), Chief Researcher, Center for International Security, Institute of World Economy and International Relations of Russian Academy of Sciences; and Sergey K. Oznobishchev, Head of Sector, Center for International Security, Institute of World Economy and International Relations of Russian Academy of Sciences, 6/22/10, “NON-NUCLEAR FACTORS OF NUCLEAR DISARMAMENT (Ballistic Missile Defense, High-Precision Conventional Weapons, Space Arms),” https://www.files.ethz.ch/isn/144178/10002.pdf

Russia’s cooperation potential. The United States is an unquestionable leader in the development of non-strategic and strategic BMD. Unlike the previous plans of the Bush Administration on the deployment of strategic BMD that had not been properly developed, the four-stage program announced by the current Administration appears to be quite well thought through. Sustained perfection of the profoundly tested Aegis sea-based BMD system with its SM-3 interceptors provides for further enhancement of the effectiveness and the range by increasing the solid-propellant mass of the interceptor (with the diameter of stages 2 and 3 increased by half from 13.5 in. to 21 in. ), as well as by upgrading the guidance and control systems. It is expected that owing to the increased speed, the interceptor missile will be capable of destroying Iran’s missiles in boost phase (providing that Aegis-capable ships are deployed in the Mediterranean Sea). Also there hardly will be any problem in adjusting them for deployment as landbased interceptors.

However, at this stage there is no ultimate certainty on the European deployment of not only the land-based version of the SM-3 interceptors, but also of the X-band (centimeter wavelength) radars. One cannot exclude the possibility of these radars to be deployed in Turkey, Georgia and Eastern Europe. In any event, these radars will be part of the general BMD of the United States and Western Europe which includes the radars of the missile early warning system.

At the same time, further buildup of GBI-type strategic three-stage ground-based interceptor missiles in Alaska (Fort Greely, 26 interceptors) and California (Vandenberg Air Force Base, 4 interceptors) is being suspended. Another 14 GBI launching silos are currently under construction in California. These launching silos are intended as reserve and will house the interceptors if necessary. Though it is assumed that these measures will protect the US against single ballistic missile launches, test launches of GBIs will continue. It is known that the flight tests have begun for the twostage version t of GBI that was previously intended for deployment in Poland.

Despite the dominance of the US in this sphere, Russia also has certain cooperation potential - primarily in the field of information support and interception capabilities of a joint BMD. At this stage, the space echelons of Russia’s missile early warning system can hardly be expected to make a major contribution to cooperation, given the current state of these echelons. And then again, the US space-based missile early warning system has growing capability in terms of predicting the trajectory of a ballistic missile once the launch is detected.

However, the probability of detecting missile launches by the space echelons may be affected by clouds at the launch areas, and therefore it may not be a hundred per cent reliable. The Russian radars of the Russian missile early warning system and of the US Ballistic Missile Early Warning System (BMEWS) are the most reliable means of missile launch detection and trajectory prediction. The US experts are well aware of the unique capability of the Russian early warning radar in Mingechaur and the one built near Armavir in terms of detecting missiles launched by Iran.

When a missile is test-launched southeastwards from the site in northern Iran, the Mingechaur radar detects it in 110-120 seconds as it progresses along its flight path, while in case of north-westward operational launches the detection speed of the radar is even higher, which is beyond the capability of any US BMEWS radars. According to the estimates of some independent experts, the integration of US and Russian missile early warning systems will increase the efficiency of detecting launches of ballistic missiles and space launch vehicles by 20 to 70 percent.

Further, there may be certain demand for Russian missile early warning radars with high manufacturing readiness that can be quickly built at the missile-threat directions.

As far as space launch vehicles, the effectiveness and range of interception is known to sharply increase if a space-based information system, such as Space Tracking and Support System (STSS), is deployed. Spacecraft of this type, each of around 650 kg, with infrared and visible-spectrum sensors should be placed in the circular orbits 1,350 to 1,400 kilometers above the ground with a 60 to 70 degree inclination. To place them in orbits, Russian launch vehicles may be used, foremost the converted heavy missiles developed under the Russia-Ukraine Dnepr Project.

In the course of the strategic arms race, the energy characteristics of the heavy missile were perfected to achieve the highest specific characteristics in its class in the world. A number of such launch vehicles converted from RS-20 (SS-18) ICBMs that had been retired upon expiration of their service life cycle were successfully used in commercial projects to launch foreign-owned satellites, demonstrating utmost reliability. Such a launch vehicle with a boost stage and an engine of multiple ignition capability may place in orbit two STSS spacecraft at a time at an altitude of up to 1,400 kilometers with the required inclination. Thus, a low orbit BMD information support force may be deployed much faster and at a significantly lower cost.

In the field of systems and capabilities of missile intercept, Russia’s advanced experience in the development of unique software for the detection of attacking missiles, discrimination of reentry vehicles against decoys and jamming, as well as other developments may be quite useful. In addition, Russia has a well-developed ground test infrastructure with a network of radar, optico-electronic and telemetry stations. Finally, it would be reasonable to include Russian antiballistic missile systems in the BMD architecture in Europe as an important element of cooperation. For example, the Triumf (Triumph) S-400 air defense systems are considerably superior to the US Patriot SAM in terms of range of destruction of airborne targets and ballistic missiles. In the future, the use of still more advanced S-500 air defense system may also be considered.

### Say Yes---Starting Big Solves/AT: Incrementalism

#### Russia proposed starting big and planning a joint missile shield as the initial goal, then filling in the details

Vladimir Frolov 11, Russian political analyst and journalist; Edward Lozansky, President and Founder of the American University in Moscow and the World Russia Forum; and Vladimir Belaeff, president of Global Society Institute, 10/28/11, “Russia's Plan to Save the Earth,” http://www.russialist.org/archives/russia-medvedev-joint-missile-defense-hopes-698.php

Recently a Pentagon official said that the United States had invited Russia to use its own radars and other sensors to monitor one or more U.S. missile interceptor flight tests, but Russia's Foreign Minister Sergey Lavrov made it clear that the offer fell far short of Moscow's calls for a role in planning a missile shield and of binding guarantees that the system would not weaken Russia. "We are being invited to monitor the implementation of a plan that we see as creating a risk to our forces of deterrence," Lavrov told reporters. "It would be better to first collectively create a missile defense architecture that would definitely be aimed outside of Europe and would not create threats for anyone inside Europe ­ and only then to start putting this system in place and inviting each side to monitor one another," he said.

#### The plan establishes data exchange and early warning integration as a medium-term step towards BMD coop---that transforms current U.S.-Russia mistrust and allows an effective response to inevitable global prolif

Alexei G. Arbatov 10, Head of the Center for International Security, Institute of World Economy and International Relations of Russian Academy of Sciences, Corresponding Member of the Russian Academy of Sciences; Vladimir Z. Dvorkin, Major-General (rtd.), Chief Researcher, Center for International Security, Institute of World Economy and International Relations of Russian Academy of Sciences; and Sergey K. Oznobishchev, Head of Sector, Center for International Security, Institute of World Economy and International Relations of Russian Academy of Sciences, 6/22/10, “NON-NUCLEAR FACTORS OF NUCLEAR DISARMAMENT (Ballistic Missile Defense, High-Precision Conventional Weapons, Space Arms),” https://www.files.ethz.ch/isn/144178/10002.pdf

Priority steps. In the meantime, all the joint projects mentioned above can hardly be implemented in the near term in view of the persisting mutual mistrust and conservatism of the state agencies of the parties, as well as considering their concerns for loosing sensitive technologies. To counter these obstacles, first of all it would be reasonable to restore the elements of cooperation that have been abandoned over the recent years. In the first place, the project of a Joint Data Exchange Center (JDEC) to monitor the launches of missiles and space launch vehicles must be immediately revived. The decision to establish the JDEC was made 12 years ago by the then presidents of Russia and the United States. The incumbent presidents of the two powers reaffirmed their intention to move on with the project at their Moscow meeting in 2009.

A more recent idea is to create a virtual JDEC which would in the first place allows avoiding the expenses for setting up a new facility to replace the one that was dismantled. In addition, it would facilitate the resolution of issues related to the liability for damages. To do so, it would be reasonable to call to mind its tasks and operational procedures that were fully agreed in the past.

The JDEC was supposed to facilitate sustainable exchange of data on ballistic missile and space launch vehicle attacks received from US and Russian missile attack warning systems (MAWS), as well as to minimize the consequences of false warning of missile and carrier vehicle launches and prevent false alarm missile launches in response. In addition, the JDEC was supposed to contribute to potential implementation of the multilateral regime of exchanging notifications on the launches of ballistic missiles and space carrier vehicles.

The basic missions assigned to the Joint Data Exchange Center were as follows:

- Providing information on announced and unannounced launches of ballistic missiles and space-launch vehicles detected by US ballistic missile early warning systems (BMEWS) and the Russian missile attack warning systems;

- Achieving fast resolution in the Joint Commission of possible ambiguous situations associated with information from early warning systems;

- Facilitating the preparation and servicing of a unified database for the multilateral regime of exchange of notifications concerning launches of ballistic missiles and space-launch vehicles.

Information was to be exchanged on the launches of ballistic missiles and carrier vehicles detected by the early warning systems, as well as on ballistic missile launches by third states that might pose a direct threat to the United States or Russia or might bring about an ambiguous situation and lead to its possible incorrect interpretation. The data intended for exchange is the information received from the space-based and ground echelons of the US and Russian early warning systems.

Information should be provided in a processed form, if possible, in near-real time.

The following formats were provided for the exchange of information:

- When a ballistic missile launch is detected: time of launch, generic missile class, geographic area of the launch, geographic area of payload impact, estimated time of payload impact, launch azimuth;

- When a launch of space vehicle is detected: time of launch, generic class, geographic area of launch, launch azimuth.

The process of data exchange was to develop in phases.

Phase I. In phase I of the JDEC operations, information was to be provided on detected launches of ICBMs and SLBMs belonging to either of the parties and, with rare exceptions, for detected launches of space-launch vehicles also belonging to either party, including firings of ICBMs, SLBMs and space-launch vehicles from territories of third states as well as launches of ICBMs, SLBMs and space-launch vehicles of third states made from the territory of the United States or Russia.

Phase II. In this phase it was assumed that Russia and the United States would provide information on detected launches included in phase I, as well as information on detected launches of other types of ballistic missiles belonging to either party with a range in excess of 1,500 kilometers and a maximum altitude in excess of 500 kilometers.

Phase III. The parties were supposed to exchange information on detected missile launches specified for the two preceding phases, as well as information on the detected launches of ballistic missiles of third states with a range in excess of 500 kilometers or an altitude in excess of 500 kilometers, if part of the flight trajectory of the ballistic missile as calculated by the launch azimuth was expected to go over the US or Russia’s territory, or if the impact area of its payload was projected to be within either party’s territory. Russia and the United States were also supposed to provide information on detected starts of space-launch vehicles of third states, if projection of the initial launch azimuth indicated an intersection of the territory of either party within the first half-orbit of launch. At the parties’ discretion, information could also be provided on other detected launches of space-launch vehicles of third states, regardless of launch azimuth.

The US and Russia were to provide information on launches of third states that they believed could create an ambiguous situation for their respective warning systems and lead to possible misinterpretation of each other’s actions. Subsequently, the Joint Commission was to consider the possibility of exchanging information on missiles that intercept objects not located on the earth’s surface (i.e. BMD and ASAT systems). In the future, the US and Russia were planning to consider the possibility of expanded data sharing on detected launches of ballistic missiles and space-launch vehicles globally, taking into account changes in the global strategic situation and the level of development of multilateral regime for the exchange of notifications of launches of ballistic missiles and space-launch vehicles.

The US and Russia were to appoint their Heads (1 person each) and Deputy Heads (2 persons for Russia and 1 person for the US) who were to have equal rights in managing the activities of JDEC. The JDEC Heads were to jointly carry out the daily management of JDEC activities and be jointly responsible for the performance of the tasks assigned to the JDEC. Operations of the JDEC were to be carried out by specially trained personnel of the parties (the US and Russia – 12 persons each: 6 teams consisting of 2 persons).The maintenance was to be performed by technical support personnel (4 persons for Russia and 2 persons for the United States). Russia was to provide security and support personnel (62 persons).

If a virtual JDEC was created in Russia’s territory at the command center of a MSWS or at the Nuclear Risk Reduction Center (Defense Threat Reduction Agency in the United States), national duty shifts were to be formed at each of the selected sites to exchange the information. The Russian duty shift would transmit the authorized information on the detected launches with a delay measured in minutes. The information transmitted to a duty shift did not need to be cleared from all false alarms, since it would be better if the BMD received erroneous information rather than missed actual missile launches.

The strengths of the virtual JDEC include reduced number of communications channels required, and increased promptness of data transmission achieved through the reduced number of transmission links.

The weaknesses of the virtual JDEC include the necessity to transmit the data through the channels of the Internet which raises the issue of protecting the exchanged data. Another weakness is the need to integrate the hardware/software of the Russian and US parts of the JDEC. Before the JDEC starts its operations, a series of additional joint research tests must be completed to resolve hardware- and software-related issues.

Still, considering the strengths and weaknesses of a virtual JDEC in terms of reliability of received information and avoiding confusion, reviving the previously agreed project appears to be the best option.

To resume joint exercise on BMD, it is essential to recreate the experience derived from the latest joint exercise on BMD in the US-NATO-Russia format when the parties achieved certain progress in the training on the conceptual structure and compatibility of information systems and means of interception. Interruption of such exercises result in the loss of the accumulated experience due to professional turnover. Meanwhile, joint research is in any case necessary to enable the parties to move from computer assisted exercises to full-scale command exercises and later on to using the US and Russian operational anti-missile weapons on test grounds, as it was agreed during the latest exercise in the US-NATO-Russia format.

Thus, the organization- and technology-related opportunities for the cooperation of Russia, the United States and the European members of NATO exist in a number of complementary areas. These opportunities may be realized if there are political decisions on the US-Russia strategic partnership at the top national level.

However, the joint exercise on TMD should reach beyond the limited theatre of operations, since given the recent developments; there is no point in convincing the Europeans that they may only be threatened by short-range ballistic missiles. In other words, the intention to cooperate with Europe only in the sphere of non-strategic BMD is an anachronism, to say the least.

There is divergence in the parties’ actual positions on BMD. The rationale of the US opponents of such cooperation may be the reluctance to make additional commitments and therefore fall into a position of dependence on Russia, as well as concerns related to a potential technology leakage.

Russia does not regard Iranian and South Korean missile capabilities as a threat, with higher priority assigned to politico-military and technical threats emanating from the United States and NATO. In the recent years, the new endeavors of Moscow and Washington have somewhat defused this perception. However, a decisive turn for the better is still a long way to go.

Still, even aside from debates on whether Iranian and South Korean missiles are posing a threat to Russia, Moscow’s cooperation with the US and NATO appears more than desirable for a variety of reasons.

First, such cooperation may play a crucial part in promoting positive strategic partnership of the two nuclear superpowers and other NATO countries. It will also embrace other areas of security and help to flesh out the new Euro-Atlantic security architecture proposed by the president of Russia with concrete programs.

Second, in case of unilateral implementation of the new plan on building BMD in Europe as proposed by the Barack Obama Administration, the absence of such cooperation will inevitably cause another BMD crisis between Russia and the West as the weapons within the BMD acquire strategic potential. Notably, a new crisis will have an even more acute and devastating character.

Third, despite the tough and well-tried measures taken by the members of the nuclear club to prevent unauthorized or accidental single missile launches, there is no hundred per cent guarantee that such launches will be always prevented. This issue is even more relevant for other existing and potential nuclear and (or) missile states. Therefore, it does make sense to protect against such cases.

Fourth, history shows that the relations between states may deteriorate quite drastically (especially in case of unstable, radical regimes), turning non-hostile nuclear missile capabilities into a key national security threat. This was the case with the USSR-China relations in the 1960s-1970s and with the US-Iranian relations in the 1980s.

Finally, even if Iran and the DPRK do not turn into Russia’s enemies, Iran with its nuclear missiles and DPRK by further developing its capabilities may potentially destabilize the situation both regionally and globally, causing a chain reaction of proliferation (in Saudi Arabia, Syria, Turkey, Egypt, Libya, Japan, South Korea, Taiwan) that would create a threat for Russia as well.

For the past four decades, ballistic missile defense was a major area of strategic rivalry in the USSR/Russia-US relations. In the new environment, with due wisdom and political will, ballistic missile defense could become a major positive factor for the consolidation of efforts of the great powers and their allies on addressing new global security challenges.

### Missile Defense Advantage

#### Only space-based defenses effectively protect allies and stop EMP attacks---those collapse the entire undersea cable network

Dr. Peter Vincent Pry 18, served as chief of staff of the Congressional EMP Commission, and on the staff of the House Armed Services Committee and at the CIA, 1/17/18, “Trump must realize Reagan's vision for Star Wars defense — and soon,” https://thehill.com/opinion/national-security/369185-trump-must-realize-reagans-vision-for-star-wars-defense-and-soon

Space-based defenses offer revolutionary advantages over existing National Missile Defenses (NMD), that cannot protect U.S. allies or bases overseas, might be hard-pressed to defend the U.S. mainland against increasingly sophisticated North Korean threats, and cannot defend the U.S. from large-scale nuclear missile threats from Russia or China.

Space-based defenses potentially can do all the above.

SDI-type defenses can intercept missiles during all phases of flight: boost-phase, mid-course, and terminal-phase. Such a system could shield U.S. allies and troops overseas; much better protect Hawaii, Alaska, and distant U.S. territories; and could not as easily be attacked, overwhelmed, or fooled with decoys as NMD.

These advantageous characteristics of space-based defenses are all the more important because of the existential threat from nuclear electromagnetic pulse (EMP) attack. Even a single warhead successfully delivered against allies overseas or against the United States could black out an entire nation and kill millions.

Even a single weapon detonated for EMP at mid-course, over the ocean, would have catastrophic consequences for the world economy. Ambassador Henry Cooper warns: “Whether deliberate or accidental, the EMP from such high-altitude explosions could disable the world’s entire undersea cable network that reportedly carries about $10 trillion of financial transactions in a single day as well as huge volumes of data, from e-mails to classified government-to-government information.”

#### Only genuine coop solves NATO-Russia tensions

Sam Nunn 10, Democratic U.S. Senator from Georgia for 24 years, co-chairman of the Nuclear Threat Initiative; Igor Ivanov, was Russia’s foreign minister from 1998 to 2004; and Wolfgang Ischinger, former German ambassador to Britain and the United States, chairman of the Munich Security Conference; all three are co-chairmen of the Euro-Atlantic Security Initiative commission, 7/21/10, “All Together Now: Missile Defense,” https://www.nytimes.com/2010/07/22/opinion/22iht-edischinger.html?\_r=1&ref=global

No other initiative has more near-term potential to ease the NATO-Russian relationship out of its petulant, impacted state, while giving a positive jolt to the revived but tentative and unfocused interest in an improved and more inclusive European security system, than missile-defense cooperation.

Were North America, Europe and Russia to make defense of the entire Euro-Atlantic region against potential ballistic missile attack a joint priority, they would — apart from addressing a concrete problem — in a single stroke undermine much of the threat analysis that sets Russia against NATO, and prove that trilateral cooperation on a key security issue is possible.

After decades of failed efforts to find common ground on missile defense, leaders in Washington, Moscow and Brussels have returned to the task. Both U.S. and Russian presidents have underscored the importance of finding a mutually acceptable approach to missile defense, and the U.S. side, in the run-up to the June 24 Washington summit, proposed a series of steps to start the process.

NATO Secretary General Anders Fogh Rasmussen last March moved three-way cooperation on missile defense to the very center of his proposed agenda, stressing the importance of creating “a missile-defense system that not only defends the Euro-Atlantic community, but one that also brings it together.”

No one thinks it will be easy. Years of thickening mistrust, differing threat analyses, and a deficit of political will still weigh on the prospects for cooperation — notwithstanding the recent improvement in U.S.-Russian relations.

Nor are the technical obstacles trivial. For both practical and political reasons a fully integrated system with joint command and control may be a reach too far. Even separate but coordinated systems, the model experts think more likely, pose formidable challenges.

But, significant as these hurdles are, the more fundamental point lies elsewhere. Political will, not technical obstacles, will determine whether missile defense becomes a pillar of a more inclusive and better-defended Euro-Atlantic community, or persists, even grows, as a source of tension and discord within what national leaders in their moment of hope at the Cold War’s close spoke of as a “Europe from the Atlantic to the Urals whole and free for the first time in 300 years.”

The necessary political will, however, will almost certainly not emerge where it must — among all three parties, North America, Europe and Russia — unless the process, the system and its implementation are of, by and for all three.

It will not come if a missile-defense system is essentially the creation of a single country with invited participation, or the work of two countries, or the project of an alliance. From the start, Europe, North America and Russia should assess jointly the common threat, and then undertake as equal parties to design from the ground up a common architecture to deal with the threat.

Elements of the Obama administration’s new U.S. four-stage territorial defense system may well provide a critical core for the effort, but the ultimate architecture and the division of labor sustaining it should be an equally balanced three-legged stool.

The reasons for treating missile-defense cooperation as an imminent and serious objective go much beyond narrow concerns. More than a potential game changer in U.S.-Russian and NATO-Russian relations, more than a crucial step in search of a sounder European security order, and more than an essential factor in creating an optimally effective defense against ballistic missile threats, genuine trilateral cooperation in this instance promises to aid progress in bolstering the nuclear nonproliferation regime.

It should add momentum to the already impressive achievements in securing nuclear weapons and materials. It would help Washington and Moscow address the role of strategic offense and defense as they contemplate new steps to render their nuclear relationship safer and more stable.

And, not least, it will also create a basis by which strategically key states, including China, can explore cooperation on the role and place of missile defense in a multipolar nuclear world.

Progress on all these fronts requires U.S., European and Russian leadership, and their success will either be enhanced or impaired by what happens in the realm of missile defense.

### Arms Control Advantage

#### Key to disarm momentum and preventing breakout if disarm is ever achieved

Oliver Thränert 15, head of the think tank at the Center for Security Studies at ETH Zurich in Switzerland, 3/1/15, “Limit missile defense—or expand it?: A German response,” Bulletin of the Atomic Scientists, Vol. 71, No. 2, p. 13-16

Missile defense systems, according to their critics, undermine strategic stability and represent an obstacle to nuclear disarmament. But in fact—whether additional nuclear powers emerge in the future or nuclear weapons are eliminated entirely—missile defense could have important stabilizing effects.

Today, Moscow and Beijing don’t perceive US missile defense as a stabilizing force. Russia and China argue that US missile defenses undermine their nuclear second-strike capabilities. Even though this claim isn’t accurate (especially in Russia’s case), both nations are modernizing their nuclear arsenals, with US missile defense as a justification. The question, then, is how to achieve conditions under which missile defense can fulfill its potential as a stabilizing force. Limiting missile defense through arms control negotiations isn’t the proper approach. Rather, discussions should focus on international cooperation in missile defense systems—and on making such systems an important stabilizing element in a world free of nuclear weapons.

More nukes, fewer nukes

It’s difficult to say whether the future will bring further nuclear proliferation or progress toward general disarmament. Under either scenario, missile defense could contribute to security.

If more and more countries seek to develop nuclear weapons, as well as missiles to deliver them, missile defense could play an important role in defending the international order. New nuclear weapon states, certainly, could be tempted to engage in aggressive behavior—invading small neighbors, for instance, on the assumption that nuclear weapons would deter outside powers from intervening (Sagan and Waltz, 1995). But if outside powers were equipped with effective missile defenses, intervention would be more likely (ideally, under a UN mandate). The more effective the missile defenses, the lower the constraints on intervention. Thus nuclear proliferators would be deterred from invading their neighbors. Nuclear aspirants in turn would be less likely to think of nuclear weapons as tools for exercising regional leverage. An important incentive for establishing nuclear weapons programs would disappear.

And what if the world achieved complete disarmament? Once again, missile defense could play a very important role in security—this time, by ensuring that nuclear weapons didn’t emerge all over again.

In a “zero” world, the reemergence of nuclear weapons would be a danger for several reasons. First, a world without nuclear weapons would not be a world without dictatorships, which means that nuclear verification and transparency would always remain fragmentary. Second, the peaceful uses of nuclear technology are becoming attractive to more and more countries. Third, a world without nuclear weapons probably wouldn’t be a world without missiles—to the contrary, civilian space programs will probably become achievable for an increasing number of states over time. Therefore, the possibility would always exist that a nation with ballistic missile capabilities could achieve nuclear breakout and immediately threaten other countries over long distances.

Missile defense systems could provide a hedge against such threats. Even a limited missile defense system could serve as insurance against clandestine nuclear rearmament at the early stages of a nation’s nuclear weapons development, when defenses would only have to provide protection against limited offensive capabilities. In a world free of nuclear weapons, missile defense could render cheating an unattractive option for potential rogue states—even if they acquired nuclear capabilities, their ability to threaten others with significant damage would be constrained. In fact, today’s nuclear weapon states would probably see establishing such conditions as an important precondition for engaging in dramatic nuclear reductions and pursuing complete disarmament. However, if missile defense is to contribute to nuclear reductions and one day to complete disarmament, the most important precondition is for the United States and NATO to cooperate on missile defense with Russia—and eventually with China and other countries.

To be sure, missile defenses cannot solve all the problems that complicate the disarmament process. But they can be an important part of the solution.

Challenging relationships

Today, Russia possesses some 1,500 strategic nuclear weapons—plus thousands of nondeployed nuclear warheads and weapons awaiting dismantlement (Arms Control Association, 2014). As long as the Russian arsenal remains so large, no US administration launching a first strike against Moscow could entertain any hope that US missile defenses would limit the damage from a Russian counterstrike to an acceptable level. Arguably, this wouldn’t change even if the Russian arsenal became much smaller. Only if the United States and Russia agreed to reduce their nuclear arsenals to very low levels—say, 100 weapons each—could Washington theoretically expect to gain a premium from launching a first strike. And even this would pertain only if US missile defenses were far superior to Russian missile defenses. Even then, no American president could be certain that no Russian second-strike weapons would penetrate US missile defenses and cause unacceptable damage to the United States and its population.

Russia says that it will not enter new negotiations on nuclear disarmament unless Washington is prepared to accept limits on missile defense. But this does not mean that Moscow is actually afraid of US missile defense. Rather, Vladimir Putin perceives nuclear weapons as a kind of great-power currency, and he does not want to negotiate that currency away. Instead, he uses US missile defense as a pretext for carrying out nuclear modernizations that were planned in any event. So it’s true that US missile defense stands in the way of further disarmament by the United States and Russia. But the reasons for that are political, not strategic.

Chinese military planners have much more reason to worry about US missile defense than do their Russian counterparts. China possesses only about 250 nuclear warheads in total (Arms Control Association, 2014). Still, it would be a big gamble for the United States to carry out a first strike against China—a successful nuclear counterstrike could not be ruled out. In any event, China is not prepared at this point to demonstrate any transparency in the nuclear arena, let alone pursue arsenal reductions. Beijing’s concerns about vulnerability vis-à-vis Washington are too great. China’s attitude is motivated in part by a perception that US missile defense is a threat to Beijing’s nuclear second-strike capability—even if this perception is not entirely valid.

Tool for disarmament

In the US-Russia and US-China relationships, missile defense stands in the way of further nuclear disarmament. But it doesn’t have to be that way. Rather, missile defense should become a tool for further disarmament. To achieve this, future negotiators should concentrate on international collaboration in missile defense, not on missile-defense limits. And they should harmonize collaboration on missile defense with a step-by-step approach to nuclear disarmament.

#### Cooperative BMD gets China into nuclear arms control---it’s the only way to create a post-START trilateral agreement

Reuben Steff 13, Lecturer in the Political Science and Public Policy Program at the University of Waikato, New Zealand, April 2013, “Cooperative Ballistic Missile Defence for America, China, and Russia,” Contemporary Security Policy, Vol. 34, No. 1, p. 94-119

The Bush administration would have benefited from adopting a realist assessment of likely responses to BMD. Realism suggests that sensitive actors are compelled to alter course in response to costs imposed upon them or to shifts in the global or regional balance of power. Indeed, cost-benefit analysis has historically played a part in motivating powerful states to attempt a rapprochement with their enemies.75 The willingness of the Bush administration in 2008, and of NATO in 2010, to begin discussions with Russia over BMD cooperation suggests a belated appreciation of this. Recently, these efforts have faltered over differing visions of what kind of system should be deployed, while both sides cite a lack of trust and political will to find a compromise as hardliners in the Kremlin and conservative Republicans in Congress view cooperation as appeasement.76 Mutual distrust is a significant obstacle to cooperation, as American and Russian officials have voiced fears of being cheated in a joint effort.77 But even in seemingly irreconcilable relationships reassurance is not impossible, nor is it without utility because it can still function to reduce the risks of miscalculations and accidental war, paving the way for substantive military reassurance later.78 Therefore extensive trust is not necessary for reassurance to begin or for cooperation to emerge.79

Furthermore, actors in both Moscow and Beijing appear to have identified BMD as the cause of a new great power security dilemma. In reference to American missile defence plans and Russia’s response, former Russian Foreign Minister Sergei Ivanov said: ‘We can break this vicious cycle only through coordinated efforts’.80 Chinese experts Zhong Jing and Pan Zhenqiang explain that Beijing does not seek to build its own security on the insecurity of others. Instead, Beijing believes that states should understand how their actions affect others and that certain decisions, like abrogating the ABM Treaty, can cause a ‘chain of actions and reactions’.81 America’s power affords it the ability to offer concessions since it can be more confident than weaker parties that it will not suffer unacceptable costs should other states fail to reciprocate, while historical cases of successful rapprochement show that it is usually the stronger party that makes the initial opening.82 Indeed, in light of the gross disparity in power in America’s favour, efforts to reassure others of American intentions could benefit from a grand strategy of restraint.83 Embracing this approach would better conform to the defensive realism world that now exists, helping to consolidate this system by reducing incentives for states to challenge the status quo. Of critical importance is Kupchan’s recognition that cooperation between democracies and nondemocracies is possible. Kupchan holds that assuming otherwise not only reduces the chance for immediate collaboration but ‘discourages non-democracies from remaining open to mutual accommodation and the exchange of concessions – steps critical to advancing reconciliation and programmatic cooperation’.84 An approach to American–Chinese and American–Russian relations that emphasizes ideational and ideological differences guarantees that cooperation on BMD will remain out of reach.

A concerted, multidimensional, and incremental reassurance programme has the greatest chance of success for two reasons. Firstly, incremental cooperative efforts will reduce the consequences of being cheated by a greedy state pretending to be a security seeker. This will build trust by signalling one’s benign intentions, and if small steps are reciprocated that create mutual gains, it can deepen trust and beget further cooperation.85 Secondly, BMD must be only one vector of security cooperation, while a gradual and incremental approach to cooperation will be more politically palatable, aiding those engaged in internal debates with hardliners since political reconciliation threatens some domestic political actors and industrial sectors who benefit from competition and who may act to block cooperative initiatives. Furthermore, changing intentions (and altering the other states’ perception of one’s intentions) is a long-term and complex process that requires a sustained and comprehensive strategy of engagement. A related part of an incremental approach will require widening the scope of cooperation beyond military collaboration to include deepening economies ties, cultural exchanges, admission of past wrongs, and the alignment of historical narratives.86 Indeed, it could greatly aid the cause of Russia–US relations if leaders on both sides came to a common agreement over their Cold War history and the cause of its ending, as US commentators repeatedly state they ‘won’ the Cold War. This acts to strengthen nationalist and hardline elements in the Russian polity who believe the West considers them to be a defeated rump state and a secondary power unworthy of equal relations.

Analysts must also recognize that BMD is set to remain a permanent feature of the international security system, as it is viewed as a military necessity by America’s armed forces, as crucial for underpinning power projection, as having bipartisan political support, and as being intertwined with the military-industrial complex. Moreover, BMD systems are proliferating throughout America’s alliance system, as NATO countries, Japan, South Korea, Taiwan, Australia, India, and Israel are cooperating on systems development, purchasing their own independent systems, or engaging in talks to host elements.87 It is necessary for all sides to discuss how to prevent the ongoing BMD cooperation between the United States and its allies from undermining strategic stability among established nuclear powers. This will require overcoming the contradiction between BMD designed to buttress America’s security guarantees to its Central European allies in the face of a resurgent Russia and the desire to increase global security by bringing Russia into Euro-Atlantic BMD efforts.88 Finally, If BMD is to function as a security management resource, and facilitate incremental nuclear disarmament, arms control may have to be reintroduced into the equation since it is a powerful signal of benign intent, especially if it reduces the ability of states to challenge the status quo.89

Reasons for Optimism under the Obama Administration

Based on the above, the following pillars should guide future efforts to construct a positive programme for ballistic missile defence (BMD) cooperation:

. the goal of joint BMD is the restoration of trust and projection of benign intentions;

. joint BMD should be one area of security cooperation amongst many;

. incremental cooperative efforts are essential;

. substantive security cooperation between democracies and non-democracies is possible; and

. BMD cooperation is most likely if the unipolar power pursues a grand strategy of restraint; arms control theory can play a positive role in joint BMD efforts.

Importantly, the United States and Russia today have more common interests than at any other time since the end of the Cold War. The Obama administration appears to realize this, noting that their paramount joint interest converges upon nuclear nonproliferation which requires the ‘active cooperation of Russia’.90 Additionally, Secretary of State Hillary Clinton stated that Washington and Moscow ‘now have common enemies’.91 Furthermore, through the 2010 Ballistic Missile Defense Review Report (BMDR), Obama altered the focus of American BMD by cancelling the Third Site in Central Europe, reportedly in exchange for Russia’s cooperation on halting Iran’s weapons programme.92 In its place the BMDR announced the European Phased Adaptive Approach (EPAA) that will be deployed in four main phases from 2011 to 2020 and is a template for deployment of other regional BMD systems – in East Asia and the Persian Gulf.93 The BMDR noted that ‘one of the benefits of the European Phased Adaptive Approach is that it allows for a Russian contribution if political circumstances make that possible’.94 In a speech on these changes, Obama cited the ‘enormous potential’ for cooperation on missile defence with Russia: ‘In confronting that [Iranian] threat, we welcome Russia’s cooperation to bring its missile defense capabilities into a broader defense of our common strategic interests, even as we continue ... our shared efforts to end Iran’s illicit nuclear program’.95 The BMDR continues: ‘both Russia and China are important partners for the future, and the United States seeks to continue building collaborative and cooperative relationships with them’.96 Another reason is that as much as Obama’s historic commitment to a nuclear free world was preceded by advocacy from senior ex-policymakers, cooperative BMD has been subject to a similar campaign.97

Obama’s overall strategic reorientation has, in some ways, followed the path laid out by defensive realist critics of the Bush administration, whose correctives emphasized strategic restraint.98 Obama’s preference for offshore balancing indicates this as it ‘relies on a reduced military presence overseas, greater reliance on regional allies’.99 Furthermore, his strategy has revealed that ‘[f]or the first time in at least 70 years, the underlying pattern of America’s foreign-policy doctrine is not the expansion of the U.S. role’.100 An important vector of this strategy has involved the objective of sharing the global security burden with American allies.101 With this in mind, Secretary of Defense Leon Panetta explained that ‘the United States must place even greater strategic emphasis on building the security capabilities of others’.102 Obama’s BMD policy has reflected this, as it emphasizes cooperation and multilateralism over the bilateral deals the Bush administration pursued.

On the resurgence of Russia and the rise of China, Obama sought to placate their fears of American power, saying ‘I’ve made it clear the United States does not fear the rise of peaceful, responsible emerging powers – we welcome them. Because when more nations step up and contribute to peace and security, that doesn’t undermine American power, it enhances it’.103 This approach was embodied by a commitment to move towards a multipartner, rather than multipolar world, since ‘no one nation – no matter how powerful – can meet global challenges alone’.104 This was consistent with the United States–Russia reset, launched in early 2009, leading to a number of mutual cooperative ventures with Moscow and the re-invigoration of nuclear arms control through New START.105 Relatedly, the 2010 National Security Strategy document downgraded America’s ideational commitment to spreading democracy when it stated: ‘Our moral leadership is ground principally in the power of our example ... not through an effort to impose our system on other people’.106 Notably, it rejected nuclear primacy by emphasizing the importance of ‘reinforcing strategic stability’ – that is, maintaining mutual deterrence – with Russia and China.107 It continued that this would be an ‘important challenge in the years ahead’, since ‘both are claiming U.S. missile defense and conventionally-armed missile programs are destabilizing’.108 Expanding on this, Ellen Tauscher said: ‘Russia is not a target of those [missile] defenses. We seek to transcend traditional thinking on strategic stability, often associated with Mutually Assured Destruction, in favour of a concept of Mutually Assured Stability’.109

Therefore, a promising proposal is for a shield whose rationale and specific role would be oriented around non-proliferation, since it threatens the freedom of action of all great powers. This would have the following benefits:

. Joint technological development would share the costs of increasing systems effectiveness. This will create industrial partnerships, which in turn generate domestic constituencies in favour of maintaining cooperation.

. It would isolate rogues, as China and Russia would have to forgo their role as supplier of arms to these states as a condition of joining any joint BMD system.

. It is more in line with a strategic environment that is characterized by transnational threats, as it would facilitate state-to-state security assurances, freeing up resources to address non-state-centric threats.

. Cooperative BMD will help to address the problems of creating a verification system to monitor global disarmament and reduce fears of cheating during the transition to low nuclear levels.110

. Cooperation on BMD could be part of a package of inducements in negotiations with proliferating states, with proposals to halt regional deployments of missile defences in exchange for a freeze on ongoing nuclear and ballistic missile development.111

. In a sign of mutual strategic restraint, BMD free zones could be established if regional states judge that deployment would be destabilizing, even as cooperation continues on joint BMD in other proliferation-susceptible regions.

. Finally, it would give China and Russia a stake in the ‘new structure of deterrence’ that the 2010 BMDR called for.112

The latter will be increasingly important in American–Chinese relations. Unless comprehensive dialogue over the role of BMD in the evolving bilateral strategic relationship takes place, the linkage between American BMD and China’s nuclear modernization programme and build-up threatens to heighten the mutual distrust regarding long-term intentions. Indeed, the emergence of a Chinese second-strike capability may not create greater strategic stability between the United States and China, especially if China is tempted by its expanding economic and military power (buttressed by its nuclear modernization programme) to behave more assertively in its immediate region. Indeed, the fear of this will compel American planners to seek additional offensive and defensive capabilities (with East Asian states demanding additional weaponry), provoking the very Chinese behaviour they seek to deter.

The Obama administration stated that it wants to engage China in dialogue on missile defence, and that ‘maintaining strategic stability in the American–Chinese relationship is as important to this Administration as maintaining strategic stability with other major powers’ – a significant change from the past.113 Furthermore, former Secretary of Defense Robert Gates stated that dialogue on the nuclear relationship would be ‘in the best interests of global security’.114 China in turn might be receptive to dialogue and future cooperation on missile defences and nuclear armaments if it is part of a larger strategic framework, and could entice the West by proposing increased transparency on the scope of its military build-up and capabilities. As such, discussions on nascent BMD cooperation could aid America and China as they seek to adjust cooperatively to the changing distribution of political, military, and economic power between them.115

Cooperative BMD Proposals and Prospects

Joint ballistic missile defence (BMD) would require surmounting technological and operational challenges, and expanding intelligence gathering. Such a system would require a diverse and potentially disparate array of radar stations, sensors and satellites, multi-tiered interceptors on hair-trigger alert, and close command-and-control relationships involving multinational forces. America’s advantage in BMD technology also represents a hurdle since it would require transfer of sensitive technology to other great powers. For these reasons, cooperation will have to be incremental. Moscow has proposed integrating its own and NATO’s BMD capabilities into a single system with full-scale interoperability. This would cover continental Europe and Russia through a ‘sectoral approach’ whereby Russia and NATO would stand ‘back to back’ and have responsibility for defending against missile attacks over a specific sector of Europe.116 This would reassure Russia that NATO BMD was not targeted at it by giving it a veto, or ‘red button’ rights, over the launch of interceptors. Furthermore, this system would be under joint command and underpinned by a legally binding agreement with NATO that neither side would target the other’s offensive missiles with their BMD interceptors. Russian Deputy Foreign Minister Sergey Ryabkov explained the logic of this approach: ‘If two separate networks are built, things won’t change for us and we will see a situation when the NATO system could potentially be used against Russia’s security interests. Cooperating on such a system would mean hurting ourselves’.117 However, this has proved a non-starter for NATO, which says it cannot be bound by any legal commitments and will not ‘outsource’ responsibility for defending its own territory to Russia.118

A second and more promising proposal has been outlined by a number of former European, Russian, and American officials, think tank experts, and academics, under the rubric of the Euro-Atlantic Security Initiative (EASI). In February 2012 they released a study entitled Missile Defense: Toward a New Paradigm.119 This put forward a proposal for the phased deployment of a cooperative BMD system to create ‘an inclusive, undivided security space free of opposing blocs and gray areas’.120 This system would provide more transparency about one another’s intentions and a more complete picture of missile threats and launches. Its proposed architecture was jointly created by a former director of the US Missile Defense Agency and a former chief of staff of the USSR Strategic Rocket Forces.121 In this system, the US/NATO and Russia would each maintain their own command and control centres on their own territory that would be connected to cooperation centres jointly staffed by officers from NATO and Russia located in Warsaw and Moscow (and possibly Brussels). Data and information about missile launches and flight trajectories received separately by Russian and US/NATO satellites would go to their respective command and control centres but would also be transferred simultaneously to the cooperation centres prior to being filtered/screened to protect sensitive information of each party. The data and information would then be fused in the cooperation centres and passed back simultaneously to both the US/NATO and Russian command and control centres. Their separate radars and sensors would jointly create an enhanced picture of launch point locations, point of impact, and early notice of attack. Keeping the systems formally separate surmounts the problems that would be involved in integrating Russian systems into NATO and US BMD command and control. Furthermore, unlike Russia’s sectoral proposal, the interceptors of all parties would remain under sovereign control, and each party would ultimately have responsibility for protecting their own territory. However, ‘separate operational protocols could be negotiated in advance to commit one party to intercept a missile flying over its territory aimed at the territory of another party’.122

This proposal also benefits from the fact that some elements of the architecture already exist and new systems could be added as they come online. For example, the United States already deploys Aegis SM-3 and will deploy new systems under the European Phased Adaptive Approach (EPAA). Russia has S-300 and S-400 air defence systems and will deploy the S-500 systems capable of intercepting shortand medium-range ballistic missiles and possibly ICBMs, and it is upgrading its Moscow-based BMD system with conventional 53TS interceptors.123 Russia has also started developing sea-based missile defence interceptors, similar to the US navy’s Aegis system.124 Additionally, the Cooperative Airspace Initiative (CAI) established by the NATO–Russia Council has run exercises designed to share information on the movements of civilian aircraft passing through NATO or Russian airspace.125 The EASI suggests that proposed CAI operations centres in Warsaw and Moscow could eventually be expanded to receive and exchange information on missile launches.126 Cooperation on intercepting short- and medium-range threats would eventually be expanded to longer-range missiles. Although initial contributions to the system would vary depending upon the investments in BMD technology that have so far been undertaken, the expectation would be that cooperation over time would lead to more equal contributions to the system. The EASI stressed that this system would be an open architecture to allow other states to contribute to the system, and would ensure the system does not come at the expense of strategic stability with China, who could add its own BMD capabilities.127

Dean Wilkening suggests that a first step between Russia and the United States would be to deploy a jointly manned NATO–Russian early warning radar in central Siberia.128 This would improve the performance of the American GroundBased Mid-Course Defense (GMD) system against rogue missiles but not Russian ICBMs, while the joint command infrastructure could be expanded into an international system if trust, political will, and reconciliation processes deepen. Wilkening suggests this could be married to other nascent efforts such as joint missile defence exercises, joint responses to common threats, a joint data fusion centre that would exchange information on missile launches from both countries’ early warning radars, and technical cooperation involving space-based infrared satellites. Finally, although technology transfer (especially in radar technology) would be a sensitive matter, it should be possible since the relevant technology is already available on the international market. If correctly implemented, Wilkening argues that this ‘provides genuine security benefits for all countries, improves strategic stability, and involves potential industrial partnerships’.129

Operational difficulties will also have to be overcome but Russia and the United States are already in the process of carrying out joint exercises in a related field. Russian troops and officials recently trained, for the first time, with American and Canadian counterparts at North American Aerospace Defense Command (NORAD)’s headquarters at Peterson Air Force Base, Colorado. The exercises simulated a joint response to a commercial airliner travelling to Russia from Alaska, and another in which an airliner was hijacked en route to the United States from Russia. As part of the simulation the NORAD base coordinated with teams at America’s Joint Base Elmendorf-Richardson in Alaska and with Russian troops operating in Russia’s far east.130 As 9/11 made clear, airliners are virtual ballistic missiles. These exercises deal with problems to be surmounted in any joint BMD system, such as rapid communications, transfer of authority across international boundaries, and disparate decision-making processes.

Joint systems could be deployed under regional organization umbrellas, such as the Six Party Talks countries negotiating with North Korea, or a Middle East entity to inoculate against Iran’s ICBM forces.131 This has merit, as a premature lunge towards comprehensive joint deployment, especially if it failed, could unravel the entire enterprise and sour political relations. An initial limited joint system would allow teething pains to be smoothed out, common protocols to be developed, experimentation with how joint control would work, and the building of necessary political trust. A joint theatre missile defence (TMD) system would fit this bill, and is an area where Russia could provide its own technological expertise and systems (S-300 and S-400 systems). A regional cooperative BMD system could evolve into a globally inclusive system. Collective security agreements could be reached in which would be agreed that an attack on one element of the system was an attack on all.

These proposals are complementary to collective actor deterrence (CAD), which could be buttressed by collective actor defense (distinguished by the acronym CAD+) – defensive systems operated by collective actors. Indeed, one of the problems with CAD is that certain actors often have less at stake in regional conflicts than others, which can change their desire to join a coalition or act with it. This could be acute in future conflicts with nuclear-armed rogues. CAD+ could decrease the risks and perceived costs that alliance members face in a crisis, facilitating joint action and therefore increasing deterrence. Defensive capabilities could also ameliorate some of the other downsides associated with collective actors by providing time for diplomatic avenues to be pursued while inoculating rogue states and decreasing their ability to leverage their ballistic missile arsenals during crises.

In the context of discussions about deploying joint BMD, engagement, agreement, and even conceptual collaboration would lead to parallel changes in conceptions of deterrence and acceptable strategic postures that do not undermine strategic stability.132 America will also have to reconsider its strategy of extended deterrence and the security demand of regional states for it, since there is a perception that the United States needs outright strategic superiority to credibly extend deterrence to its allies. David Cortright and Raimo Va¨yrynen note that

[i]f the United States, Russia and China were able to work together more constructively, without threatening each other and while providing mutual security assurances, it would be much easier to extend a mantle of security assurance to other states and regions.133

This would be facilitated if the United States made the sale of BMD to its allies conditional upon their agreement to forgo the acquisition of nuclear arms and destabilizing offensive weapons, as this exacerbates regional security dilemmas and lowers the regional status quo for Russia and China. In other words, deterrence stability in regional dyads will complement great power stability and reassurance at a global level.

Political Obstacles and Arms Control

Ballistic missile defence (BMD) cooperation faces political obstacles in the United States, as Republicans have criticized Obama for cancelling the Third Site in Europe and for appeasing Russia.134 But cooperation has precedents. President Ronald Reagan, and his Secretary of Defense Caspar Weinberger, when referring to their proposal for a multi-tier BMD system in the 1980s, the Strategic Defense Initiative (SDI), said that ‘we would hope and assume that the Soviets ... would develop about the same time we did the same kind of effective defense’, and offered confidence-building measures.135 Reagan even went so far as to state that America would give the Soviet Union BMD systems at some future point.136 According to James Mann, Reagan also personally sought to tone down the rhetoric contained in NSDD-75, a key strategic document of his first term, as he sought to emphasize the importance ‘of compromise with the Soviet leadership’ to pursue arms control negotiations based on ‘strict reciprocity’.137 At the 1986 Reykjavik summit Reagan went to lengths to reassure Gorbachev that he would not use SDI to launch a first strike, declaring: ‘That’s why I propose to eliminate ballistic missiles and share SDI with you’.138 Reagan’s private correspondence confirms that this was not a cynical ploy. In a letter to William Buckley Jr. in May 1987, Reagan wrote: ‘When I announced SDI I made it plain ... that I favoured sharing it with everyone’.139

The prescription outlined here may seem more far-reaching than common defensive realist proposals that usually emphasize the importance of maintaining deterrence and arms control. But cooperative BMD would greatly aid these efforts and may be essential for successfully concluding new arms control treaties beyond New START (and for expanding the treaty to other nuclear powers). New START was signed on 8 April 2010, setting a limit of 1,550 deployed strategic warheads by Moscow and Washington. An important segment of the treaty’s preamble recognized that there was an ‘interrelationship between strategic offensive arms and strategic defensive arms, that this interrelationship will become more important as strategic nuclear arms are reduced, and that current strategic defensive arms do not undermine the viability and effectiveness of the strategic offensive arms of the Parties’.140 Following New START, the Obama administration stated its interest in a follow-on treaty that would include, for the first time, tactical nuclear weapons and warheads in storage.141 However, the US Senate had made it clear that BMD would not be included in these talks.142 This is in conflict with Russia’s statements that a follow-on treaty will only be possible ‘in the framework of a comprehensive approach to strategic stability [that includes BMD]’.143

Russia is wary of lower nuclear levels absent reassurance over the goals of America’s BMD programme. Furthermore, New START’s preamble implicitly notes that reaching low nuclear numbers will eventually require expanding the arms control process to China and other nuclear powers, stating that the treaty was signed ‘with a view to expanding this process in the future, including to a multilateral approach’.144 However, Chinese officials have stated that they will only join the American–Russian nuclear arms control process once nuclear parity with Russia and the United States is reached. But China is unlikely to be satisfied with nuclear parity if it is surrounded by a regional and global BMD shield from which it is excluded. Like Moscow, Beijing will have to be reassured that its deterrent is not undermined by US BMD. Arms control could prove critical to achieve this. If the US, Russia, and China agree to make cooperative BMD part of a future multilateral arms control process, it would require protocols to reveal details related to the amount of deployments, type of interceptors, and technical details such as interceptor speeds and placement of radars.

This raises the issues of verification and information exchange. Prior successful arms control treaties, such as the Intermediate Nuclear Forces (INF) Treaty, offer a practical example of how this could be achieved. The INF Treaty’s verification regime was the most detailed and stringent in the history of nuclear arms control. It included baseline inspections to attain a picture of the number of weapons and placements of deployments; closeout inspections at eliminated facilities to verify that all INF-related activities had ceased; elimination inspections to confirm the destruction of missiles; ‘short-notice’ inspections over a period of 13 years; continuous portal monitoring inspections to observe items coming in and out of missile factories; and establishment of a Special Verification Commission to discuss and resolve issues related to implementation. As a result of its success, almost all subsequent arms control agreements have contained some element of on-site inspections and a similar inspection regime could be established for BMD. Furthermore, contrary to arguments made by arms control sceptics that their success or failure merely reflects the temperature of political relations at the time, INF Treaty negotiations began and were ultimately concluded during a difficult period of the Cold War and at a time when most experts claimed they were impossible.145 A final important lesson of the INF Treaty is that negotiating such treaties can be prolonged, demanding, and complex. After all, the INF Treaty took approximately 10 years to be concluded. The process was not linear and it goes without saying that any attempt to insert BMD into a new multilateral arms control process will also likely be a long-term and incremental process accompanied by fits and starts.

Conclusion

Shiping Tang explained that the international system has changed from an offensive world to a defensive world. Clearly, this has led to greater security for states. Efforts to consolidate this world, and perhaps eventually move beyond it, are a venture defensive realists should embrace. This is especially the case since the George W. Bush presidency provided empirical support that unilateral ballistic missile defence (BMD) in a defensive realist world does not pay; deployment undermined great power relations and did not dissuade proliferation. As such, consensus amongst the great powers on a way forward over BMD may be the only way to ensure it does not continue to undermine international security.

Cooperation on BMD between the United States, China, and Russia could prove essential to move towards further reductions in nuclear arsenals. Furthermore, jointly deployed BMD would build trust, bind concerned states together, leverage their joint resources, and increase their ability to protect themselves from mutual threats. The proposal at the heart of this article may appear idealistic, but it is consistent with defensive realist goals. The Obama administration’s preference for dialogue, multilateralism, and arms control is a step in the right direction. Although a new BMD arms control regime is currently ruled out by the Obama administration, future progress may be possible in this area in the context of a larger reassurance programme.

This may increase the freedom of action during Obama’s second term. Indeed, Obama explicitly made this point during a hot mike incident in March 2012, when he said to Russian President Dmitry Medvedev that ‘[o]n all these issues, but particularly missile defense ... this can be solved’ as he would have ‘more flexibility’ in his second term.146 Furthermore, America’s Russian Ambassador Michael McFaul said on 4 April 2012 that American–Russian collaboration ‘will be one of the most important issues for the second term of the Obama administration’ and ‘[t]he president believes that this [BMD] is an issue where we can turn from confrontation to cooperation’.147 These statements are consistent with defensive realist expectations that states are strategic actors and learn from their mistakes. Obama’s tacit recognition that unilateral BMD during the Bush administration induced a security dilemma with China and Russia appears to have led him to conclude that a new cooperative direction during his second term is necessary. Obama’s intention to forge a second arms control treaty with Russia will be difficult, if not impossible, without agreement on BMD.

The case for BMD cooperation is strengthened by considering the most likely alternative. China is bolstering its second-strike capability in the face of the expanding American BMD system and growing more assertive. Chinese officials openly declared the United States to be China’s ‘greatest national security threat’ and view relations in zero-sum terms.148 For his part, Vladimir Putin said in March 2012 that ‘whatever you call it, this has some elements of an arms race’.149 His government, he added, will ‘under no circumstances surrender our strategic deterrent capability, and indeed, will in fact strengthen it’.150 Putin directly linked these moves to BMD, claiming that Russia was being ‘pushed into action by the United States and NATO missile defense policies’.151

Absent cooperative BMD, Beijing and Moscow will continue taking measures to counter American BMD. Even though politics will dominate whether joint BMD with Russia and China ever becomes a reality, cooperation on BMD has strengthened security ties between the United States and its allies, opened up new avenues for joint industrial cooperation, and is now interpreted as key to strengthening their ability to wage collective deterrence. Defensive realism supports a favourable view, as BMD has worked for collective advantage. However, this has so far come at the expense of improving ties with Moscow and Beijing. But there is no reason why extending BMD cooperation would not have a countervailing binding effect.

#### All arms control collapses without Chinese participation, even if New START is extended

Richard Weitz 19, Senior Fellow and Director of the Center for Political-Military Analysis at Hudson Institute, 11/25/19, “Richard Weitz: Even If New START Is Extended, Strategic Arms Control Will Die Unless China Is Involved in New Treaties,” https://russiancouncil.ru/en/analytics-and-comments/interview/richard-weitz-even-if-new-start-is-extended-strategic-arms-control-will-die-unless-china-is-involved/?sphrase\_id=34284765

What measures do you think Russia and the U.S. should take upon the expiration of the New START Treaty?

One of the crucial treaties between the U.S. and Russia is the New START Treaty which is set to expire soon. There are three possible options of what could happen with the agreement. The U.S. is still on the fence, and President Trump reportedly will not decide before next year.

First, it could expire in February 2021 without extension and without replacement, after which we will no longer have a bilateral strategic arms control treaty between Moscow and Washington for the first time in decades.

The second option, publicly supported by the Russian government, would be for the two presidents to extend the Treaty by up to five years, as provided by the protocol. Such a decision will be easy for the U.S., as the approval of Congress is not required. Russian officials say that they have to go back to the Duma for approval, which could take as much as six months. Still, President Putin could presumably push for rapid action on the grounds of national security.

The third option is to develop something better. The problem with the New START Treaty is that it limits just Russia and the U.S., though Kazakhstan, Belarus and Ukraine are technically included as they inherited some of the Soviet arsenals. In the past, the Russian government said that other (nuclear weapons states) should participate in these treaties.

The New START Treaty, like its earlier versions, focuses on long-range nuclear arm missiles and bombers. A new type of strategic arms control treaty could limit additional types of weapons, such as short-range missiles and non-nuclear weapons that could potentially cause significant damage. Russia has always pushed to include strategic missile defences in these strategic arms control treaties, while U.S. officials have pressed to include so-called tactical nuclear weapons, amongst other areas, but both sides would abandon these positions in the course of the talks.

President Trump would prefer this — to get a new treaty that would include additional systems and countries, especially China. The problem is that time is limited. According to the official position of the Russian Foreign Ministry, there is no longer enough time for Russia to negotiate a new treaty before the New START expires. Therefore many experts would want to extend the New START Treaty for at least a few more years to give us sufficient time to develop a more comprehensive agreement.

What instruments could one use to encourage China to join international agreements regulating arms control?

Getting China involved in nuclear arms limitations is difficult. China, of course, has always been involved in the more extensive nuclear negotiations in recent decades: it has joined the Non-Proliferation Treaty (NPT). Unlike the U.S. and Russia, China has a No First Use (NFU) doctrine, saying the PLA will never use nuclear weapons first. Chinese officials say that they are uninterested in joining Russian-US agreements like INF and New START since they have fewer nuclear weapons than Russia or the U.S. They also claim, not very credibly, that their weapons do not threaten other countries. A more recent argument one hears in Beijing is that it's impractical and too complex to enlarge these treaties. The Chinese also accuse the U.S. of trying to shift the blame for the collapse of arms control on China.

Nonetheless, even if New START is extended, strategic arms control will die unless China is involved in these treaties. The U.S. Senate is hardly likely to ratify another such treaty without some limits on China’s arsenal. And I think it is possible China would join; we have seen China changing its policy on other major military issues, such as acquiring aircraft carriers, for example. They now have de facto foreign bases. And it seems to me that since China is stronger militarily than it was in the past, which should make them more comfortable with greater transparency. It won't be in China's benefit if we have an unconstrained arms race in the case of the collapse of all these treaties because China refused to join.

The U.S. continues trying to persuade the Chinese to join international agreements, yet they resist. So I am hopeful our Russian colleagues will join the process and help to educate the Chinese about some of the benefits they could get from joining the process – reducing the risk of war, potential misperceptions and so on.