SSQ
STRATEGIC STUDIES QUARTERLY

WINTER 2017 VOL 11, NO. 4

STRATEGIC STUDIES QUARTERLY • WINTER 2017

AUP

SSQ Strategic Studies Quarterly

Strategic Studies Quarterly

An Air Force–Sponsored Strategic Forum on
National and International Security

WINTER 2017 VOLUME 11, NO. 4

Policy Forum

Feature Article

Perspectives

Book Review

On US Nuclear Deterrence

Many Americans and some in the US military will never have the opportunity to be educated on the nuclear deterrent—will not ever find time to ponder why we have it or to understand what its utility is today and in the future. However, understanding the essence of nuclear deterrence is important regardless of one's military service, branch, or career field because nuclear weapons are the ultimate guarantor of US military power and security, and understanding how they fulfill this role should be fundamental to any practitioner of the profession of arms.

Unfortunately, since the end of the Cold War, along with the dramatic reduction in the US nuclear weapons stockpile, the deterioration of the infrastructure to support the remaining stockpile, and the aging of the delivery systems that constitute the triad, there has been a dearth of attention paid to the rationale for the nuclear deterrent. The underlying principles and rationale for the deterrent have not gone away, but we have stopped educating, thinking, and debating, with informed underpinnings, the necessity and role of the US nuclear deterrent in today's world. Even more concerning has been the lack of informed debate on the subject. We have raised three generations of Air Force officers who may not have been exposed to the most fundamental and yet relevant arguments surrounding deterrence from the late nuclear theorists Herman Kahn and Thomas Schelling.

When you stop thinking about something, typically what follows is you stop investing in it. When you stop investing in it, the people expected to perform the mission lose focus, morale declines, and some bad things can happen, such as the unintentional movement of nuclear weapons from Minot Air Force Base to Barksdale Air Force Base in 2007. It is hard to imagine that the series of failures that led up to this event could ever have happened during the Cold War given the intense focus the Air Force had on the nuclear mission. But, as a former commander of Strategic Air Command observed when referring to this incident, the unintentional movement was probably the best thing that could have happened to the US nuclear deterrent. Nobody died, nobody got hurt, and control of the weapons was maintained, but the incident provided a much-needed wake-up call that we had stopped paying attention to something still very relevant and still very important to the defense of the United States and the stability of the world.

Of course, context matters. The collapse of the Soviet Union and the confident expectation of a new relationship with Russia dominated in the 1990s. The context post-9/11 further contributed to the lack of attention. Our focus changed to terrorism, and it remains a concern today. Seven years later in 2008, a foundational strategy document, the *Joint Operations Environment* (*JOE*), was drafted to assess the environment in which our military could be expected to operate in the future and to posit the highest priority threats our military would face. The number one threat at the top of the draft version of the *JOE* was the detonation of a nuclear device by a terrorist organization in one or two cities in the United States. Certainly, if a 10-kiloton weapon exploded in Central Park or Times Square it would be a god-awful day for the United States and certainly a terrible day for the citizens of New York City. But the nation would survive. But if Russia or China were to unleash its nuclear arsenal on the United States—something each is certainly capable of doing—it would be the end of the United States. These existential threats to our very existence as a nation should remain and do remain the number one threats to the United States.

Skeptics may ask, what are the odds of that happening? The point is no one knows for sure. But thinking about this event and devising ways to prevent or minimize its likelihood is the job of the US military. For "red-zone" events on the classic risk matrix, particularly those with low probability but extremely high consequence, the nation expects the military to pay attention and not simply assume away the risk. When a military capability exists that threatens national survival it is not the role of the military to weigh the odds of its use. History has taught us that when a military capability exists, the will to use it can change in very short order—unless the decision maker is effectively deterred.

Recently, we have seen some change in US thinking. The 2016 version of the *JOE* strategy document mentions the importance of nuclear deterrence several times and the possibility that nuclear weapons could proliferate and maybe even be used in the coming years up to 2035. This change within the *JOE* reflects progress in our nuclear focus and thinking.

Deterrence Defined

To deter is defined as to turn aside, discourage, or prevent someone from acting. Key is the notion that someone or some decision body can be influenced by the actions of another. In the context of nuclear

deterrence the intent is to cause a decision maker (or decision makers) to refrain from certain acts, under certain circumstances, out of fear that if they take those actions they will fail to achieve their objectives (deterrence by denial) and/or suffer unacceptable consequences (deterrence by threat of punishment). Further, the decision maker must also believe that refraining from the specific action is the best possible choice of all of the likely miserable choices. It may not be a good choice, but in light of the threatened consequences, it must be the least worst option.

Why We Have Nuclear Weapons

Fundamentally, we have nuclear weapons to deter attack on the United States and our allies. Further, with regard to our allies, the US nuclear deterrent is meant to assure them that the United States will use its nuclear arsenal to deter adversary aggression against them as well. We offer this "nuclear umbrella" so as to strengthen our alliances and also encourage our allies to not develop their own nuclear deterrent. In essence, nuclear assurance is a fundamental and demonstrably effective part of the US nonproliferation policy.

Demonstrating Deterrence

For deterrence to be effective for national defense and assurance, the United States must possess two things: capability and will. Simply having capability is not sufficient. Both capability and the will to use it must be made believable in the mind of the adversary. Demonstrations of capability and will are essential to ensure adversaries receive a clear signal of what the United States can do and what it is willing to do.

At the end of World War II we demonstrated our capability and will emphatically over Hiroshima and Nagasaki. During the Cold War, we showed our capability by building an effective triad of delivery vehicles and conducting 1,054 nuclear tests. Of those, 219 tests were detonated above ground or in shallow water so there was a visible effect—like the sinking of ships or the destruction of military equipment. These visible signs certainly painted a clear picture of US capabilities for the Soviet Union. There was also a demonstration of US will in some of these tests. Indeed, some tests and their frequency were as much a part of signaling our will as they were of testing new weapon designs.

Today the United States and Russia demonstrate capability with tests of their delivery systems. US intercontinental ballistic missiles launch from Vandenberg Air Force Base, California, and from submarines impacting in the Kwajalein atoll. The Russians launch both their sea-based and land-based missiles from west to east across Siberia, impacting in Kamchatka. The Russians further demonstrate the bomber leg of their triad by flying nuclear cruise missile–capable bombers near Alaska and off the east and west coast of the US mainland.

Contributing to the earlier discussed reduction in focus, between 1992 and 2008 the United States allowed the bomber leg of the triad to atrophy. Bombers had been taken off constant alert at the end of the Cold War, and though the United States claimed to retain the capability, it rarely demonstrated it and hence put in question this leg of our triad's credibility. In fact, by 2008 US Strategic Command devolved to conducting only command-post exercises for the nuclear war plan. While these exercises were useful training for the command-and-control element of the deterrent, they did not produce the kind of signaling required for deterrence, nor did they ever explicitly demonstrate capability. Beginning in 2009, field-training exercises (FTX) were reinstituted. These training events visibly exercise the critical elements of the bomber leg, to include the generation of tankers, bombers, aircrew, maintenance personnel, security forces, and weapons load crews to alert status; the uploading of nuclear weapons; and the scramble launching of the bombers and tankers to conduct simulated nuclear missions and their recovery to dispersed locations. In addition, the nuclear command-and-control aircraft also participate and exercise their wartime mission. An FTX demonstrates capability and will while signaling the credibility of the nuclear force to those we want to deter. It is intentionally made visible to China and Russia to create the awareness that is fundamental to deterrence.

Stanley Kubrick's satirical Cold War movie, *Dr. Strangelove*, illustrates this point. Good satirical comedy is most effective when it contains a thread of truth, and in this case the truth Kubrick's screenwriters likely called upon came from the writings of Schelling and Kahn, the two great nuclear deterrence theorists of the day. At the end of the movie, after one nuclear bomb detonates on the Soviet Union, the Russian ambassador says this is a terrible thing. Of course the US president agrees. But the Russian ambassador then reveals the existence of a

secret automated doomsday system that will now instantly launch the entire Soviet arsenal against the United States. Peter Sellers, acting as the president, replies, "Mr. Ambassador, you know, of course, that the whole point of a doomsday machine is lost if you keep it a secret!"

One can signal will through tests and exercises—and also through rhetoric. Nikita Khrushchev used rhetoric when addressing the United States at the United Nations when he said, "We will bury you." John Kennedy made rhetorical statements during the Cuban missile crisis when he declared a launch of a nuclear missile from Cuba against any target in the Western Hemisphere would be met with a full retaliatory response of the United States against the Soviet Union. That is a very strong redline and a way of signaling will. Consider Kim Jung Un and his "sea of fire" comments. Kim uses rhetoric to signal his willingness to cross certain thresholds, whether they be chemical, biological, or nuclear. A few years ago the United States announced a redline in Syria with the intent of deterring Bashar al-Assad from using chemical weapons in his civil war. But the declaration of redlines must be carefully considered, for if one ever backs away from a declared redline the resulting injury to credibility can lead to future miscalculation on the part of adversaries and, perhaps just as importantly, can degrade the credibility of our assurances to allies.

Could the "Unthinkable" Happen?

Between the United States and Russia the credibility of each respective deterrent force is well understood. Both face an existential threat to this day, which is held at bay by similar stakes and risks. The strategic nuclear relationship is stable because there is no huge imbalance in strategic forces, nor is there a particular vulnerability either side has that would invite the other to strike first. This is the essence of strategic stability. Consequently, there is not a single day that our adversaries wake up and calculate that it would be a good day to launch a nuclear attack on the United States or its allies.

However, a change in Russia's declaratory nuclear policy in the past few years may in fact reflect a lowered threshold for the first use of a nuclear weapon in an otherwise conventional theater conflict for the first time since the Cold War. Russia's new declaratory policy is to threaten to escalate to limited nuclear use to coerce Western capitulation in a conventional conflict they see as not going in their favor and to actually

launch limited nuclear strikes for this reason if necessary. The Russians may have always thought this way, but now they have declared it. This expectation of advantage from coercive nuclear threats or use could potentially lead to future miscalculation on the part of the Russians about how the United States might respond.

Russian President Putin has boasted that he could have Russian troops in five NATO capitals in two days. So, here is a hypothetical miscalculation: After early success in a conflict initiated by invading Russian forces against NATO forces in the Baltic states, the Russians find themselves on the defensive and in retreat. It would seem reasonable that they would consider using the low-yield battlefield nuclear weapons that they are currently fielding to stand firm in their declaratory policy of "escalate to de-escalate," in the belief that the United States would not respond with higher collateral-damage nuclear weapons because it no longer has similar low-yield weapons in its inventory. But this is precisely what the United States might feel it has to do to preserve the long-term credibility of the nuclear deterrent and commitment to the alliance. Clearly we must address the potential for such Russian miscalculation.

Unlike Russia, China has declared a no-first-use policy. But if read carefully, the policy is rife with caveats and exceptions that suggest in a losing position in a conventional fight they too would consider nuclear first use. History teaches that various dynasties throughout China's history have typically collapsed not from external invasion but from internal revolt. It would stand to reason given China's current military power and its weaker neighbors (arguably with the exception of Russia), the most likely threat to the sustainment of the current dynasty (the Communist Party) is from internal revolt. In most of the last century, the unifying factor in post–World War II China was Communist ideology and the deified figure of Mao Tse-tung. Today, no one in China wears Mao suits or carries his little red book. Today, there appears to be a fervent rise in nationalism encouraged by the Communist Party. The party is not deified. Instead, pride in the party's promise ("We are back—150 years of shame are behind us. We are a great power and a great nation. We not only deserve but demand and command respect") may be the underpinning of the Communist Party's legitimacy. So here is another hypothetical miscalculation: one could envision that if China were to find itself in a conflict with the United States in a fight over the South China Sea, it would consider crossing the nuclear threshold to prevent defeat and the

prospect of being "dethroned" by its own populace should the Potemkin village of its promises be realized. And, further, might they calculate (or miscalculate) that the United States would not dare cross the threshold in response out of fear of a Chinese nuclear attack on the US mainland?

To be sure, these are hypotheticals, but as soon as one starts talking about first use in localized theater conventional conflicts (and both Russia and China have), it demands that we not only start thinking and war-gaming these types of scenarios but also that we closely examine our current nuclear force structure and ask ourselves if we have the right equipment to first deter and second to present appropriate response options to the US president.

North Korea and the Nuclear Imbalance

As discussed, Russia, China, and the United States have similar stakes in the nuclear game. But with North Korea there is an imbalance. North Korea has all its chips on the table while we do not, because we hold an existential threat over it and it does not hold one over us. This imbalance in the stakes is a new twist to the nuclear deterrence calculus of the past 70 years. It is important to analyze the impact of this imbalance in stakes because it is possible that the threshold for first use is different when an imbalance exists.

During the Cold War we targeted a lot of things in the Soviet Union mostly because we did not know with absolute certainty what they feared or valued most. As a result, we considered the matter broadly and held five different target sets at risk and assumed the Soviets had to fear at least three or four of those sets. While we did not deliberately target population centers, there were targets close to population centers, the destruction of which would certainly have caused a lot of civilian casualties. The strategy was not a so-called minimal deterrent—just have the minimum capability to threaten to destroy all of their cities—because we were not sure Stalin or Mao even cared about their people. After all, Stalin killed 25 million of his own people after World War II and is quoted as saying the death of a human being is a tragedy but the death of 25 million humans is a statistic. Mao Tse-tung said he did not need a lot of nuclear weapons to deter the United States: "If I kill 300 million of them and they kill 300 million of us I still have a billion people and they have nothing."

The imbalance of stakes in North Korea could, ironically, lead Kim Jong Un (another tyrant who has shown little concern for his own populace) to nuclear first use. Recalling the fates of Saddam Hussein and Mu'ammar Gaddhafi and the likely endgame for himself in a lost conventional fight, he might conclude he has nothing more to lose by crossing the nuclear threshold in a conventional fight on the Korean peninsula. Presented in nuclear deterrence terms, in spite of the US existential threat, Kim could decide using a nuclear weapon may not be his personal least worst option. In that regard, how much have we thought recently about entering a nuclear battlefield and operating in a nuclear environment? We did this during the Cold War. In current circumstances, we need to be thinking again about what the fights of the future are going to be like if someone detonates a nuclear weapon on a future battlefield.

Assuring Allies

When considering the assurance element of our nuclear deterrent policy it is important to remember that the United States does not get to decide if our allies are assured—they do. We cannot make them assured; they decide if our assurance is credible. The United States learned this lesson in 2010. For budgetary reasons the US Navy wanted to retire the nuclear-tipped Tomahawk land attack cruise missile (TLAM/N) carried on attack submarines in the Western Pacific. Apparently unbeknownst to our allies, this weapon had been taken off the subs and stored ashore for quite a while, and it was going to cost the US Navy a lot of money to get them refurbished and recertified for use. From the Navy perspective the missile was not being used and was expensive to redeploy. From the policy perspective the Obama administration wanted to de-emphasize our reliance on nuclear weapons, and eliminating this class of weapons seemed like a great way to show the world we were serious about decreasing our arsenal. We announced the decision to eliminate the TLAM/N in the 2010 Nuclear Posture Review without consulting the Japanese or the South Koreans. The Japanese objected strenuously, and the United States was puzzled by the reaction to what seemed to be a logical decision. The Japanese objected because they believed the TLAM/N, with its forward presence in the Western Pacific, was the only credible deterrent to the Chinese and the Russians. They questioned the credibility of a US deterrent based only on the US threat of launching an intercontinental

ballistic missile from either our ICBM fields or *Ohio*-class submarines to come to their defense. They did not think the Chinese or the Russians would adequately believe such threats. Instead, they feared such a method of attack could invite a retaliatory attack on the US mainland and they did not believe the United States would be willing to "trade Seattle for Tokyo." In sum, the elimination of TLAM/N undermined our assurance of Japan. What had assured them was a nuclear capability that had a smaller yield than an ICBM, which could be deployed from in theater, for an in-theater scenario, and that would have the possibility of not presenting a threat to major cities of the combatants involved but instead could be used in a tactically credible manner. The Japanese believed the threat of the United States using TLAM/Ns provided a credible deterrent of an attack on them. Furthermore, they believed the Chinese and Russians felt the same way.

To rebuild assurance the United States successfully persuaded Japan that the bomber leg of the triad could be deployed in theater and was flexible enough to deliver capabilities similar to the TLAM/N, for example, air-launched cruise missiles (ALCM) and/or gravity bombs. Subsequent deployments of elements of the bomber leg to Guam have served to reassure the Japanese and the South Koreans. Indeed, when bomber training missions are flown over the Korean peninsula or in the Western Pacific they serve two purposes: to deter North Korean aggression and, just as importantly, to assure the South Koreans and the Japanese that the US nuclear umbrella is very real and credible. Again, assurance is critical to support US alliances and US nonproliferation policy. Japan and South Korea certainly have the knowhow, tools, and materials available to field a nuclear arsenal, but the United States does not currently believe that their doing so would be in either their interests or ours.

During the 2016 presidential campaign, a candidate suggested it might be cheaper if Japan and South Korea developed their own nuclear weapons. But we must ask ourselves, would that result in a safer world? Today, several countries hang in the balance between assurance and possible proliferation. Japan, South Korea, and Taiwan are capable. They could join the nuclear club quickly if no longer assured. If Shiite Iran were to build a nuclear weapon, it is likely Sunni-dominated Saudi Arabia would respond in kind. And if Saudi Arabia went nuclear, would Turkey be interested in doing the same? Egypt? While none of these proliferation

scenarios are certain, they are possible, and it is not likely that a world with this level of proliferation would be a safer place.

In the case of assurance, we can decide that assurance is an important goal, but we cannot decide who is assured—and in some cases our assurance efforts have failed, even with friends and allies. France was not assured the United States would trade New York City for Paris and built its own nuclear deterrent. Israel could not be assured by anyone in the West and reportedly has its own unacknowledged nuclear deterrent.

Our Nuclear Deterrent Future

Unlike Russia, China, Pakistan, India, and now North Korea, the United States has uniquely and unilaterally decided not to build new nuclear weapons. We are maintaining our current stockpile, which consists of the B61 gravity bomb for the B-2 bomber and the NATO deterrent force, the W76 and W88 warheads for our submarine-launched ballistic missiles (SLBM), the W78 and W87 warheads for our ICBMs, and the W80 warhead for our cruise missiles. (Incidentally, the number represents the year they were designed. So our newest nuclear weapon is a 1988 design. The oldest is the B61 gravity bomb, a 1961 design that is now being refurbished.) This life extension is the only allowed effort to sustain our deterrent, while most every other nuclear-armed country is building new nuclear weapons and adding to inventory. Russia, for example, is not only building new strategic nuclear weapons, but it also is building and fielding new tactical/theater nuclear weapons. It is mounting and deploying nuclear warheads on surface-to-air missiles and surface-to-surface missiles such as the Iskandar, which is deployed in Eastern Europe. Moscow is adding nuclear capability atop antiballistic missiles and in torpedoes, depth charges, and cruise missiles that can be launched from airplanes and from surface ships. The Russians have also discussed the possibility of placing nuclear-armed cruise missiles on icebreakers in the Arctic with the ability to range the continental United States. In sharp contrast, with the exception of a variant of the B61, which can be delivered by only a small percentage of the Air Force fighter fleet of aircraft, the United States has eliminated all of the tactical nuclear weapon capability it fielded in the Cold War. The bottom line is, despite the Russian political pledge to do the same, we eliminated and the Russians are building up.

China, which once felt it could adequately deter the United States with 20 multi-megaton armed, silo-based ICBMs, is in the process of deploying land-mobile, nuclear-tipped ICBMs as well as multiple short- and intermediate-range missiles that are nuclear capable. In addition, the Chinese have begun deployment of a fleet of nuclear missile–armed submarines.

The development of new weapon systems and new warheads that put at risk US forces and our allies in Asia and Europe as well as the US homeland is the path China and Russia are on. Meanwhile, current US policy continues to prohibit the design and building of any new nuclear weapons.

Even if given the green light to design and build a single new type of nuclear weapon, our ability to do so is at best problematic. The infrastructure that once existed in the Cold War to design, engineer, and manufacture nuclear warheads en masse is, in the words of the bipartisan 2009 Perry-Schlesinger report on America's strategic posture, "decrepit." Even more concerning is the aging out of the human capital knowhow to design, engineer, and manufacture a new weapon. Recall our newest weapon was designed in 1988. Not many people left in the enterprise have ever built or tested a new weapon. In 10 years, they will all be gone. And in 10 years, what if the geopolitical situation in the world (think mass proliferation) should worsen? Will the United States be in a position to build new or additional weapons should a future president decide that is what is required for credible deterrence and national security? Russia will be, China will be, and even Pakistan will be, each of which today can and is building more new nuclear weapons than the United States is able to.

So, failing an investment in the reconstitution of a nuclear weapon–production enterprise as a hedge against future geopolitical uncertainty, what options does the United States have in the near term to hedge against this scenario? Or worse yet, should some technical problem render either a single class of SLBM or ICBM warhead or a missile system or submarine unusable for an extended period of time (think years), what options does the United States have to maintain effective deterrence vis-à-vis the Russians? The only answer to both scenarios is the ALCM. Because of the "bomber counting rule" in the New Start Treaty, a nuclear bomber only counts as one of the 1,550 weapons either side is allowed to field on their strategic deterrent platforms regardless of how

many bombs can be loaded on a single bomber. So a B-52 counts as one weapon even though it can carry up to 20 nuclear-armed cruise missiles. Consequently, in either of the above scenarios, the president could direct the B-52 force to return to alert status with some 400 nuclear-armed cruise missiles postured in a survivable mode, similar to a submarine at sea, within a matter of days. In fact, besides being the most cost-imposing weapon system in the triad, the ALCM is the only hedge the United States has against either a dangerous change in the geopolitical environment or a technical failure in either of the other two legs of the triad. This is the imperative for fielding the so-called long-range standoff cruise missile replacement of the aging ALCM.

Nuclear Perspective

Some planners may think the buildup of Russian tactical nuclear weapons is not particularly threatening to our conventional forces. Compared to the Hiroshima bomb at 10 kilotons and the Nagasaki weapon at approximately 16 kilotons, a nuclear artillery shell with only a one-half kiloton yield might seem inconsequential. This is where the numbers become enlightening when put into perspective. A one-half kiloton nuclear artillery shell is equivalent to 500 Mark 84, 2,000-pound bombs detonating simultaneously right next to your unit. A more recent comparison is the massive ordnance air burst (MOAB) bomb. One-half kiloton equates to 30 MOABs detonating simultaneously adjacent to your command post or your deployed force. And that half-kiloton round can be fired from 20 miles away through a 155mm equivalent artillery piece, with more likely to follow.

If deterrence were ever to fail and the nuclear threshold crossed, be it next month, next year, or in 50 years, will the United States have the right tools to offer the president to de-escalate the situation on acceptable conditions? One thing is certain: if China, Russia, or North Korea cross the threshold of first use against one of our allies, deployed US forces, or the homeland, I expect one of the first things the president would do is turn to the secretary of defense and say, "Make them stop, now!" Our response must be more flexible than to assert we can put a multi-hundred-kiloton weapon on their nation's capital in 30 minutes. The president and the nation deserve more options than that.

Conclusion

Historical evidence and reason lead me to believe that the US nuclear deterrent has successfully accomplished its purpose since 1945. In fact, nuclear weapons are the one set of military systems that have been 100 percent successful in their assigned mission. They have deterred attack on the United States and its allies, assured our allies, and, though not specifically called out in US policy, deterred major nuclear powers from engaging in global conventional warfare on the scale we witnessed in the first half of the last century. However, there is no evidence that our self-imposed policies and constraints have constrained any other nuclear-armed or nuclear-aspiring power. Simple prudence now demands that we take steps necessary to ensure the continued health of our current nuclear deterrent. We must recapitalize all elements of the triad and make the appropriate investments in the Department of Energy infrastructure and human capital to ensure that presidents in 10, 20, 30, 40 years and beyond have the necessary tools at hand to effectively deter against all existential threats. SSQ

Gen Kevin P. Chilton, USAF, Retired
Former commander, US Strategic Command

Highlighting Artificial Intelligence: An Interview with Paul Scharre

Director, Technology and National Security Program Center for a New American Security

Conducted 26 September 2017

SSQ: What is the best way to prepare for an artificial intelligence future?

Mr. Scharre: People have been talking about AI for decades and there have been cycles of excitement, hype, and disappointment. We are in a period right now of intense excitement and progress. In just the last five years we've seen several things emerge. The first is big data that can be used to train learning machines. That combines with more powerful computer processing capabilities that can be used for parallel computations for deep neural networks. And finally there have been advances in the algorithms. All of this has come together to enable machine learning, often using deep neural networks, that can make machines very effective at solving a variety of problems. We are seeing this technology being applied to a whole range of industries including finance and transportation, and there are many national security applications as well. The best way to think about AI is not as a discrete kind of technology, like you might think of hypersonics, but something that is more like a basic enabling technology like electricity. Kevin Kelly, editor of *Wired* magazine, has suggested that just as electricity empowered and enlivened all sorts of objects, AI will similarly cognitize objects making them more intelligent and useful. Now, there are limitations to AI today. It is very narrow—domain specific—and does not have the kind of general-purpose reasoning capability that humans do or the kinds of scary AI one sees in science fiction. But even still, AI today is a very powerful technology. Many people compare it to a new industrial revolution in its capacity to change things. It is poised to change not only the way we think about productivity but also elements of national power. Just as past industrial revolutions transferred power to the more industrialized nations,

AI will do something similar. But those elements of national power and advantage may look different. What is it that gives an actor a competitive advantage, whether a corporation or government? Is it better data, better algorithms, human capital, technology, or the right ideas for implementing them? The first-order questions we should be thinking about are: what is this technology, what is the essence of what is occurring, and how do we think about strategic advantage? What will position the United States for strategic advantage, and how do we maintain it? With all the disruption AI brings there is great opportunity and also a lot of risk, particularly for a nation like the United States that is heavily invested in the current way of doing things. We spend quite a bit of money each year on defense and national security programs and so far we don't rely on AI to any great extent. So how do we need to shift what we are doing as a result of AI?

SSQ: A recent study predicted that by 2025 over 70 billion objects would be network enabled. Should we be rethinking the internet of things?

Mr. Scharre: The trends in the internet of things are new and are happening out of anyone's control. The proliferation of the internet of things is going to force us to rethink elements of the internet and connectivity from a standpoint of cybersecurity and personal security. We need to better prepare for the world that is coming. William Gibson, the science fiction writer who coined the term cyberspace, has said: "Cyberspace, not so long ago, was a specific elsewhere, one we visited periodically, peering into it from the familiar physical world. Now cyberspace has everted. Turned itself inside out. Colonized the physical." In many ways, cyberspace is not a place but rather a layer on top of our existing reality. So through our various connected devices, whether in our pockets or our cars, we are now able to connect with others around the world. The trend is toward more internet connections and more devices whether in our homes or as wearable devices. There are a number of challenges that come with this trend. The baseline challenge for these devices is that the cybersecurity for these devices is incredibly poor. We tend to rush these devices to market even if they contain many vulnerabilities. Then we try to close the vulnerabilities later after deploying them and think about security as the last step. Many of these devices are very insecure, and the effect is not only that people can hack the devices in your home to spy on you but also that these devices can be leveraged as part of bot nets for things such as DDOS [distributed denial of

service] attacks. The Mirai bot net in 2016 is one example. So this is a major problem. Societies need to reevaluate their views on cybersecurity as a whole and in particular the risks to their personal security that come with these devices. One of my favorite hacks came from an episode of the TV show "South Park." The scenario used a character talking to "Alexa" [the virtual assistant AI from Amazon] during the show commanding Alexa to do things. Now if you had one of these devices in your home, it would respond to the television program rather than you. Again, the risk comes from someone being able to reach into your home via the network or some other method. So the internet of things is an interesting challenge. But most people who are buying these devices do not know how secure or insecure these objects are since there is no way for a consumer to know this. So these limitations create a big challenge.

SSQ: Are the risks of AI overblown, or do we have reason to be concerned?

Mr. Scharre: It depends on the kind of risks we are talking about. With any type of new technology there is going to be risk associated with implementation. Because we don't always understand the capabilities of the technology, we miss some of the risks involved and many of the unresolved safety concerns. For instance, consider electricity. It's not going to rise up and kill us all, but if one is careless, it can be dangerous and life threatening. We have learned the safety protocols of electricity, such as grounding and other precautions. Now we need to do the same with AI. We also need to think about people intentionally using AI for malicious purposes—something that is inevitable. State and non-state actors are going to use AI for nefarious ends and we must be prepared for this. Given the safety risks and vulnerabilities, we also need to be worried about AI systems that might be exploited or manipulated in some way. Current generation AI systems have safety problems that are not yet solved. These are also very serious concerns some experts have raised not about today's systems but more about the long-term implications. If AI systems become more intelligent, particularly if they develop in the direction of a general-purpose learning ability—which doesn't exist today—then this would raise significant long-term safety questions.

SSQ: As artificial intelligence becomes more ubiquitous and more powerful, should the United States attempt to control AI by enhancing human intellect through gene manipulation?

Mr. Scharre: This is a great question. Let me reframe the issue just a bit. During the first industrial revolution, we were able to create machines that were much stronger than human beings to perform various kinds of tasks. We are now creating machines that are smarter than humans—if the task is narrow enough and we have enough data to support it. So it seems as if for many applications we will be able to leverage machines in very specific ways. In many cases, even if machines are not qualitatively as smart as humans in making the best quality decisions, machines are faster than humans and can be employed cheaply and at scale, which is a great advantage. We have seen this kind of application in stock trading where the speed advantage emerges. We have seen this in Twitter bots where the advantage of scale would not be possible if you were trying to use a million people to replicate content. At the same time, the best general-purpose learning system on the planet is the human brain in terms of quality, robustness, perception, flexibility, and responding to novelty. This is unlikely to change any time soon. While it's possible there may be something in AI that changes this, it does not appear likely in the near future. Given these limitations, we should be thinking about the best way to blend intelligence—human cognition and machine learning working together. One challenge is going to be how we avoid making it more difficult for humans to stay engaged as the speed of action increases due to automation. It doesn't matter that humans make better qualitative decisions for stock trading and are more cognizant of manipulation; you simply cannot compete at the speed of automated stock-trading algorithms. There is potential for using AI and automation in warfare or national security applications, particularly in domains that are native to machines, such as the electromagnetic spectrum or cyberspace. In this type of world, how do humans cope with an environment where we may be approaching a battle for singularity, where the pace of battle becomes so fast that humans are not able to comprehend what is happening and react to events fast enough? We have some narrow settings in the military today where this already is the case, for instance with missile defense systems operating in automatic mode. The domain in which humans can no longer react fast enough is expanding over time. There are certainly risks when automating. Machines today are very brittle and do not have the common sense we expect from humans or the ability to understand context. This limits the machine's ability to recognize errors and stop if it malfunctions. So we might want

to also think about how to increase human performance directly. Today there are many ways to enhance human performance through medicine—for instance, drugs such as Modafinil and Adderall to increase stamina, alertness, or concentration. The military is conducting some interesting studies in this area by using some of these drugs—mostly in aviation—but adoption is extremely slow in the military overall. This is the case even though the new drugs are better than the ones the military is currently using. For example, we give dextroamphetamine to pilots and caffeine of course to all sorts of troops in an unregulated fashion. But studies have shown that Modafinil is more effective at enhancing cognitive performance with fewer side effects than dextroamphetamine or caffeine. We should be looking at ways to enhance human performance, including genetics that we may see happening in the coming decades. Now anything that alters humans directly raises a host of serious legal, ethical, and social issues, and I don't want to dismiss them. We need to be careful to ensure that we're not exposing our troops to potentially harmful treatments. But we also don't want to miss out on an opportunity to enhance their performance and potentially save lives. The way to deal with this challenge is to confront these issues directly and work through them. There are things we could be doing with technologies that are well understood, effective, and reasonably safe that we are not doing because so far we have not been willing to grapple with these question in the military.

SSQ: Some people claim the US will "never" use autonomous lethal military systems. Is this realistic?

Mr. Scharre: The Pentagon is taking a cautious, hedging approach to autonomous weapons. The official policy, which I was involved in while working for DOD, approves certain things that we are already doing, such as autonomous missile defense systems. The policy then also creates a new process for approving new technology if people want to use autonomy in a novel way that's never been done before in weapon systems. So now there is a process for stakeholders to come together and evaluate ideas before adopting new uses of autonomy in weapons. When former Deputy Secretary of Defense Bob Work was at the Pentagon, he spoke about this and in essence stated we are not planning to use lethal autonomous weapons but if others do, we might have to. Air Force Gen Paul Selva has spoken on this a number of times and has said he feels it

is essential to keep humans responsible for using lethal force. This raises a slightly different question: how do we think about accountability and responsibility? One of the challenges here is making a clear, bright line. Look at the example of self-driving cars. In theory, there is a clear difference between a car driven by a human and a car driven by a machine autonomously. But what we see in practice is creeping autonomy in a wide range of functions, such as intelligent cruise control, automatic collision avoidance, automatic lane keeping, and automatic parking. We are seeing a slow shift in various functions to the machine. The human is still sort of responsible for driving, but what we mean by "driving" begins to change over time and it starts to look a lot more like what we see in commercial airlines. The plane can basically fly itself and the pilot is there in case of an emergency and in some cases to be a scapegoat if something goes wrong. As automation continues to creep forward, how does this change the role of the human, and how do we ensure the human is ultimately responsible for what happens on the battlefield?

SSQ: What is the most futuristic AI technology we will see in the next 20 years? And the next 100 years?

Mr. Scharre: What we are likely to see in the next 20 years, given current advances in AI, is implementation of various narrow AI capabilities. I suspect we are likely to be surprised by how capable some of these applications might be but also how brittle they are. Consider DeepMind's program AlphaGo that learned to play the game of Go. Many people thought this application would take much longer to perfect than it actually did. Additionally, the system defeated its human Go adversary quite handily. So one of the effects we see is, often AI capabilities seem very distant but then, seemingly overnight, AI moves from not very good to much better than the best human player. Another aspect I think we are likely to see in the next two decades is the surprise factor—how machines can learn in novel ways. Sometimes these surprises are good, sometimes not so good. My favorite example is a bot that was learning to play the game of Tetris learned to pause the game right before the last brick fell so it would never lose. That was allowed according to its programming, but probably not what the designers meant it to do. Brittleness is another important attribute of AI and something we will have to grapple with as these technologies are implemented in various applications. AlphaGo learned to play on a standard 19-by-19-inch Go board and is better

than any human at playing that game, but its intelligence is very narrow. AlphaGo cannot transfer its experience in playing to give it a leg up on learning how to play chess or checkers. It can't even play Go very well on a differently sized board. This is very different from a human player who can take concepts from one game and apply them somewhere else. So the systems will remain very brittle—being very powerful, but in an instant becoming very dumb.

In the longer term over the next century, I think it is very likely we will have systems that can overcome some of the weaknesses of AI systems today. One of these areas is the ability to transfer learning from one task to another. AI will be able to learn over multiple domains. The future will move from today's narrow learning systems to wider, general-purpose learning systems. Many will ask the question: when will AI reach human-level intelligence? But this is the wrong question. Why would we assume humans are the benchmark for intelligence? Why would we assume machines will evolve intelligence in the same way as humans? Humans today can still do things machines cannot do. But in the future we are more likely to see machines that have general-purpose abilities and manifest them in ways very different from today. One hundred years from now, I suspect people will continue to say, machines are very smart but they are not smart like people. This is only because we increasingly narrow down the things that make us uniquely human. We are likely to see very powerful general-purpose systems and that will create a range of tricky problems as we develop AI.

SSQ: Mr. Scharre, on behalf of Team *SSQ*, thank you for sharing your views on artificial intelligence with the *SSQ* audience and for peering into a future we hope will produce great promise for mankind. SSQ

For More Information

Scharre recommends the following links for those interested in learning more about artificial intelligence:

- https://www.wired.com/2014/10/future-of-artificial-intelligence/
- https://www.cnas.org/publications/reports/patriot-wars
- https://www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future/

- https://arxiv.org/pdf/1606.06565.pdf
- http://nautil.us/issue/40/learning/is-artificial-intelligence-permanently-inscrutable
- http://nautil.us/issue/27/dark-matter/artificial-intelligence-is-already-weirdly-inhuman
- http://www.evolvingai.org/fooling

China's Institutional Challenges to the International Order

Huiyun Feng
Kai He

Abstract

This article examines one critical but understudied question: *how* does China challenge the international order through multilateral institutions? By integrating institutional balancing theory in international relations (IR) and prospect theory in behavioral psychology, this article introduces a "prospect-institutional balancing" model to explain how China has utilized two types of institutional balancing strategies to challenge the US-led international order. We argue that China is more likely to use inclusive institutional balancing to challenge the United States in an area where it has a relatively advantageous status, such as the economic and trade arena. When China faces a security challenge with disadvantageous prospects, it is more likely to take risks to conduct exclusive institutional balancing against the United States. Using China's policy choices in the Asian-Pacific Economic Cooperation (APEC) and the Conference on Interaction and Confidence-Building Measures in Asia (CICA) as two case studies, the project tests the validity of the "prospect-institutional balancing" model.[1] It concludes that China's institutional challenge to the international order will be more peaceful than widely predicted.

✳ ✳ ✳ ✳ ✳

Huiyun Feng is a senior lecturer in the School of Government and International Relations at Griffith University in Brisbane, Australia.

Kai He is a professor of international relations in the Griffith Asia Institute and Centre for Governance and Public Policy at Griffith University in Brisbane, Australia.

This project is supported by the Korea Foundation, the Australian Research Council (project no. FT160100355), and the MacArthur Foundation (grant no. 16-1512-150509-IPS).

The rise of China is one of the most dynamic political events in world politics in the twenty-first century. Scholars and policy analysts have debated China's challenges to the international order as well as the implications for world politics. One critical but understudied question is *how* China challenges the international order. If China uses military means to overthrow the system (as power transition theory might expect) as Germany and Japan did in WWII, then military conflicts between China and the United States will be unavoidable. However, if China relies on multilateral institutions and institutional balancing strategies to challenge the international order, a peaceful power transition in the international system will become probable.

Borrowing insights from institutional balancing theory and prospect theory helps examine China's two institutional balancing approaches in challenging the US-led international order. This suggests that China is more likely to use *inclusive* institutional balancing—that is, to join and reform the rules and norms of existing institutions to maximize its economic gains in the liberal economic order. When facing security pressures and threats from US alliance-based bilateralism—the major feature of the security order—China is more likely to adopt *exclusive* institutional balancing, for example establishing and strengthening non–US-involved multilateralism, to minimize its potential losses in the security arena.

This article proceeds in four parts. First, by critically examining the "China debate" it argues that the current debate oversimplifies the dynamics of the international order and overemphasizes China's threats. How China challenges the international order is the key to examining the consequences of the rise of China. Second, integrating prospect theory with institutional balancing theory creates a "prospect-institutional balancing" model to explain how China copes with challenges and threats in the two components of the international order: the economic sub-order and the security sub-order. Third, the article provides case studies to examine China's inclusive institutional balancing through advocating the Free Trade Area of the Asia-Pacific (FTAAP) at the APEC as well as its exclusive institutional balancing through promoting the "New Asian Security" concept at the CICA. The conclusion suggests that although China's challenges to the international order will be inevitable, the outcome of the institutional balancing may be more peaceful than widely predicted.

China's Rise and the Dynamics of the International Order

Scholars have debated China's rise and its implications for the international order since the 1990s. Most realists, especially offensive realists and power transition theorists, are pessimistic about China's rise in the international order because a rising power, by definition, is revisionist in nature, which aims to overthrow the existing international order. On the contrary, liberals optimistically argue that China will be a status quo power because China has benefited significantly from the current international order, which it should sustain rather than overturn. The uncertain constructivist school focuses on the role of ideas and norms of the existing international order in shaping China's foreign policy. It suggests that China's future is still unwritten, because ideas and norms in the international order are easy to interpret but hard to predict. While all three schools of thought have valid arguments in certain aspects, they suffer two analytical weaknesses: a static and holistic view of the international order and insufficient attention to China's different strategies in challenging the international order.[2]

Realism: China Is a Revisionist Power

To a certain extent, different stripes of realism share a common argument about threats or potential threats of a rising China to the existing international order, although they disagree on the level of China's challenges as well as how to deal with China. For example, John Mearsheimer's offensive realism suggests that as a rising power, China will do what the United States did in the nineteenth century: pursue regional hegemony in its own hemisphere.[3] This revisionist behavior will be inevitably at odds with US hegemony—the essence of the existing international order. Therefore, Mearsheimer concludes that the rise of China will be "unpeaceful" and the United States will do anything to constrain, contain, and slow down China's rise.[4] Mearsheimer's argument is shared by power-transition theorists who suggest that the power transition in the international system is likely to end up with military conflicts and war between a rising power and the hegemon.[5]

Although defensive realists believe states are pursuing security instead of power in the international system, they are also pessimistic about the consequence of China's rise, US decline, and the transformation of the international system.[6] For example, as Christopher Layne points out, the emerging multipolarity caused by China's rise will be a nightmare for

US policymakers who still live in the unipolar illusion.[7] However, some defensive realists believe China will rise eventually, but its challenges and threats to the United States will still be limited over a relatively long time, especially in the military domain.[8] The policy recommendation of defensive realists is an offshore balancing strategy.[9] It means that the United States should gradually withdraw its security commitments and avoid a direct power competition with China in the Asia Pacific. Moreover, the United States should encourage other Asian countries, such as Japan, South Korea, and India, to balance rising threats from China.

Most realists label China as a revisionist state regarding the existing international order. China's "assertive diplomacy" since 2009 and the US "pivot toward Asia" during Obama's second term can be seen as an inevitable power struggle and competition between a revisionist power and the status-quo hegemon, as many realists have predicted.[10]

Liberalism: China Is a Beneficiary of the Existing Order

Most liberals have an optimistic view of China's rise for two reasons. First, economic liberalism suggests that economic interdependence can make war costly for all countries and therefore will alleviate the intensity of strategic competition between the United States and China.[11] Next, institutional liberalism argues that China has benefited tremendously from the current international order after the Cold War, and therefore the stakes are too high for China to overthrow the system. In IR theorist G. John Ikenberry's words, the Western liberal order is easy to join but hard to overturn.[12] Although the United States might lose its hegemon status in the future multipolar world, it can still play a leadership role in the Western order.[13] In other words, the Western order built by the United States after World War II may not be able to stop China's rise, but it will shape and constrain its behavior. Therefore, most liberals advocate an engagement policy toward China so that China will be further integrated, enmeshed, and entangled by international rules and institutions.[14]

China's "charm offensive" in the 1990s and "peaceful rise" pledge in the early 2000s seem to support the "status quo" foreign policy suggested by liberals.[15] China strengthened its economic ties with the United States and joined the World Trade Organization in 2001.[16] China also alleviated regional suspicions toward its economic and military ascent by actively participating in regional multilateral institutions and strengthening confidence-building measures.[17] However, as mentioned above,

China's assertive turn in diplomacy after 2009 has cast a deep-seated doubt about the liberal optimism regarding China's rise. One remaining question is whether liberals are totally wrong. In other words, has China really decided to give up all the benefits from economic interdependence and the existing international order?

Constructivism: Socialize China into the Existing Order

Constructivists highlight the role of norms, culture, and ideas in constituting state behavior.[18] Although they agree that China's rise is a challenge to the international order, they suggest that the prevailing norms, culture, and ideas can socialize China's behavior to make it fit with the existing international order. For example, East Asia international relations expert Alastair Iain Johnston suggests that Chinese foreign policy elites have been socialized by cooperative security norms and rules through participating in multilateral institutions since the Cold War.[19] This socialization effect in turn allowed Chinese foreign policy elites to educate their leaders about what China should do in the international system and directly contributed to the cooperative direction of China's foreign policy in the post–Cold War era.

Like Johnston, political scientist Jeffrey Legro suggests that Chinese political leaders are experiencing a clash of ideas and intentions regarding China's future role in the international system.[20] Other powers, especially the United States, should keep their ideational engagement with China so Chinese political elites can be further socialized by Western ideas, especially democracy and liberalism. The rise of the Soviet-like "new thinking" in China will eventually lead China to embrace democracy and the existing international order. In a similar vein, Like Legro, Johnston's policy suggestion is to further engage China through multilateral institutions so that Chinese leaders and policy elites can be continuously socialized by cooperative norms in security and foreign policy decision making. The US call for China to become a "responsible stakeholder" in the early 2000s can be seen as an engagement effort to socialize China into the existing international order.[21]

Like liberals, constructivists also face difficulties in explaining China's "assertiveness turn" in foreign policy after 2009. One possible explanation may lie in the contingent nature of ideas and intentions as well as the nonlinear socialization process. For example, Johnston might

argue that the socialization process of cooperative security norms is interrupted by other norms, such as nationalism or realpolitik.

While all three schools of thought contain some elements of truth, they suffer two analytical weaknesses: a static and holistic view of the international order and insufficient attention given to China's different strategies in challenging the international order. First, they hold a static and holistic view of the international order. In a realist world, the international order equals the international system, in which a rising power like China will inevitably challenge the status quo. When liberals argue that China is a beneficiary of the existing order, they also assume that there is only one Western order or liberal order in the world. Constructivists assume that some universal norms in one ideational system, such as cooperative security or democracy, may constitute and socialize Chinese elites' ideas in making policies.

Yet, "order" is a contested concept in international relations. Order can be just descriptive in nature in that scholars treat *order* as a synonym of *system*. International affairs scholar James Rosenau suggested that an analytic concept of order, or an empirical order, can "be located on a continuum which differentiates between those founded on cooperation and cohesion at one extreme and those sustained by conflict and disarray—i.e., disorder—at the other."[22] On the other hand, scholars can claim normative meanings to *order*, that is, a desirable outcome of states' interactions. Hedley Bull defined order as "a pattern that leads to a particular result, an arrangement of social life such that it promotes certain goals or values."[23] Similarly, Muthiah Alagappa conceptualizes order as "a formal or informal arrangement that sustains rule-governed interaction among sovereign states in their pursuit of individual and collection goals."[24] Generally, realists treat order more as a fact, while liberals and constructivists view order more as a rule or a value. However, as mentioned before, all of these three schools of thought to a certain extent hold a static and holistic conceptualization of order.[25]

In fact, the so-called international order has many components or sub-orders, which makes the transformation of the international order more dynamic than widely believed. According to Alagappa, order is built on the interaction among states. Different types of state interactions, therefore, can create different sub-international-orders, such as an economic order, a political order, and a security order in the world. Moreover, the change of the international order will not happen at one

time or overnight. Instead, one component of the international order, such as the economic order, may transform first while others may stay the same. In other words, the transformation of the whole international order will take time and happen gradually.

China might challenge the security order as realists predict, but it is not rational to overthrow the economic order, because, as liberals argue, China has been a "winner" by joining the liberal economic order after the Cold War. In addition, China's communist ideology might be at odds with the democracy-based political order, but it will not lead to war as long as China does not export communism or revolution to the outside world. Therefore, the holistic and static view of the "international order" oversimplifies the complex nature of the international order and thereby overemphasizes the potential dangers or threats from the rise of China.

Second, there is no doubt that China will challenge some components of the international order. However, how China will challenge the international order is still an unanswered question and deserves serious scholarly inquiry and scrutiny. On the one hand, if China uses military means to overthrow the existing order just like Japan and Germany did in World War II, then a hegemonic war or a power-transition conflict between a rising China and the existing hegemon as well as other regional powers, such as Japan, seems unavoidable. On the other hand, if China uses other means, such as institutions, to challenge some parts of the existing international order, then the outcome of China's challenges might not be conflictual. China can become a rule-maker or rule-reformer to transform the international order from within. As political scientists Randall Schweller and Xiaoyu Pu point out, China's "rightful resistance" toward US-led international order might not lead to war or conflict in the post–US-hegemony era.[26]

Prospect-Institutional Balancing Model: How Will China Challenge?

Built on prospect theory from behavioral economics and institutional balancing theory from IR, a "prospect-institutional balancing" model emerges to explain how China will challenge the different components of the international order or the sub-international orders. To simplify the model's application, we only focus on two parts of the international order in world politics: the liberal economic order and the US bilateralism-based security order in the Asia Pacific.

Institutional balancing theory is realism-based, which suggests that the high level of economic interdependence among states in the context of deepening globalization encourages states to choose multilateral institutions instead of traditional military means to pursue security and interests under the anarchic international system. It is applied to explain the proliferation of multilateral institutions in the Asia Pacific, such as the ASEAN Regional Forum (ARF), the ASEAN Plus Three (APT), and the East Asia Summit (EAS), after the Cold War.[27]

According to institutional balancing theory, there are two types of institutional balancing: inclusive and exclusive. Inclusive institutional balancing means to invite a target state into an institution and use the rules and norms of the institution to constrain the behavior of the target state. The establishment of the ARF is seen as an inclusive institutional balancing of ASEAN states in constraining China's behavior in the 1990s. Exclusive institutional balancing intends to exclude a target state from an institution and utilize the unity and cohesion of the institution to exert pressures toward or countervail threats from the target state. The APT is an example of exclusive institutional balancing conducted by ASEAN states and three major powers in East Asia to enhance cooperation among them as well as deal with pressures from the United States after the 1997 Asian economic crisis.[28]

China's institutional challenges to the international order are remarkable after the 2000s. On the one hand, China has adopted inclusive institutional balancing against the United States through actively engaging existing institutions, such as the APT, the EAS, and APEC. On the other hand, it has also chosen exclusive institutional balancing targeting the United States through non-US institutions, such as the Shanghai Cooperation Organization (SCO) and the CICA. After the 2008 financial crisis, China became even more proactive in proposing new multilateral institutions, such as the Asian Infrastructure Investment Bank, the Community of Common Destiny, as well as the "One Belt, One Road" (OBOR)—an ambitious investment initiative across Europe and Southeast Asia. It might still be debatable whether the OBOR is a multilateral institution or not. However, to streamline the implementation of the OBOR, some types of multilateral institutions around the OBOR might be inevitable in the future.

One puzzle about China's institutional behavior is its different strategies toward different institutions.[29] As mentioned before, China has used

both inclusive and exclusive balancing in different institutions. To better understand the consequences of China's institutional challenges to the international order, it is imperative to know under what conditions or *when* China will adopt inclusive institutional balancing and under what conditions and *when* exclusive institutional balancing. The existing institutional balancing theory is inadequate to answer this question.

This article borrows insights from prospect theory, a behavioral economics/psychology theory, to address this *when* question. From laboratory experiments, Daniel Kahneman and Amos Tversky, the originators of prospect theory, found that the way people interpret their situation for making choices—as a domain of either gains or losses—influences how they behave in terms of their risk orientation.[30] People tend to evaluate choices with respect to a reference point; they choose risk-averse behavior in a domain of gains but risk-acceptant behavior in a domain of losses. In other words, if people are in an advantageous situation (a domain of gains), they are more likely to behave cautiously (be risk averse) to protect their gains. However, when people are in a disadvantageous situation (a domain of losses), they are more likely to choose risky behavior (be risk acceptant) that may either reverse or worsen their losses.[31] In other words, they choose irrationally by going "against the odds" of expected utility calculations, as in the case of the debt-ridden lottery player in the domain of losses whose odds (probability) of winning the lottery (achieving gains) are much worse than losing the purchase price (incurring losses) of the lottery ticket.[32]

Integrating prospect theory and institutional balancing suggests three outcomes: (1) inclusive institutional balancing is less risky than exclusive institutional balancing, because the latter is more oriented toward alienation, antagonism, and rivalry than the former; (2) a state is more likely to choose inclusive institutional balancing in an arena where it has clear advantages (i.e., when its decisions are framed in a domain of gains); and (3) a state is more likely to adopt exclusive institutional balancing in an arena where it has clear disadvantages (i.e., when its decisions are framed in a domain of losses). Applying this "prospect-institutional balancing" model to China's different institutional strategies suggests two hypotheses:

1. When facing pressures in a sub-international order where China has a comparative advantage, Chinese leaders are more likely to

be framed in a domain of gains and thereby to adopt a risk-averse policy of inclusive institutional balancing.

2. When facing pressures in a sub-international order where China does not enjoy a comparative advantage, Chinese leaders are more likely to be framed in a domain of losses and thereby to adopt a risk-acceptant policy of exclusive institutional balancing.

To test this prospect-institutional balancing model, two brief case studies will be used to examine China's institutional strategies in APEC and CICA.[33] Each case examines Chinese leaders' domain of actions when facing challenges to see whether Chinese leaders behave in a domain of gains or a domain of losses. The prospect-institutional balancing model is used to predict what Chinese leaders will do. The results are compared to China's actual policy choices.

China's Institutional Strategies in APEC and CICA

China has adopted inclusive institutional balancing and exclusive institutional balancing strategies through the APEC and CICA respectively to deal with economic and security pressures from the United States. At the 2014 APEC meeting in Beijing, China actively promoted the Free Trade Area of the Asia-Pacific (FTAAP) for offsetting negative influences and the impact of the US-led Trans-Pacific Partnership (TPP). In 2014, China reinvigorated the CICA, a less-known security institution across Asia, to countervail security pressures from the "US pivot" policy by the Obama administration.

The TPP and China's Inclusive Institutional Balancing through the FTAAP

The APEC is an important multilateral institution aiming to promote free trade and economic liberalization in the Asia Pacific. It was established in 1989 and has 21 members from the Asia Pacific now, including the United States and China. However, due to the stalled Doha Round of trade negotiations in the World Trade Organization (WTO), states have started some bilateral and minilateral free trade negotiations at the beginning of the 2000s. Although the 21 APEC leaders still gather annually, the APEC's role in promoting free trade at the regional level has gradually marginalized and diminished.

The TPP, a smaller free trade pact than the APEC, is a product of widespread dissatisfaction over the stalled Doha Round in the WTO as well as the slow development of APEC. It originated from the Trans-Pacific Strategic Economic Partnership (TPSEP) agreement, a four-country trade agreement among Brunei, Chile, Singapore, and New Zealand in 2005. Starting in early 2008, the United States joined negotiations to establish a broad and high standard trading bloc—the TPP—on the basis of TPSEP with support from other US allies in the Asia Pacific, such as Australia, Canada, and Japan. In February 2016, 12 countries signed the TPP agreement.[34] Because of its relatively high admission standards, especially on protection for intellectual property, high labor and environmental codes, and restriction on state-owned enterprises, China is intentionally excluded from the TPP. The Obama administration was clear that the purpose of the TPP is to prevent China from writing the trading rules in the Asia Pacific.[35] In the eyes of Chinese elites, the TPP is nothing but a balancing strategy of the United States aiming to undermine China's economic power and influence in the Asia Pacific region.[36]

Facing US challenges through the TPP, China can adopt either exclusive or inclusive institutional balancing. For exclusive institutional balancing, China will need to form a new trading bloc to purposefully exclude the United States so the China-led new trading bloc can countervail pressures from the TPP. For inclusive institutional balancing, China will need to create and dominate a larger trading bloc including the United States so China can use this bigger trading bloc to dilute the negative influence of the TPP. It is worth noting that the Chinese government publicly stated that it would examine the possibility to join the TPP after the 12 countries signed the TPP agreement in February 2016. However, it is still not clear whether the statement is genuine or rhetorical in nature due to the mounting difficulties for the Chinese economy to meet the TPP standards in a short period.

According to the "prospect-institutional balancing" model, China's policy choices are shaped by the nature of the challenge. In the economics and trading arena, China has enjoyed a relatively advantageous position since the 2008 global financial crisis. That crisis started in the United States and spread to the whole world quickly. Although China's economic growth was also dragged down to 9 percent in 2008, it was still the most dynamic economy in the world. In addition, the Chinese government announced a two-year, four-trillion Chinese Yuan ($586

billion) stimulus plan to beef up its economy. It was the largest economic stimulus plan ever undertaken by the central government. As Dominique Strauss-Kahn, then the managing director of the International Monetary Fund, pointed out, "It's a huge package. . . . It will have an influence not only on the world economy in supporting demand but also a lot of influence on the Chinese economy itself, and I think it is good news for correcting imbalances."[37] To a certain extent, China was regarded as the hope of economic recovery in the world after the 2008 global financial crisis.[38]

In 2010, China passed Japan to become the second-largest economy in the world after the United States.[39] In 2013, China overtook the United States as the largest trading nation in the world.[40] In 2014, the IMF announced that according to purchasing power parity, China's economy has passed the United States as the largest economy in the world. Although the Chinese government seems reluctant to celebrate its economic success publicly, it is difficult to deny that its economic performance is relatively better than that of the rest of the world, especially compared to the West, when measured in terms of economic growth. It is also an underlying reason why the United States became so active in forming the TPP after 2008 to countervail China's economic influence in the Asia Pacific.

This relative economic advantage has placed Chinese leaders in a domain of gains when facing the TPP pressures from the United States. Therefore, according to the prospect-institutional balancing model, China is more likely to adopt an inclusive institutional balancing strategy. In fact, China has chosen inclusive institutional balancing to promote the FTAAP through the APEC. The strategic purpose of the FTAAP is to dilute the potential negative impacts from the TPP.

Establishing a regional free-trade agreement was not a new idea in the Asia Pacific. Japanese economist Kiyoshi Kojima is usually credited for first advancing such a Pacific free trade agreement concept in 1966. In the late 1980s, the Pacific Economic Cooperation Council and the later APEC were formed to encourage economic cooperation and trade liberalization in the region. In more recent times, US economist C. Fred Bergsten has been at the forefront as an advocate of an FTAAP. In 2006, Bergsten published an article in *Financial Times* suggesting that a regional trading bloc in the Asia Pacific can be a "plan B" to respond to the stalled trade negotiation in the Doha Round in the WTO.[41] The

APEC, therefore, has become a logical platform to promote the FTAAP. For example, the APEC officially announced that it would examine the long-term prospect of an FTAAP in 2006.

China has been an active member of APEC since it joined. Chinese leaders took the APEC summit meeting seriously because it is an important diplomatic platform to engage other countries, especially the United States. For example, it is reported that China and the United States utilized the APEC meeting to restore bilateral relations after the 1995–1996 Taiwan crisis.[42] However, China normally played a participant or a follower role in the APEC. There are two reasons for this. First, China is a latecomer to the liberal trade regime because it officially joined the WTO in December 2001. Although it has become the largest trading nation, until now China has not been granted a "market economy" status in the WTO. Therefore, as a beneficiary of the world trade regime, its contribution to the APEC is limited.

Second and more important, APEC is a loosely organized forum without enforcement mechanisms. The decision making of APEC is based on consensus and voluntarism. In other words, despite the fact that APEC leaders like to gather annually, APEC itself is just a place to propose ideas—not to implement them. Therefore, some critics suggest that APEC, like other multilateral institutions in Asia, is just a "talk shop" without teeth. For China, it can actively participate in the APEC, but there is no tangible benefit for it to lead the APEC. As for the proposal of establishing the FTAAP, China's original attitude was lukewarm at best just because of the "talk shop" nature of the APEC.

However, China's policy toward the APEC and the FTAAP changed dramatically in 2014 when the TPP challenges from the United States were approaching China's economy. In 2014, China was the host nation of the APEC summit in Beijing. Using its hosting role, China proactively advocated the establishment of the FTAAP. More importantly, China encouraged other APEC members to endorse a roadmap to form the FTAAP. If the FTAAP was just an idea or a proposal without any implementation plan before, it had a clear blueprint after the 2014 APEC meeting. President Xi hailed this new development as "a historic step we took in the direction toward realizing the FTAAP, marking the official launch of the FTAAP process and demonstrating the confidence and determination of the APEC in advancing regional economic integration."[43]

Although the final establishment of the FTAAP is still uncertain, China's changing policy toward the FTAAP serves two strategic purposes for China. First, since Xi Jinping came to power in 2013, China has gradually abandoned the traditional "keeping-a-low-profile" principle and started a foreign policy of striving for achievement. Hosting APEC in Beijing provided an opportunity for Xi to implement his new principle of striving for achievement.[44] Therefore, the FTAAP can be seen as a product of China's new proactive foreign policy under Xi. Additionally, the FTAAP can serve as an inclusive institutional balancing against the United States and its TPP. Differing from the TPP with only 12 members, the FTAAP includes all APEC nations.

While the United States stated that it would write the trading rules in the TPP, the FTAAP, if established under Chinese leadership, will become a rule-making arena for China. Moreover, it is clear that China intends to use the FTAAP to subsume the TPP in the future. For example, Xi clearly stated at the 2014 APEC meeting that the FTAAP can be the "aggregation" of existing free-trade arrangements, including the TPP and the Regional Comprehensive Economic Partnership (RCEP). In other words, the FTAAP will eventually take over both TPP and RCEP in leading regional trade and cooperation.

It is worth noting that China also actively engages in the negotiations of the RCEP, which is widely seen as a counterinstitution of the TPP. However, there are two reasons why the RCEP is not an exclusive institutional balancing of China against the United States. First, the RCEP is not led by China but by ASEAN. Actually, China has different views than ASEAN on the framework of the RCEP. While China preferred to develop the RCEP on the basis of ASEAN Plus Three, some ASEAN countries and Japan supported a broader structure of the RCEP (i.e., ASEAN Plus Six). Eventually, ASEAN and Japan won the "battle" and the current RCEP is based on the ASEAN Plus Six. Therefore, it is hard to argue that the RCEP is *China*'s exclusive institutional balancing strategy against the United States or the TPP—although it might help China countervail pressures from the TPP to a certain extent.

Second, the principle of the RCEP is an open or inclusive free-trade agreement. It means that the United States can join the RCEP anytime it wants. The problem is not that ASEAN or China wanted to exclude the United States from the RCEP but that the United States did not want to join in the first place, because the free-trade and investment

standards of the RCEP are too low compared to the TPP. Therefore, it is the United States that excluded itself from the RCEP, not China or ASEAN per se. This is why China has to choose APEC/FTAAP as a new inclusive institutional balancing strategy to further balance or dilute the potential negative impacts of TPP.

Still, China's high-profile effort in advocating the FTAAP does not mean that the FTAAP will be a success in promoting regional economic cooperation or trade liberalization. However, it serves China's institutional balancing purpose. On the one hand, the FTAAP offers a rule-making opportunity for China to compete with the United States in constructing the future trading regime in the Asia Pacific. On the other hand, it will reduce the negative economic impacts of the TPP on China's economy because all TPP members are included in the FTAAP. If both TPP and FTAAP are established, China will enjoy the same trading privileges with the TPP nations even though it is excluded from the TPP.

President Donald Trump's withdrawal from the TPP in early 2017 has brought uncertainties for the regional free-trade regime and China's foreign policy. It is hard to foresee what China will do without the TPP, because many domestic and international factors might influence its foreign and economic policies. However, institutional balancing theory suggests two preliminary predictions. First, without the TPP pressure, China's incentive to push the FTAAP will be reduced. Although it might still publicly support a region-wide free-trade agreement or the FTAAP, the lack of balancing pressure from the TPP will limit its substantial efforts in the FTAAP. Second, China might focus on the development of the RCEP since it has the potential to replace ASEAN's leadership in the RCEP. However, it will not be easy, because ASEAN and Japan will conduct inclusive institutional balancing against China inside the RCEP.

Thus, in facing US challenges in the economic arena, especially through the TPP, China has adopted an inclusive institutional balancing strategy through promoting FTAAP in APEC. Because of China's relatively strong economic performance after the 2008 financial crisis, Chinese leaders acted against the TPP challenge in a domain of gains. The inclusive institutional balancing is a risk-averse behavior because the FTAAP does not directly antagonize either the United States or the TPP. It is still a balancing strategy because the FTAAP has the potential to dilute the influence and impact of the TPP and the United States in the region. Therefore, China's FTAAP policy basically supports the first

hypothesis of the prospect-institutional balancing model, which suggests that China is more likely to adopt an inclusive institutional balancing strategy in an issue area where it has relative advantages compared to others.

US Pivot and China's Exclusive Institutional Balancing in CICA

The Obama administration adopted the "pivot toward Asia" after the 2008 financial crisis.[45] In 2011, Secretary of State Hillary Clinton published an article in *Foreign Policy* titled "America's Pacific Century," which emphasized US renewed interests in the Asia Pacific.[46] In late 2011, Obama paid a 10-day visit to the Asia Pacific to attend the East Asia Summit (EAS) in Bali, Indonesia. It was the first time the United States participated in the summit as a full member. Obama raised the South China Sea issue with Chinese Premier Wen Jiabao at the meeting. Moreover, in his speech in Australia, Obama reconfirmed the US pivot or rebalancing strategy in the Asia Pacific, because "the United States will play a larger and long-term role in shaping this region and its future."[47]

In June 2012, US defense secretary Leon Panetta announced the United States would reconfigure US forces to deploy 60 percent of its naval power to the Asia Pacific. The adjustments included "six aircraft carriers, and a majority of the Navy's cruisers, destroyers, littoral combat ships and submarines."[48] Moreover, Secretary Panetta ensured the coming budget cut would not affect US security commitments to the region. Given the fact that the United States already had 50 percent of its warships in the Pacific, the 10 percent increase of naval power seemed not very significant from a pure military perspective. However, considering US budget constraints at home as well as the unstable situation in the Middle East, it may have stretched thin what the United States could possibly do in the Pacific.

More importantly, the US pivot strategy aims at increasing the flexibility of US military deployments in the region. Instead of maintaining expensive permanent bases in Asia, the United States promoted a more flexible deployment approach in which its troop presence "will be smaller, more agile, expeditionary, self-sustaining, and self-contained."[49] More specifically, the United States will move or rotate its troops through different ports in the region. Although it is a less expensive deployment option, it will require greater cooperation from its Asian allies who will host US troops on their soil. In addition, it will also require upgrading

the military capabilities of its Asian allies or partners to facilitate military coordination with US troops.[50]

Multilaterally, the United States actively participated in regional institutions, such as the ARF and EAS. It is a sea change in US foreign policy compared with the George W. Bush administration, when Secretary of State Condoleezza Rice would consistently skip ARF meetings. Strategically, the United States started to strengthen traditional ties with allies, such as Japan, the Philippines, and Australia in the Asia Pacific. During his visit to Australia, Obama announced deploying 2,500 Marines in Darwin.[51] The United States also reached an agreement with Singapore to base several combat ships in its ports. In November 2011, Secretary Clinton visited Manila and signed the "Manila Declaration" to strengthen the Philippines' surveillance capabilities in the South China Sea.[52]

The US pivot is a clear containment effort in the eyes of Chinese leaders, although US officials publicly denied that it targeted China.[53] Facing US pivot pressures in the security arena, China has two strategic options. The first one is to form a military-based alliance to deal with military pressure from the strengthened US alliances in the region. It is a traditional realist policy rooted in either balance of power or balance of threat theories. Another option is institutional balancing, which means to use multilateral institutions to countervail US pressures. It is a policy option advocated by institutional balancing theory and soft balancing theory, which suggest that economic interdependence increases the potential costs of military-based balancing or hard balancing. Therefore, multilateral institutions become a useful diplomatic tool for states to balance against outside pressures.[54]

In fact, China has adopted both balancing strategies in dealing with the US "pivot" pressure. Militarily, China has strengthened its own capabilities (internal balancing) and tightened strategic ties with Russia (external balancing). Although neither China nor Russia admitted that their close military cooperation targeted the United States, their upgraded "strategic partnership" is widely seen as a "soft alliance" against the United States, the common threat for both China and Russia.[55] China's military-based balancing strategy against the United States deserves a serious inquiry, which is beyond the scope of this article. Here the main focus is on China's institutional balancing strategies through multilateral institutions, not internal or external balancing as Kenneth Waltz suggested.[56]

As mentioned before, the US pivot is multifaceted in nature. Strengthening military ties with traditional allies is only one part of the story. The United States has also used multilateral security institutions (such as the ARF) to pressure China on the South China Sea issues. Facing US pressures through multilateral institutions, China can choose either inclusive institutional balancing or exclusive institutional balancing. However, which policy China will choose depends on the domain of action that Chinese leaders are framed in according to the prospect-institutional balancing model.

Militarily, China is still far away from catching up with the United States. There are many military indicators that show the capability distance between China and the United States in technology, weaponry, and strategy. One simple way to gauge military power is to compare the military budgets of the two countries. China's defense spending is always a myth for analysts because of its less transparent political system.[57] In 2015, the Chinese government officially announced its defense budget of $146 billion, an increase of 11 percent from the budget of $131 billion in 2014. In comparison, the US defense budget is around $597 billion in 2015—four times the Chinese budget. Even with the most aggressive estimate from the Stockholm International Peace Research Institute, China's actual military spending was $214 billion, still only a third of the US budget.[58]

The huge military power gap between the United States and China has put the Chinese decision makers in a domain of losses in dealing with US challenges in the military arena. This disadvantageous situation encourages Chinese leaders to choose a risk-acceptant behavior in choosing institutional balancing means. According to the prospect-institutional balancing model, China is more likely to adopt exclusive institutional balancing when Chinese leaders are framed in a domain of losses. Through excluding the United States from a multilateral institution that China leads, China can utilize the cohesion and unity of the institutions to offset the pressures from the United States, although it is a risky institutional choice due to its potential antagonism toward the United States.

In 2014, China actively reinvigorated the CICA, an old security institution initiated by small central Asian countries, to exercise its exclusive institutional balancing against the United States. The CICA was first proposed by Kazakhstan President Nursultan Nazarbayev on 5 October

1992. It is a loosely organized, security-oriented multilateral institution in Asia. Originally, it had 15 members, including China, Russia, and some Central Asian and West Asian countries. It was not well known in the world because of its relatively slow institutionalization and development. The first foreign minister meeting of the CICA took place in 1999, and the first CICA summit meeting was in 2002. Due to the proliferation of the multilateral institutions in the Asia Pacific, the CICA did not attract much attention until 2014 when China chaired it. China hosted the fourth CICA summit in Shanghai, which became the largest ever participation by the heads of state and governments. The UN secretary general also attended the summit.

Through the "host" diplomacy by the Chinese, President Xi advocated a new "Asian security concept" at the CICA summit. According to Xi, "it is necessary to advocate common, comprehensive, cooperative, and sustainable security in Asia. We need to innovate our security concept, establish a new regional security cooperation architecture, and jointly build a road for security of Asia that is shared by and win-win to all."[59] It is worth noting that this was not the first time China promoted this type of cooperative security ideas. China advocated a similar "new security concept" at the ARF meeting in the 1990s.

However, there are two distinctions in Xi's speech at the CICA. First, China proposes a new security architecture targeting the US-led regional security order. It is still not clear what a security architecture based on "common, comprehensive, cooperative, and sustainable security" looks like and how Asian countries can achieve it. However, the real message between the lines of Xi's speech is that it is time to abandon the US-led, post–World War II regional security order. Moreover, Xi directly challenged the presence of the United States in the Asia Pacific. In his speech, Xi stated "it is for the people of Asia to run the affairs of Asia, solve the problems of Asia and uphold the security of Asia. The people of Asia have the capability and wisdom to achieve peace and stability in the region through enhanced cooperation."[60] Although Xi did not mention the United States in name, the implication is clear that Asia is for Asians and the United States should go home.

The United States is not a formal member of CICA; neither is Japan—both countries have an observer status. As one reporter mentioned, more than half of the CICA members are authoritarian regimes according to the Western standard.[61] Therefore, the CICA became a useful diplomatic

tool for China to gather support from states with similar ideologies and political systems. The unity and coherence of the CICA became a valuable form of soft power for China to countervail pressures from the United States. While the United States actively advocated its pivot to Asia through strengthening bilateral alliances, China (with the endorsement of the other CICA members) strongly promoted a multilateral security order based on cooperative security ideas. The competition between US bilateralism and Chinese multilateralism in regional security signifies the inevitable clash of ideas between the hegemon and a rising power during the power transition period. Although it is still too early to say whose version of regional security will win out, China's policy through the CICA is a clear exclusive institutional balancing strategy against the United States.

It is worth noting that the CICA is by no means the only institutional platform for China to challenge the United States. The Shanghai Cooperation Organization (SCO) is also a non-US security institution led by China and Russia. Like CICA, the SCO has become an important diplomatic arena for China to conduct its exclusive institutional balancing against the United States. The close military cooperation among the SCO members, such as joint military exercises, might not directly challenge US security and interests in the short run. In the long run, however, the cohesion of the SCO will be a valuable institutional asset for China to pool resources against the United States if necessary.

In short, China has adopted an exclusive institutional balancing strategy against the US pivot-to-Asia challenge in the security arena. Due to the huge power gap between the United States and China, Chinese leaders, especially Xi Jinping, are placed in a domain of losses, which encourages risk-acceptant behavior. Exclusive institutional balancing is more risky than inclusive institutional balancing due to its alienating and antagonistic nature. Just because no country likes to be excluded by others, this exclusive design of multilateral institutions becomes an important diplomatic weapon to address external threats and challenges from an outside target state.

Finally, it should be noted that prospect-institutional balancing is only partially supported in this case study. Facing the security challenges and threats from the United States, China indeed chose both traditional military-based balancing and exclusive institutional balancing strategies. But China's military-based balancing is beyond the explanatory domain

of the prospect-institutional balancing model, which reveals the theoretical limitation of the model. However, the prospect-institutional balancing model can still serve as an analytical tool to explain a state's institutional strategy in dealing with institutional pressures and challenges.

Conclusion

It is too pessimistic to predict or prescribe a conflictual and inevitable clash between China and the existing international order. Although China will challenge the existing order, how China will do it or which strategy it will use is still an understudied question. Moreover, which part of the international order China will take on is still uncertain. Therefore, it is too early to predict a coming conflict with China without carefully examining its various strategies in different sub-international orders.

Integrating prospect theory and institutional balancing theory introduces a prospect-institutional balancing model to explain how China deals with pressures from the United States in different issue areas. Facing US economic pressures through the TPP, Chinese leaders responded in a domain of gains because the Chinese economy was in much better shape than the rest of the world after the 2008 financial crisis. Therefore, China has adopted a risk-averse policy to conduct an inclusive institutional balancing strategy against the US TPP through promoting the FTAAP, because the FTAAP could reduce US influence and offset trading pressure from the TPP.

When the United States challenged China in the security arena through the pivot-toward-Asia policy in 2011, Chinese leaders were framed in a domain of losses due to the huge military power gap between the two nations. Consequently, Chinese leaders have conducted a risk-acceptant policy, that is, exclusive institutional balancing, against the US pressures in the CICA. Since the CICA is a non-US security institution, it provides the opportunity and platform for China to gather support and pool resources from other CICA members against the United States. In the 2014 CICA meeting in Shanghai, Xi advocated a new Asian security concept based on multilateralism as well as an "Asia-is-for-Asians" philosophy. Although it is unclear whether Xi's new Asian security concept can actually succeed beyond the CICA, the balancing goal of this new concept has been fulfilled. On the one hand, China has implied that the US-pivot policy was an outdated strategy, which should be replaced by multilateralism and cooperative security. On the other hand, China's

message is clear toward the outside world that the Chinse vision of the new security architecture will be more peaceful than widely predicted. In other words, what Xi really suggests is that it is time for other Asian countries to abandon the old US-led security order and embrace the new Chinese one.

China's rise will inevitably challenge the existing international order as we have seen from China's "assertiveness turn" in diplomatic strategy after the global financial crisis. However, we suggest that institution-based balancing and counterbalancing between China and the United States might not lead to war or conflict as realists predict. China intends to write new rules and develop new norms differing from the ones in the existing international order. However, China will also be constrained by these new norms and rules. This "lock-in" effect of multilateral institutions will ensure that a new type of power transition based on institutional balancing rather than traditional military means might be more peaceful than widely predicted. However, our case study on the CICA in the security arena also indicates that both the United States and China have also pursued military balancing besides institutional balancing against one another. As Winston Churchill used to say, "To jaw-jaw is always better than to war-war." The future of the international order depends on the wisdom of policy makers in selecting the right institutional tool to solve traditional problems. SSQ

Notes

1. Members of APEC include Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Chinese Taipei, Thailand, the United States, and Vietnam. Members of CICA include Afghanistan, Azerbaijan, Bahrain, Bangladesh, Cambodia, China, Egypt, India, Iran, Iraq, Israel, Jordan, Kazakhstan, the Republic of Korea, Kyrgyzstan, Mongolia, Pakistan, Palestine, Qatar, Russia, Tajikistan, Thailand, Turkey, United Arab Emirates, Uzbekistan, and Vietnam.

2. For critical reviews on China's rise and international relations theory, see Kai He and Huiyun Feng, "Xi Jinping's Operational Code Beliefs and China's Foreign Policy," *Chinese Journal of International Politics* 6, no. 3 (1 September 2013): 209–31, http://doi.org/f47mpw; Kai He and Huiyun Feng, "China's Bargaining Strategies after the Cold War: Successes and Challenges," *Asian Security* 10, no. 2 (June 2014): 168–87, http://doi.org/cb3k; and Huiyun Feng and Kai He, "China under Xi Jinping: Operational Code Beliefs, Foreign Policy, and the Rise of China," in *Chinese Foreign Policy Under Xi*, ed. Hoo Tiang Boon (London: Routledge, 2017).

3. John Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton, 2001).

4. For similar containment arguments, see Denny Roy, "Hegemon on the Horizon? China's Threat to East Asian Security," *International Security* 19, no. 1 (Summer 1994): 149–68, http://www.jstor.org/stable/2539151; and Gerald Segal, "East Asia and the 'Constrainment' of China," *International Security* 20, no. 4 (Spring 1996): 107–35, http://www.jstor.org/stable/2539044.

5. For a general power transition argument, see A. F. K. Organski, *World Politics* (New York: Knopf, 1958); Organski and Jack Kugler, *The War Ledger* (Chicago: University of Chicago Press, 1980); and Robert Gilpin, *War and Change in World Politics* (Cambridge: Cambridge University Press, 1981). For applications of power transition theory to China's rise, see Douglas Lemke and Ronald Tammen, "Power Transition Theory and the Rise of China," *International Interactions* 29, no.4 (2003): 269–71, http://doi.org/fssct7; and Ronald Tammen and Jacek Kugler, "Power Transition and China-US Conflicts," *Chinese Journal of International Politics* 1, no. 1 (2006): 31–55, http://doi.org/dvvtjb; and Jack Levy, "Power Transition Theory and the Rise of China," in *China's Ascent*, ed. Robert Ross and Zhu Feng (Ithaca, NY: Cornell University Press, 2008), 11–33. For criticisms of applying power transition theory to China's rise, see Steve Chan, *China, the U.S., and the Power-Transition Theory* (London: Routledge, 2008).

6. For defensive realism, see Kenneth Waltz, *Theory of International Politics* (New York: McGraw-Hill, 1979); Jeffrey Taliaferro, "Security Seeking under Anarchy," *International Security* 25, no. 3 (Winter 2000/01): 128–61, http://doi.org/cp9t8q; Stephen Walt, *Taming American Power: The Global Response to U.S. Primacy* (New York: W. W. Norton, 2005); and C. L. Glaser, "Realists as Optimists: Cooperation as Self-Help," *International Security* 19, no. 3 (Winter 1994/95): 50–90, http://www.jstor.org/stable/2539079.

7. Christopher Layne, "The Unipolar Illusion: Why New Great Powers Will Rise," *International Security* 17, no. 4 (Spring 1993): 5–51, http://www.jstor.org/stable/2539020; Layne, "House of Cards: American Strategy toward China," *World Policy Journal* 14, no. 3 (Fall 1997): 77–95, http://www.jstor.org/stable/40209546; and Layne, *The Peace of Illusions: American Grand Strategy from 1940 to the Present* (Ithaca, NY: Cornell University Press, 2006).

8. Thomas J. Christensen, "Posing Problems without Catching Up: China's Rise and Challenges for US Security Policy," *International Security* 25, no. 4 (2001): 5–40, http://doi.org/bzptvc; Aaron L. Friedberg and Robert S. Ross, "Here Be Dragons: Is China a Military Threat?," *The National Interest* 103 (September–October 2009): 19–34, http://nationalinterest.org/greatdebate/dragons-3816; and Michael Beckley, "China's Century?: Why America's Edge Will Endure," *International Security* 36, no. 3 (Winter 2011/12): 41–78, http://www.jstor.org/stable/41428109.

9. Christopher Layne, "Offshore Balancing Revisited," *Washington Quarterly* 25, no. 2 (Spring 2002): 233–48, https://muse.jhu.edu/article/36688; and Walt, *Taming American Power*.

10. John J. Mearsheimer, "The Gathering Storm: China's Challenge to US Power in Asia," *Chinese Journal of International Politics* 3, no. 4 (December 2010): 381–96, http://doi.org/d28xwp. For US pivot toward Asia, see Hillary Clinton, "America's Pacific Century," *Foreign Policy* 189, no. 1 (11 October 2011): 56–63, http://foreignpolicy.com/2011/10/11/americas-pacific-century/; Kenneth Lieberthal, "The American Pivot to Asia," *Foreign Policy*, 21 December 2011, http://foreignpolicy.com/2011/12/21/the-american-pivot-to-asia/; and Robert Dreyfuss, "Fool's Errand: America's Pivot to Asia," *The Diplomat*, 5 December 2012, http://thediplomat.com/2012/12/americas-pivot-has-no-clothes/. More recently, US officials have used the term "rebalance" to describe the pivot to Asia. We have elected to continue using the original term "pivot" in this article.

11. For some liberal discussions, see James L. Richardson, "Asia-Pacific: The Case for Geopolitical Optimism," *National Interest*, no. 38 (Winter 1994/95): 28–39, http://www.jstor

.org/stable/42896882; Ralph A. Cossa and Jane Khanna, "East Asia: Economic Interdependence and Regional Security," *International Affairs* 73, no. 2 (April 1997): 219–34, http://www.jstor.org/stable/2623825; and David Shambaugh, "China Engages Asia: Reshaping the Regional Order," *International Security* 29, no. 3 (Winter 2004/05): 64–99, http://www.jstor.org/stable/4137556.

12. *See* G. John Ikenberry, "The Rise of China and the Future of the West: Can the Liberal System Survive?," *Foreign Affairs* 87, no. 1 (January/February 2008): 23–35, https://www.foreignaffairs.com/articles/asia/2008-01-01/rise-china-and-future-west.

13. See the following, all by G. John Ikenberry, "Liberalism and Empire: Logics of Order in the American Unipolar Age," *Review of International Studies* 30, no. 4 (October 2004): 609–30, http://www.jstor.org/stable/20097941; *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major War* (Princeton, NJ: Princeton University Press, 2001); and *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order* (Princeton, NJ: Princeton University Press, 2011).

14. For an engagement argument, see Elizabeth Economy, "Don't Break the Engagement," *Foreign Affairs* 83, no. 3 (May/June 2004): 96–109, http://www.jstor.org/stable/20033978. For a critical evaluation, see Paul A. Papayoanou and Scott L. Kastner, "Sleeping with the (Potential) Enemy: Assessing the U.S. Policy of Engagement with China," *Security Studies* 9, no. 1–2 (1999): 157–87, http://doi.org/fg23cq.

15. *See* Joshua Kurlantzick, *Charm Offensive: How China's Soft Power Is Transforming the World* (New Haven, CT: Yale University Press, 2008); and Zheng Bijian, "China's 'Peaceful Rise' to Great-Power Status," *Foreign Affairs* 84, no. 5 (September/October 2005): 18–24, http://www.jstor.org/stable/20031702.

16. *See* Robert D. Hormats, Elizabeth Economy, and Kevin Nealer, eds., *Beginning the Journey: China, the United States, and the WTO* (New York: Council on Foreign Relations, 2001).

17. Marc Lanteigne, *China and International Institutions: Alternate Paths to Global Power* (New York: Routledge, 2005); and Kai He, *Institutional Balancing in the Asia Pacific: Economic Interdependence and China's Rise* (New York: Routledge, 2009).

18. For a general social constructivism theory, see Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999).

19. Alastair Iain Johnston, *Social States: China in International Institutions 1980–2000* (Princeton, NJ: Princeton University Press, 2008).

20. Jeffrey Legro, "What China Will Want: The Future Intentions of a Rising Power," *Perspectives on Politics* 5, no. 3 (September 2007): 515–34, http://www.jstor.org/stable/20446501.

21. *See* Robert Zoellick, "Whither China: From Membership to Responsibility?" (speech, National Committee on US–China relations, New York City, New York, 21 September 2005), http://www.ncuscr.org/files/2005Gala_RobertZoellick_Whither_China1.pdf.

22. James Rosenau, "Governance, Order, and Change in World Politics," in *Governance without Government: Order and Change in World Politics*, ed. James Rosenau and Ernst-Otto Czempiel (Cambridge: Cambridge University Press, 1992), 11.

23. Hedley Bull, *The Anarchical Society: A Study of Order in World Politics* (London: Macmillan, 1977), 3–4.

24. Muthiah Alagappa, "The Study of International Order: An Analytical Framework," in *Asian Security Order: Instrumental and Normative Features*, ed. Alagappa (Stanford, CA: Stanford University Press, 2003), 39.

25. *See* Kai He, "Contested Regional Orders and Institutional Balancing in the Asia Pacific," *International Politics* 52, no. 2 (February 2015): 208–22, http://doi.org/cb3t.

26. Randall L. Schweller and Xiaoyu Pu, "After Unipolarity: China's Visions of International Order in an Era of US Decline," *International Security* 36, no. 1 (Summer 2011): 41–72, http://www.jstor.org/stable/41289688.

27. For institutional balancing theory, see Kai He, *Institutional Balancing in the Asia-Pacific: Economic Interdependence and China's Rise* (London: Routledge, 2009). For an application of institutional balancing theory, see Seungjoo Lee, "Institutional Balancing and the Politics of Mega-FTAs in East Asia," *Asian Survey* 56, no. 6 (November/December 2016): 1055–76, http://doi.org/cb3v.

28. Kai He, "Institutional Balancing and International Relations Theory: Economic Interdependence and Balance of Power Strategies in Southeast Asia," *European Journal of International Relations* 14, no. 3 (September 2008): 489–518, http://doi.org/cvs2zj.

29. *See* Scott L. Kastner, Margaret M. Pearson, and Chad Rector, "Invest, Hold Up, or Accept? China in Multilateral Governance," *Security Studies* 25, no. 1 (February 2016): 142–79, http://doi.org/cb3w.

30. Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* 47 (March 1979), 263–91, http://www.jstor.org/stable/1914185. Tversky died in 1996, and Kahneman was awarded the 2002 Nobel Prize in economics for his work in prospect theory.

31. Rose McDermott, "Prospect Theory in Political Science: Gains and Losses from the First Decade," *Political Psychology* 25, no. 2 (April 2004): 294, http://doi.org/fr6f3x.

32. Prospect theory has other interesting findings, such as the endowment effect and loss aversion. In this article, we focus on the framing effect—that is, how the domains of action with respect to the reference point influence risk propensity and behavior. For discussions of other findings of prospect theory, see Jack S. Levy, "Prospect Theory and International Relations: Theoretical Applications and Analytical Problems," in *Avoiding Losses/Taking Risks: Prospect Theory and International Conflict*, ed. Barbara Farnham (Ann Arbor: University of Michigan Press, 1995), 119–46; Robert Jervis, "Political Implications of Loss Aversion," *Political Psychology* 13, no. 2 (June 1992): 187–201, http://www.jstor.org/stable/3791678; Jervis, "The Implications of Prospect Theory for Human Nature and Values," *Political Psychology* 25, no. 2 (April 2004): 163–76, http://doi.org/dgh7f5; Barry O'Neill, "Risk Aversion in International Relations Theory," *International Studies Quarterly* 45, no. 4 (December 2001): 617–40, http://www.jstor.org/stable/3096063; and Kai He, *China's Crisis Behavior: Political Survival and Foreign Policy after the Cold War* (Cambridge: Cambridge University Press, 2016).

33. A "congruence test" method is employed in case studies. If China's policy choice fits what the model suggests, i.e., inclusive institutional balancing in an advantageous situation and exclusive institutional balancing under a disadvantageous condition, then the model passes the congruence test. Otherwise, it fails the congruence test and we need to find a new model or variables to explain China's behavior.

34. US President Donald Trump withdrew the United States from the TPP in January 2017. Without the United States, the influence and future of the TPP will be full of uncertainties.

35. Jackie Calmes, "Trans-Pacific Partnership Text Released, Waving Green Flag for Debate," *New York Times*, 5 November 2015, https://www.nytimes.com/2015/11/06/business/international/trans-pacific-trade-deal-tpp-vietnam-labor-rights.html?mcubz=1.

36. Kenneth Lieberthal and Jisi Wang, "Addressing U.S.-China Strategic Distrust," John L. Thornton China Center Monograph Series, no. 4, Brookings Institution, 30 March 2012, https://www.brookings.edu/research/addressing-u-s-china-strategic-distrust/; Michael J. Green and Matthew P. Goodman, "After TPP: The Geopolitics of Asia and the Pacific," *Washington Quarterly* 38, no. 4 (Winter 2016): 19–34, http://doi.org/cb3x; and Jane Perlez, "U.S. Allies See

Trans-Pacific Partnership as a Check on China," *New York Times*, 6 October 2015, https://www.nytimes.com/2015/10/07/world/asia/trans-pacific-partnership-china-australia.html?mcubz=1. For some primary Chinese sources, see Tang Bi and Lin Guijun, "Kua Taipingyang Huoban Guanxi Xieding dui Zhongguo Zhanlue de Yingxiang yu Zhongguo de Duice" ["The Strategic Impacts of TPP and China's Policy Responses"], *Shehui Kexue Yanjiu* [*Social Science Research*], no. 6 (2012), 16–20; Sun Suyuan, "Meiguo TPP Zhanlue de Sanchong Xiaoying" ["Three Effects of America's TPP Strategy"], *Dangdai Yatai* [*Journal of Contemporary Asia Pacific Studies*], no. 3 (2013): 4–22; and Shen Minghui, "Meiguo de Quyu Hezuo Zhanlue: Quyu haishi Quanqiu—Meiguo Tuidong TPP de Xingwei Luoji" ["America's FTA Strategy: Regional or Global? The Behavioral Logic behind American Promotion of TPP"], *Dangdai Yatai* [*Journal of Contemporary Asia Pacific Studies*], no. 6 (2013): 70–94.

37. David Barboza, "China Plans $586 Billion Economic Stimulus," *New York Times*, 9 November 2008, http://www.nytimes.com/2008/11/09/business/worldbusiness/09iht-yuan.4.17664544.html?mcubz=1.

38. *See* Dean Baker, "China's Chance to Be our Economic Saviour," *The Guardian*, 22 September 2011, https://www.theguardian.com/commentisfree/cifamerica/2011/sep/22/china-world-economic-saviour.

39. David Barboza, "China Passes Japan as Second-Largest Economy," *New York Times*, 12 August 2010, http://www.nytimes.com/2010/08/16/business/global/16yuan.html?pagewanted=all&_r=0.

40. Angela Monaghan, "China Surpasses US as World's Largest Trading Nation," *The Guardian*, 10 January 2014, https://www.theguardian.com/business/2014/jan/10/china-surpasses-us-world-largest-trading-nation.

41. Fred Bergsten, "Plan B for World Trade: Go Regional," *Financial Times*, 16 August 2006, http://www.ft.com/cms/s/0/f5eec3f8-2cc3-11db-9845-0000779e2340.html?ft_site=falcon&desktop=true.

42. *See* He, *China's Crisis Behavior*; and Qian Qichen, *Ten Episodes in China's Diplomacy* (New York: Harper Collins, 2006).

43. Shen Qing, "APEC Roadmap on FTAAP a Historic Decision: Xi," *Xinhua*, 11 November 2014.

44. Yan Xuetong, "From Keeping a Low Profile to Striving for Achievement," *Chinese Journal of International Politics* 7, no. 2 (1 June 2014): 153–84, http://doi.org/cb3z.

45. We use the term "pivot" throughout this article even though the term "rebalance to Asia" has been used more recently.

46. Clinton, "America's Pacific Century."

47. President Barack Obama, "Remarks by President Obama to the Parliament," Daily Comp. Pres. Docs., 2011 DCPD no. 201100873 (speech, Parliament House, Canberra, Australia, 17 November 2011), 3, https://www.gpo.gov/fdsys/pkg/DCPD-201100873/pdf/DCPD-201100873.pdf.

48. Jane Perlez, "Panetta Outlines New Weaponry for Pacific," *New York Times*, 1 June 2012, http://www.nytimes.com/2012/06/02/world/asia/leon-panetta-outlines-new-weaponry-for-pacific.html?mcubz=1.

49. Lt Gen Wallace Gregson Jr., retired, "Understanding the US Pivot to Asia" (remarks, Brookings Institution Conference, Washington, DC, 31 January 2012), http://www.brookings.edu/events/2012/0131_us_asia.aspx.

50. Mark E. Manyin, Stephen Daggett, Ben Dolven, Susan V. Lawrence, Michael F. Martin, Ronald O'Rourke, and Bruce Vaughn, *Pivot to the Pacific? The Obama Administration's "Re-*

balancing" toward Asia (Washington, DC: Congressional Research Service, 28 March 2012), 11–12, https://fas.org/sgp/crs/natsec/R42448.pdf.

51. Jackie Calmes, "A U.S. Marine Base for Australia Irritates China," *New York Times*, 16 November 2011, http://www.nytimes.com/2011/11/17/world/asia/obama-and-gillard-expand-us-australia-military-ties.html.

52. *See* Office of the Spokesperson, "Signing of the Manila Declaration on Board the USS *Fitzgerald* in Manila Bay, Manila, Philippines," US Department of State, 16 November 2011, Washington, DC, https://2009-2017.state.gov/r/pa/prs/ps/2011/11/177226.htm.

53. For Chinese views on the pivot, see Yan Xuetong, "Strategic Cooperation without Mutual Trust: A Path Forward for China and the United States," *Asia Policy*, no. 15 (January 2013): 4–6, http://doi.org/cb3q; and Lieberthal and Wang, "Addressing U.S.-China Strategic Distrust."

54. For soft balancing, see R. A. Pape, "Soft Balancing against the United States," *International Security* 30, no. 1 (Summer 2005): 7–45, http://www.jstor.org/stable/4137457; and T. V. Paul, "Soft Balancing in the Age of US Primacy," *International Security* 30, no. 1 (Summer 2005): 46–71, http://www.jstor.org/stable/4137458.

55. Huiyun Feng, *The New Geostrategic Game: Will China and Russia Form an Alliance against the United States?*, DIIS Policy Report 2015:07 (Copenhagen: Danish Institute for International Studies, 2015), https://www.diis.dk/en/research/the-new-geostrategic-game.

56. For internal and external balancing through military means, see Waltz, *Theory of International Politics*.

57. *See* ChinaPower Team, "What Does China Really Spend on Its Military?," Center for Strategic and International Studies, 28 December 2015, http://chinapower.csis.org/military-spending/.

58. Adam Taylor and Laris Karklis, "This Remarkable Chart Shows How U.S. Defense Spending Dwarfs the Rest of the World," *Washington Post*, 9 February 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/02/09/this-remarkable-chart-shows-how-u-s-defense-spending-dwarfs-the-rest-of-the-world/?utm_term=.d6ae0b5035f2.

59. Jinping Xi, "New Asian Security Concept for New Progress in Security Cooperation" (remarks, Fourth Summit of the Conference on Interaction and Confidence Building Measures in Asia, Shanghai, 21 May 2014).

60. Ibid.

61. Jamil Anderlini, "China Reinvigorates Regional Clubs to Counter US Power," *Financial Times*, 20 May 2014, http://www.ft.com/cms/s/0/a01c11b8-e009-11e3-9534-00144feabdc0.html.

Commanding the Trend: Social Media as Information Warfare

Lt Col Jarred Prier, USAF

Abstract

This article demonstrates how social media is a tool for modern information-age warfare. It builds on analysis of three distinct topics: social networking, propaganda, and news and information sharing. Two case studies are used to show how state and nonstate actors use social media to employ time-tested propaganda techniques to yield far-reaching results. The spread of the propaganda message is accomplished by tapping into an existing narrative, then amplifying that message with a network of automatic "bot" accounts to force the social media platform algorithm to recognize that message as a trending topic. The first case study analyzes Islamic State (IS) as a nonstate actor, while the second case observes Russia as a state actor, with each providing evidence of successful influence operations using social media. Coercion and persuasion will continue to be decisive factors in information warfare as more countries attempt to build influence operations on social media.

✳ ✳ ✳ ✳ ✳

For years, analysts in the defense and intelligence communities have warned lawmakers and the American public of the risks of a cyber Pearl Harbor. The fear of a widespread cyber-based attack loomed over the country following intrusions against Yahoo! email accounts in 2012, Sony Studios in 2014, and even the United States government Office of Personnel Management (OPM) in 2015. The average American likely did not understand exactly how, or for what purposes, US adversaries

---

Lt Col Jarred Prier, USAF, currently serves as director of operations for the 20th Bomb Squadron. He completed a USAF fellowship at the Walsh School of Foreign Service at Georgetown University and earned a master's degree from the School of Advanced Air and Space Studies at Air University, Maxwell Air Force Base, Alabama. Prier also holds a master of science degree in international relations from Troy University, Alabama. This article evolved from his thesis.

were operating within the cyber domain, but the implications of future attacks were not difficult to imagine. Enemies of the United States could target vulnerable power grids, stock markets, train switches, academic institutions, banks, and communications systems in the opening salvos of this new type of warfare.[1]

In contrast to more traditional forms of cyberattack, cyber operations today target people within a society, influencing their beliefs as well as behaviors, and diminishing trust in the government. US adversaries now seek to control and exploit the trend mechanism on social media to harm US interests, discredit public and private institutions, and sow domestic strife. "Commanding the trend" represents a relatively novel and increasingly dangerous means of persuasion within social media. Thus, instead of attacking the military or economic infrastructure, state and nonstate actors outside the United States can access regular streams of online information via social media to influence networked groups within the United States. This article analyzes how two US adversaries hijacked social media using four factors associated with command of the trend. First it provides a basis for commanding the trend in social media by analyzing social media as a tool for obtaining and spreading information. It then looks more specifically at how US adversaries use social media to command the trend and target US citizens with malicious propaganda. Next, the two most prominent, recent case studies provide evidence of how nonstate and state actors use social media to counter the United States. The first case study covers IS from 2014 to 2016 by examining the group's use of social media for recruiting, spreading propaganda, and proliferating terror threats. The second case describes the pattern of Russian hacking, espionage, disinformation, and manipulation of social media with a particular focus on the United States presidential election of 2016. Evidence for this second case study comes from nearly two years of research on Twitter accounts believed to be part of a Russian information warfare network. The article concludes with implications and predictions of how social media will continue to develop, what can be expected in the future, and how the United States can respond to the growing threat of adversaries commanding the trend.

Commanding the Trend in Social Media

The adaptation of social media as a tool of modern warfare should not be surprising. Internet technology evolved to meet the needs of

information-age warfare around 2006 with the dawn of Web 2.0, which allowed internet users to create content instead of just consuming online material. Instead, the individual could decide what was important and only read what was important, on demand. Not only could users select what news they want to see, but they could also use the medium to create news based on their opinions.[2] The social nature of humans ultimately led to virtual networking. As such, traditional forms of media were bound to give way to a more tailorable form of communication. US adversaries were quick to find ways to exploit the openness of the internet, eventually developing techniques to employ social media networks as a tool to spread propaganda. Social media creates a point of injection for propaganda and has become the nexus of information operations and cyber warfare. To understand this we must examine the important concept of the social media trend and look briefly into the fundamentals of propaganda. Also important is the spread of news on social media, specifically, the spread of "fake news" and how propaganda penetrates mainstream media outlets.

Trending Social Media

Social media sites like Twitter and Facebook employ an algorithm to analyze words, phrases, or hashtags to create a list of topics sorted in order of popularity. This "trend list" is a quick way to review the most discussed topics at a given time. According to a 2011 study on social media, a trending topic "will capture the attention of a large audience for a short time" and thus "contributes to agenda setting mechanisms."[3] Using existing online networks in conjunction with automatic "bot" accounts, foreign agents can insert propaganda into a social media platform, create a trend, and rapidly disseminate a message faster and cheaper than through any other medium. Social media facilitates the spread of a narrative outside a particular social cluster of true believers by commanding the trend. It hinges on four factors: (1) a message that fits an existing, even if obscure, narrative; (2) a group of true believers predisposed to the message; (3) a relatively small team of agents or cyber warriors; and (4) a network of automated "bot" accounts.

The existing narrative and the true believers who subscribe to it are endogenous, so any propaganda must fit that narrative to penetrate the network of true believers. Usually, the cyber team is responsible for crafting the specific message for dissemination. The cyber team then generates

videos, memes, or fake news, often in collusion with the true believers. To achieve the effective spread of propaganda, the true believers, the cyber team, and the bot network combine efforts to take command of the trend. Thus, an adversary in the information age can influence the population using a variety of propaganda techniques, primarily through social media combined with online news sources and traditional forms of media.

A trending topic transcends networks and becomes the mechanism for the spread of information across social clusters. Here the focus is primarily on Twitter, a "microblogging" site where each post is limited to 140 characters.[4] Facebook also has a trends list, but it is less visible than the Twitter trends list, and the two applications serve different purposes. Facebook maintains a function of bringing friends and families together. On Facebook, your connections are typically more intimate connections than you would expect on Twitter, which focuses less on bringing people together and more on bringing ideas together. As a microblog, Twitter's core notion is to share your thoughts and feelings about the world around you with a group of people who share similar interests. The individuals who follow each other may not be friends but could be a team of like-minded academics, journalists, sports fans, or politicos. When a person tweets, that tweet can be viewed by anyone who follows that person, or anyone who searches for that topic using Twitter's search tool. Additionally, anyone can "retweet" someone else's tweet, which broadcasts the original to a new audience. Twitter makes real-time idea and event sharing possible on a global scale.[5] Another method for quick referencing on Twitter is using a "hashtag." The tweet would then be visible to anyone who clicked on the link along with all of the other tweets using the same hashtag.

A trend can spread a message to a wide group outside of a person's typical social network. Moreover, malicious actors can use trends to spread a message using multiple forms of media on multiple platforms, with the ultimate goal of garnering coverage in the mainstream media. Command of the trend is a powerful method of spreading information whereby, according to an article in the *Guardian*, "you can take an existing trending topic, such as fake news, and then weaponise it. You can turn it against the very media that uncovered it."[6]

Because Twitter is an idea-sharing platform, it is very popular for rapidly spreading information, especially among journalists and academics;

however, malicious users have also taken to Twitter for the same benefits in recent years. At one time, groups like al-Qaeda preferred creating websites, but now, "Twitter has emerged as the internet application most preferred by terrorists, even more popular than self-designed websites or Facebook."[7] Twitter makes it easy to spread a message to both supporters and foes outside of a particular network. Groups trying to disseminate a message as widely as possible can rely on the trend function to reach across multiple networks.

Three methods help control what is trending on social media: trend distribution, trend hijacking, and trend creation. The first method is relatively easy and requires the least amount of resources. Trend distribution is simply applying a message to every trending topic. For example, someone could tweet a picture of the president with a message in the form of a meme—a stylistic device that applies culturally relevant humor to a photo or video—along with the unrelated hashtag #SuperBowl. Anyone who clicks on that trend list expecting to see something about football will see that meme of the president. Trend hijacking requires more resources in the form of either more followers spreading the message or a network of "bots" (autonomous programs that can interact with computer systems or users) designed to spread the message automatically. Of the three methods to gain command of the trend, trend creation requires the most effort. It necessitates either money to promote a trend or knowledge of the social media environment around the topic, and most likely, a network of several automatic bot accounts.

Bot accounts are non-human accounts that automatically tweet and retweet based on a set of programmed rules. In 2014, Twitter estimated that only 5 percent of accounts were bots; that number has grown along with the total users and now tops 15 percent.[8] Some of the accounts are "news bots," which just retweet the trending topics. Some of the accounts are for advertising purposes, which try to dominate conversations to generate revenue through clicks on links. Some bots are trolls, which, like a human version of an online troll, tweet to disrupt the civil conversation.

For malicious actors seeking to influence a population through trends on social media, the best way to establish trends is to build a network of bot accounts programmed to tweet at various intervals, respond to certain words, or retweet when directed by a master account. Figure 1 illustrates the basics of a bot network. The top of the chain is a small

core group. That team is composed of human-controlled accounts with a large number of followers. The accounts are typically adversary cyber warriors or true believers with a large following. Under the core group is the bot network. Bots tend to follow each other and the core group. Below the bot network is a group consisting of the true believers without a large following. These human-controlled accounts are a part of the network, but they appear to be outsiders because of the weaker links between the accounts. The bottom group lacks a large following, but they do follow the core group, sometimes follow bot accounts, and seldom follow each other.

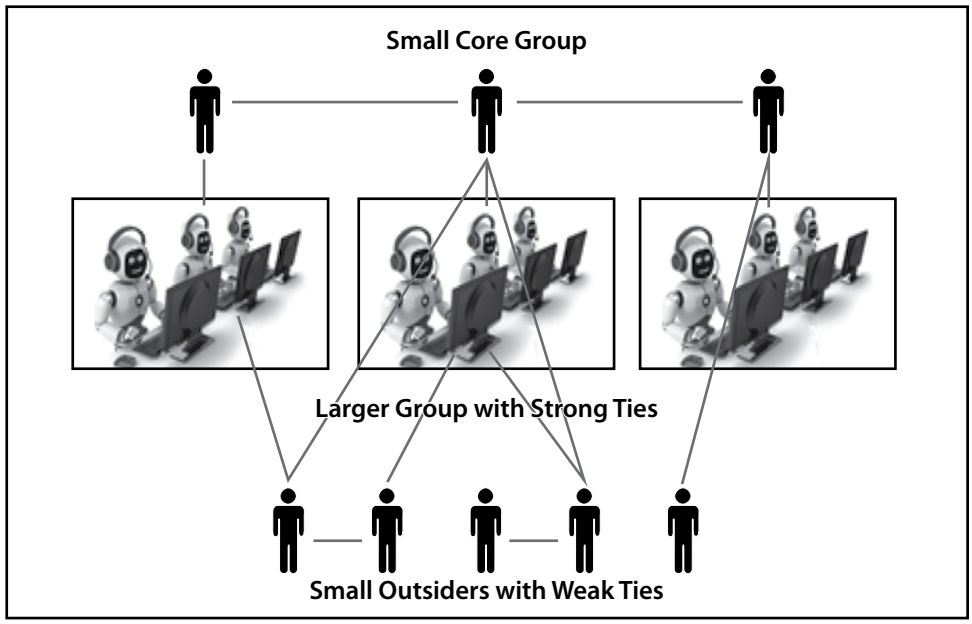


Figure 1. Illustration of a bot network

Enough bots working together can quickly start a trend or take over a trend, but bot accounts themselves can only bridge the structural hole between networks, not completely change a narrative. To change a narrative, to conduct an effective influence operation, requires a group to combine a well-coordinated bot campaign with essential elements of propaganda.

Propaganda Primer

Messaging designed to influence behavior has been around for centuries but became easier as methods of mass communication enabled wider dissemination of propaganda. Observing the rise of mass media and its presence in daily life, French philosopher Jacques Ellul noted the simplicity of propaganda in 1965. According to Ellul, "Propaganda ceases where simple dialogue begins."[9] That said, it is worth noting Eric Hoffer's comments that "propaganda on its own cannot force its way into unwilling minds, neither can it inculcate something wholly new."[10] For propaganda to function, it needs a previously existing narrative to build upon, as well as a network of true believers who already buy into the underlying theme. Social media helps the propagandist spread the message through an established network. A person is inclined to believe information on social media because the people he chooses to follow share things that fit his existing beliefs. That person, in turn, is likely to share the information with others in his network, to others who are like-minded, and those predisposed to the message. With enough shares, a particular social network accepts the propaganda storyline as fact. But up to this point, the effects are relatively localized. The most effective propaganda campaigns are not confined just to those predisposed to the message. Essentially, propaganda permeates everyday experiences, and the individual targeted with a massive media blitz will never fully understand that the ideas he has are not entirely his own. A modern example of this phenomenon was observable during the Arab Spring as propaganda spread on Facebook "helped middle-class Egyptians understand that they were not alone in their frustration."[11] In short, propaganda is simpler to grasp if everyone around a person seems to share the same emotions on a particular subject. Even a general discussion among the crowd can provide the illusion that propaganda is information.[12] In other words, propaganda creates heuristics, which is a way the mind simplifies problem solving by relying on quickly accessible data. The availability heuristic weighs the amount and frequency of information received, as well as recentness of the information, as more informative than the source or accuracy of the information.[13] Essentially, the mind creates a shortcut based on the most—or most recent—information available, simply because it can be remembered easily. Often, the availability heuristic manifests itself in information received through media coverage. The availability heuristic is important to understanding individual opinion formation and how propaganda can exploit the shortcuts our minds make to form opinions. The lines in figure 2 show formation

of opinions temporally, with bold arrows influencing a final opinion more than light arrows. The circled containers indicate a penetration point for propaganda exploitation. As previously described, mass media enables rapid spread of propaganda, which feeds the availability heuristic. The internet makes it possible to flood the average person's daily intake of information, which aids the spread of propaganda.

One of the primary principles of propaganda is that the message must resonate with the target. Therefore, when presented with information that is within your belief structure, your bias is confirmed and you accept the propaganda. If it is outside of your network, you may initially reject the story, but the volume of information may create an availability heuristic in your mind. Over time, the propaganda becomes normalized—and even believable. It is confirmed when a fake news story is reported by the mainstream media, which has become reliant on social media for spreading and receiving news.

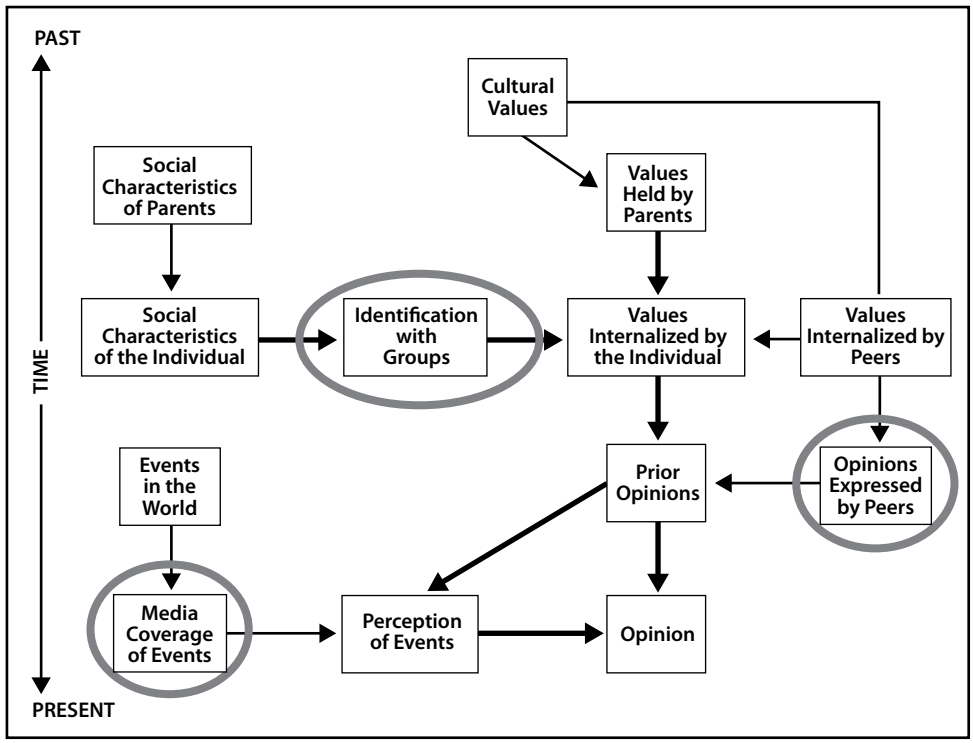


Figure 2. Model of individual opinion formation. (Reproduced by permission from Alan D. Monroe, *Public Opinion in America* [New York: Dodd, Mead, and Co., 1975], 147.)

Figure 3 maps the process of how propaganda can penetrate a network that is not predisposed to the message. This outside network is a group that is ideologically opposed to the group of true believers. The outside network is likely aware of the existing narrative but does not necessarily subscribe to the underlying beliefs that support the narrative.

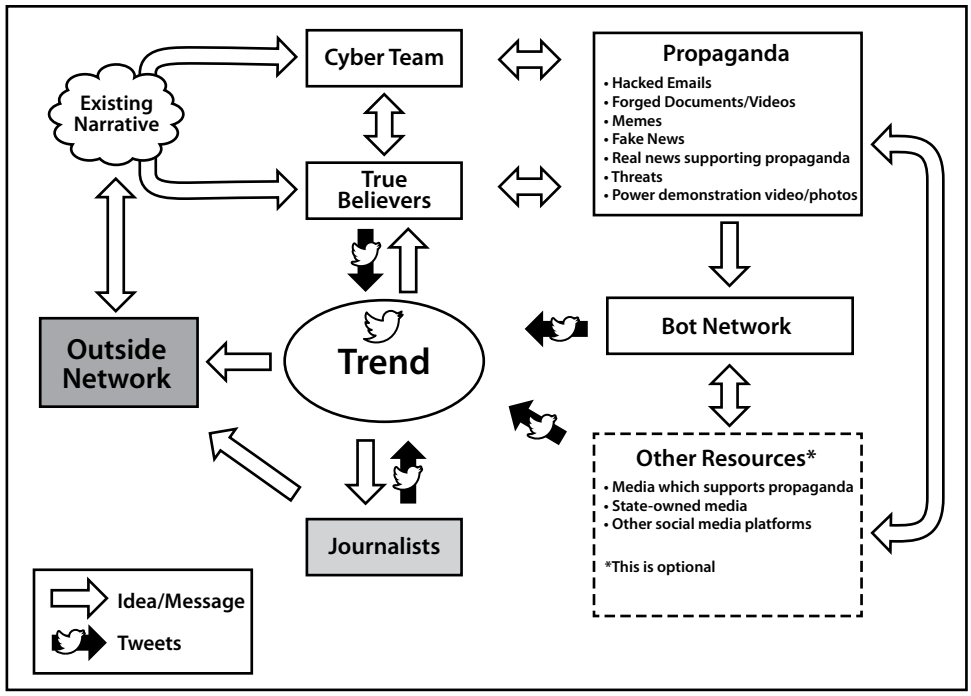


Figure 3. Process map of how propaganda spreads via the trend

Command of the trend enables the contemporary propaganda model, to create a "firehose of information" that permits the insertion of false narratives over time and at all times.[14] Trending items produce the illusion of reality, in some cases even being reported by journalists. Because untruths can spread so quickly now, the internet has created "both deliberate and unwitting propaganda" since the early 1990s through the proliferation of rumors passed as legitimate news.[15] The normalization of these types of rumors over time, combined with the rapidity and volume of new false narratives over social media, opened the door for "fake news."

The availability heuristic and the firehose of disinformation can slowly alter opinions as propaganda crosses networks by way of the trend, but

the amount of influence will likely be minimal unless it comes from a source that a nonbeliever finds trustworthy. An individual may see the propaganda and believe the message is popular because it is trending but still not buy into the message itself. Instead, the individual will likely turn to a trusted source of news to test the validity of the propaganda. Therefore, we must now analyze modern journalism to determine how command of the trend can transform propaganda from fake news to real news.

Social Networks and Social Media

Currently, 72 percent of Americans get digital news primarily from a mobile device, and people now prefer online news sources to print sources by a two-to-one ratio.[16] The news consumer now selects from an abundance of options besides a local newspaper, based on how the consumer perceives the credibility of the resource. As social media usage has become more widespread, users have become ensconced within specific, self-selected groups, which means that news and views are shared nearly exclusively with like-minded users. In network terminology, this group phenomenon is called homophily. More colloquially, it reflects the concept that "birds of a feather flock together." Homophily within social media creates an aura of expertise and trustworthiness where those factors would not normally exist. Along the lines of social networking and propaganda, people are more willing to believe things that fit into their worldview. Once source credibility is established, there is a tendency to accept that source as an expert on other issues as well, even if the issue is unrelated to the area of originally perceived expertise.[17] Ultimately, this "echo chamber" can promote the scenario in which your friend is "just as much a source of insightful analysis on the nuances of U.S. foreign policy towards Iran as regional scholars, arms control experts, or journalists covering the State Department."[18]

If social media facilitates self-reinforcing networks of like-minded users, how can a propaganda message traverse networks where there are no overlapping nodes? This link between networks is only based on that single topic and can be easily severed. Thus, to employ social media effectively as a tool of propaganda, an adversary cannot rely on individual weak links between networks. Instead, an adversary must exploit a feature within the social media platform that enables cross-network data sharing on a massive scale: the trending topics list. Trends are visible to everyone. Regardless of who follows whom on a given social media plat-

form, all users see the topics algorithmically generated by the platform as being the most popular topics at that particular moment. Given this universal and unavoidable visibility, "popular topics contribute to the collective awareness of what is trending and at times can also affect the public agenda of the community."[19] In this manner, a trending topic can bridge the gap between clusters of social networks. A malicious actor can quickly spread propaganda by injecting a narrative onto the trend list.

The combination of networking on social media, propaganda, and reliance on unverifiable online news sources introduces the possibility of completely falsified news stories entering the mainstream of public consciousness. This phenomenon, commonly called fake news, has generated significant criticism from both sides of the American political spectrum, with some labeling any contrary viewpoints fake. In reality, fake news consists of more than just bad headlines, buried ledes, or poorly sourced stories.[20] Fake news is a particular form of propaganda composed of a false story disguised as news. On social media, this becomes particularly dangerous because of the viral spread of sensationalized fake news stories.

A prime example of fake news and social media came from the most shared news stories on Facebook during the 2016 US presidential election. The source of the fake news was a supposedly patriotic American news blog called "End the Fed," a website run by Romanian businessperson Ovidiu Drobota. One story stating that the pope endorsed Donald Trump for president received over one million shares on Facebook alone, not to mention shares on Twitter.[21] Other fake news stories from that site and others received more shares in late 2016 than did traditional mainstream news sources (see figure 4).[22]

It is important to recognize that more people were exposed to those fake news stories than what is reflected in the "shares" data. In some cases, people would just see the story in a Facebook or Twitter feed; in many cases, people actively sought out news from those sources, which are fiction at best and foreign propaganda at worst. Over time, those fake news sources become trusted sources for some people. As people learn to trust those sources, legitimate news outlets become less trustworthy. A 2016 poll by Gallup showed American trust in mass media is at an all-time low.[23]

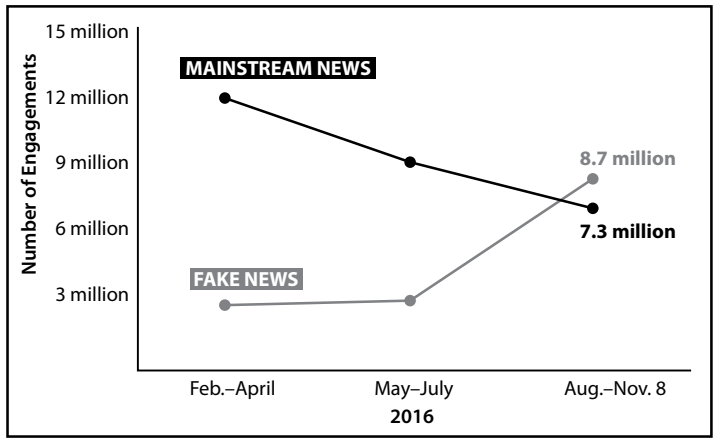


Figure 4. Total Facebook engagements for top 20 election stories

When news is tailorable to one's taste and new stories are popping up around the world every second, mainstream journalists have to change their methods to compete with other sources of news. Therefore, if social media is becoming a source for spreading news and information, journalists will try to keep up by using social media to spread their stories and to acquire information first. According to an Indiana University School of Journalism study, the most common use of social media for journalists is to check for breaking news.[24] As a result, mainstream journalists tend to use tweets as a legitimate source, especially when there is a lack of more valid or confirmed sources.[25] Overreliance on social media for breaking news can become problematic in the midst of an ongoing information operation. If an adversary takes control of a trend on Twitter, the trend is likely to be noticed by mainstream media journalists who may provide legitimacy to a false story—essentially turning fake news into real news. This is the initial setup for how social media became extremely influential via an adversary's propaganda. IS and Russia successfully manipulated social media, particularly Twitter. Although they had different objectives, the tools and techniques were similar. Both foreign actors used command of the trend to spread propaganda that influenced the emotions, opinions, and behavior of US citizens in a manner antithetical to US interests. In essence, IS and Russia hijacked social media through propaganda narratives, true believers, cyber warriors, and a bot network.

Hijacking Social Media—the Case of IS

IS could be considered either a large terrorist organization or a very fragile state with a weak army. However, the perception of IS varies. To believers, IS is a religious caliphate, but much of the rest of the world assumes it is a terrorist group that represents a perversion of faith. IS managed to master the art of manipulation because a single message simultaneously targeted potential allies and foes alike. Its use of social media is a case study in effective propaganda techniques that bolstered recruiting, increased brand recognition, and spread terror with minimal effort. It quickly became the first organization to use social media effectively to achieve its goals.

Although IS may use terrorism as a tactic, the organization behaves differently than any other terrorist organization in the world.[26] The differences are apparent in every aspect, from operations to recruiting to governing. The last factor is the key discriminator. As a descendant of al-Qaeda in Iraq, the group struggled to find its way after the death of leader Abu Musab al-Zarqawi in 2006; under the leadership of Abu Bakr al-Baghdadi the group has established clear lines of authority, taxation and educational systems, trade markets, even policing and a judiciary (covering civil, criminal, and religious complaints).[27] Gaining and holding land is just a part of what IS believes is the destiny of the organization and its followers. Certainly, the desire is to create a caliphate,[28] but its ultimate purpose is more apocalyptic in nature: IS seeks to usher in the end of the world.[29] Its members believe that their actions will bring the forces of the world to attack their caliphate and result in the imminent defeat of the infidel army in the Syrian town of Dabiq, thus triggering the end of the world and the final purge of evil.[30] IS is a revolutionary force with doomsday cult beliefs.[31]

To advance the organization's objectives, IS used messages that served to spread its propaganda on social media to a broad audience that fit within a narrative of strength for the supporter and a narrative of terror for the adversary. In other words, IS cyber warriors combined propaganda with command of the trend to accomplish three things with one message. First, they demonstrated the weakness and incompetence of the international community to fight them online and on the battlefield. Second, they injected terror into the mainstream media. Finally and most importantly, they recruited new fighters to join them on the battlefield in Iraq and Syria—and online.

Islamic State Commanding the Trend

Through a combination of ingenious marketing and cyber mastery, IS bolstered its message around the world. First, the group refined IS branding. The organization projects a very specific image to the world that affects the viewer differently based on beliefs. To a follower, the images that are shared via social media demonstrate strength and power. To the nonfollower, the images are grotesque and horrifying. In other words, no matter what IS puts out in social media the result is a win for the organization because the same message successfully targets two different groups. The amplification of those messages by creating trends on Twitter is guaranteed to get further attention once the tweet falls into the mainstream media. Thus, IS is capable of using relatively small numbers of Twitter users (see table 1) to project an aura of strength.

The method for expanding the reach of a single IS tweet or hashtag involves a network of legitimate retweets combined with bots and unwitting Twitter users. While IS does maintain a strong network of true believers, the numbers are relatively small and spread thinly across the Middle East. Therefore, IS must game the system and rig Twitter for a message to go viral. One high-tech method for creating a bot network was a mobile app called "Dawn of Glad Tidings." The app, designed by IS cyber warriors, provides updates on IS activities and spiritual guidance to the user. When users download the app, they create an account that links to their Twitter account, which then gives the app generous permissions, allowing the app to tweet using that user's account.[32] The app then retweets on behalf of the user when a master account sends an IS-branded tweet.

Over time, the hashtag generates enough tweets to start localized trends. Once the trend surfaces, it is broadcast over trend-monitoring networks, like the Arabic Twitter account @ActiveHashtags.[33] That causes the hashtag to gather more attention across the region and then be retweeted by real followers and other bot accounts. The final step in the process is when the trend goes global.

Table 1. Snapshot of Islamic State Twitter activity

Twitter-related activity studied	Related statistics
Estimated number of overt IS Twitter accounts	46,000
Number of "bot" accounts	6,216
Average number of tweets per day per user	7.3
Average number of followers	1,004
Most common year accounts created	2014
Top languages	Arabic (73%), English (18%), French (6%)
Top locations	"Islamic State," Syria, Iraq, Saudi Arabia[a]

Source: J. M. Berger and Jonathon Morgan, "The ISIS Twitter Census," Brookings Institute, accessed 20 March 2015, https://www.brookings.edu/research/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter/.

[a]Based on location-enabled users and self-defined account locations

Worldwide trends on Twitter have been a boon for IS. Creating and hijacking trends garnered attention for the group that would otherwise have gone unnoticed on social media. The peak of IS trend hijacking was during the World Cup in 2014—as one of the world's most popular sporting events, it was no surprise that the hashtag #WorldCup2014 trended globally on Twitter nonstop during the tournament. At one point though, nearly every tweet under this hashtag had something to do with IS instead of soccer. The network of IS supporters and bot accounts hijacked the trend. Because people were using the hashtag to discuss the matches and advertisers were using the trend for marketing, Twitter struggled to stop the trend and the subsequent IS propaganda effort.

In fact, IS cyber warriors and true believers foiled most of the early attempts by Twitter to stop IS from using their platform to spread propaganda. Twitter's initial reaction was to suspend accounts that violated the user terms of the agreement. The result was creative user names by IS supporters; for example, a user named @jihadISIS42 was created after @jihadISIS41 was suspended, which was set up after @jihadISIS40 was suspended.[34] Each new account demonstrated a deep dedication to the cause that, when combined with the seemingly significant presence on social media, presented the group as dominating social media.

In the case of #WorldCup2014, IS took command of the trend by hijacking, using the opportunity to push recruiting messages, and making

terror threats against the tournament venues in Brazil. Additionally, the co-opted hashtag often directed users to other hashtags in what was ultimately a successful attempt to generate worldwide trends of other IS-related themes. One successful hashtag-creation effort was #StevensHeadinObamasHands, which included memes of President Barack Obama and IS-held American journalist Steven Sotloff. The implication was that the president of the United States did not care to or was powerless to stop the murder of an American citizen. Once again, IS appeared to be disproportionately powerful because of the command of the trend.

Due to the organization's aggressive communications strategy and branding, the IS social media presence consistently outperforms similar jihadist groups in the region that have the same number of, or more, followers.[35] Unlike al-Qaeda, which largely limited its online activity to websites, IS wanted to communicate with a broader audience—it wants to communicate directly to the whole world. In addition to spreading terror threats, the appearance of the group as a powerful state appealed to a group of true believers who turned to IS as new recruits to fight in Iraq and Syria. IS used social media from 2014 to 2016 to demonstrate power, sow fear in the international audience, and recruit the true believers. All the while, they used the true believers following on social media to boost their trends on social media. However, the group currently finds itself altering its modus operandi due to the recent loss of territories in Iraq and Syria, combined with a spate of successful terrorist-style attacks in Europe. The ongoing worry for counterterrorism experts is finally beginning to come to fruition: the recruit staying home to fight instead of joining IS overseas.

After years of maintaining a significant presence on social media, IS is using Twitter less now for official communication. The reasoning is likely twofold. First, the group has lost territory in Iraq and Syria and is adjusting its strategies. Second, Twitter has removed over 600,000 IS-related accounts consisting of bots, cyber warriors, and true believers.[36] Additionally, Twitter has adjusted the program to find terror-related videos, memes, and photos soon after an account from the IS network posts the propaganda. The reasons IS seemed so powerful is that, when viewed through the lens of terrorist groups, it advertised using weaponized social media campaigns. Its intense social media presence, ghastly videos, massive

recruiting, and victories against Iraqi security forces made IS seem disproportionately stronger than it was.

In summation, IS serves as a model for any nonstate group attempting to use social media for cyber coercion. Table 2 summarizes its use of the four requirements to gain command of the trend based on the analysis within this case study.

Table 2. Islamic State case study analysis

Requirement	Example
Propaganda narratives	1. IS is strong; everyone else is weak. 2. True believers should join the cause.
True believers	Muslims believing in the caliphate of al-Baghdadi
Cyber warriors	Propaganda makers, video editors, app programmers, recruiters, spiritual leaders using low- and high-tech tools to advertise IS on social media
Bot network	Unwitting victims of spiritual-guidance app "Dawn of Glad Tidings"

At the same time IS was weaponizing Twitter, Russia was using it to simultaneously cause confusion and garner support for its invasion of Crimea. Soon, Russia's command of the trend would be used to target the United States 2016 presidential election.

Russia: Masters of Manipulation

Russia is no stranger to information warfare. The original technique of Soviet actors was through *aktivnyye meropriyatiya* (active measures) and *dezinformatsiya* (disinformation). According to a 1987 State Department report on Soviet information warfare, "active measures are distinct both from espionage and counterintelligence and from traditional diplomatic and informational activities. The goal of active measures is to influence opinions and/or actions of individuals, governments, and/or publics."[37]

In other words, Soviet agents would try to weave propaganda into an existing narrative to smear countries or individual candidates. Active measures are designed, as retired KGB General Oleg Kalugin once explained, "to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs." Editor, translator, and analyst of Russian Federation trends Michael Weiss says,

"The most common subcategory of active measures is *dezinformatsiya*, or disinformation: feverish, if believable lies cooked up by Moscow Centre and planted in friendly media outlets to make democratic nations look sinister."[38]

The techniques Russia uses today are similar to those they used during the Cold War, but dissemination is more widespread through social media. Recently, the Russian minister of defense acknowledged the existence of their cyber warriors in a speech to the Russian parliament, announcing that Russia formed a new branch of the military consisting of information warfare troops.[39] The Internet Research Agency, as it was called in 2015, now seems to be the information warfare branch he openly admitted to. This army of professional trolls' mission is to fight online. The Russian trolls have a variety of state resources at their disposal, including a vast intelligence network to assist their cyber warriors. The additional tools available to Russia also include RT (Russia Today) and Sputnik, the Kremlin-financed television news networks broadcasting in multiple languages around the world. Before the trolls begin their activities on social media, the cyber warrior hackers first provide hacked information to Wikileaks, which, according to CIA director Mike Pompeo, is a "non-state hostile intelligence service abetted by state actors like Russia."[40] In intelligence terms, WikiLeaks operates as a "cutout" for Russian intelligence operations—a place to spread intelligence information through an outside organization—similar to the Soviets' use of universities to publish propaganda studies in the 1980s.[41] The trolls then take command of the trend to spread the hacked information on Twitter, referencing WikiLeaks and links to RT news within their tweets. These Russian efforts would be impossible without an existing network of American true believers willing to spread the message. The Russian trolls and the bot accounts amplified the voices of the true believers in addition to inserting propaganda into that network. Then, the combined effects of Russian and American Twitter accounts took command of the trend to spread disinformation across networks.

The cyber trolls produced several hoaxes in the United States and Europe, like the Louisiana hoax, according to Adrian Chen in his article "The Agency" in the *New York Times Magazine*.[42] Protests of police departments throughout the United States during the summer of 2015 provided several opportunities to manipulate narratives via social media, and it is likely Russian trolls hijacked some of the Black Lives Matter–related

trends to spread disinformation and accuse journalists of failing to cover important issues.[43] The Russian trolls said the idea was to spread fear, discrediting institutions—especially American media—while making President Obama look powerless and Russian president Vladimir Putin more favorable.[44]

Several hijacked hashtags in 2015 attempted to discredit the Obama administration while spreading racist memes and hoaxes aimed at the African American community. In other words, the Russian trolls seemed to target multiple groups to generate anger and create chaos. One particularly effective Twitter hoax occurred as racial unrest fell on the University of Missouri campus that fall.

#PrayforMizzou

On the night of 11 November 2015, #PrayforMizzou began trending on Twitter.[45] The trend was a result of protests at the University of Missouri campus over racial issues; however, "news" slowly started developing within the hashtag that altered the meaning and soon shot the hashtag to the top of the trend list. The news was that the KKK was marching through Columbia and the Mizzou campus. One user, display name "Jermaine" (@Fanfan1911), warned residents, "The cops are marching with the KKK! They beat up my little brother! Watch out!" Jermaine's tweet included a picture of a black child with a severely bruised face; it was retweeted hundreds of times. Additionally, Jermaine and a handful of other users continued tweeting and retweeting images and stories of KKK and neo-Nazis in Columbia, chastising the media for not covering the racists creating havoc on campus.

Looking at Jermaine's followers, and the followers of his followers, one could observe that the original tweeters all followed and retweeted each other. Those users also seemed to be retweeted automatically by approximately 70 bots. These bots also used the trend-distribution technique, which used all of the trending hashtags at that time within their tweets, not just #PrayforMizzou. Spaced evenly, and with retweets of real people who were observing the Mizzou hashtag, the numbers quickly escalated to thousands of tweets within a few minutes. The plot was smoothly executed and evaded the algorithms Twitter designed to catch bot tweeting, mainly because the Mizzou hashtag was being used outside of that attack. The narrative was set as the trend was hijacked, and the hoax was underway.

The rapidly spreading image of a bruised little boy was generating legitimate outrage across the country and around the world. However, a quick Google image search for "bruised black child" revealed the picture that "Jermaine" attached to the tweet was a picture of an African American child who was beaten by police in Ohio over one year earlier. The image and the narrative were part of a larger plot to spread fear and distrust. It worked.

The University of Missouri student body president tweeted a warning to stay off the streets and lock doors because "KKK members were confirmed on campus." National news networks broke their coverage to get a local feed from camera crews roaming Columbia and the campus looking for signs of violence. As journalists continued to search for signs of Klan members, anchors read tweets describing shootings, stabbings, and cross burnings. In the end, the stories were all false.

Shortly after the disinformation campaign at Mizzou, @Fanfan1911 changed his display name from Jermaine to "FanFan" and the profile picture of a young black male changed to the image of a German iron cross. The next few months, FanFan's tweets were all in German and consisted of spreading rumors about Syrian refugees. Russian active measures in Europe around this time were widely reported, and the account that previously tweeted disinformation regarding Mizzou now focused on messages that were anti-Islamic, anti–European Union, and anti-German Chancellor Angela Merkel. His tweets reached a crescendo after reports of women being raped on New Year's Eve 2016. Some of the reports were false, including a high-profile case of a 13-year-old ethnic-Russian girl living in Berlin who falsely claimed that she was abducted and raped by refugees.[46] Once again, Russian propaganda dominated the narrative.[47] Similar to previous disinformation campaigns on Twitter, the Russians trolls were able to spread the information because of an underlying fear and an existing narrative that they were able to exploit. The trolls used trend-hijacking techniques in concurrence with reporting by Russian state-funded television network Russia Today. To attempt to generate more attention to the Russian anti-Merkel narrative in European media, Russian foreign minister Sergey Lavrov accused German authorities of a "politically correct cover-up" in the case of the Russian teen.[48] Because of the Russian propaganda push, the anti-immigration narrative began spreading across traditional European media.[49] In fact, a magazine in

Poland devoted an entire issue to the topic of Muslim immigration with a disturbing cover photo entitled "Islamic Rape of Europe."[50]

In addition to the German tweets, FanFan began tweeting in English again in the spring of 2016. His tweets and the tweets of other Russian trolls were spreading in America. The narrative they spread was developing a symbiotic relationship with American right-wing news organizations like Breitbart and its followers on social media—a group of true believers in the Russian propaganda narrative.

Additionally, the troll network already seeded various social media platforms with pages designed for spreading disinformation.[51] Seemingly patriotic American Facebook pages linked articles to RT, legitimate American news sources advocating a right-leaning perspective, Breitbart, right-wing conspiracy sites like InfoWars, and non-factual "news" sites like the Conservative Tribune and Gateway Pundit. The Facebook pages also linked to Russia-run sites with nothing but false news stories. Based on anti-Obama sentiment, the Facebook pages were popular among conservative users but not getting broad exposure. Before 2016, Russian active measures were also used in European elections, most notably the "Brexit" campaign. One European expert on Russia quoted in the *Atlantic* article "War Goes Viral" summarized Putin's intent as "not to make you love Putin"; instead "the aim is to make you disbelieve anything. A disbelieving, fragile, unconscious audience is much easier to manipulate."[52] Active measures enable manipulation. Smearing political candidates, hacking, the spread of disinformation, and hoaxes all contribute to a breakdown of public trust in institutions.

As the 2016 US presidential campaign began in earnest, much of the online animosity was now directed at Obama's potential successor: Hillary Clinton. She became a rallying cry for Trump supporters and a force-multiplying tool for the Russian trolls.

Influencing the 2016 Presidential Election

According to the Office of Director of National Intelligence (ODNI) Report on Russian Influence during the 2016 presidential election, "Moscow's influence campaign followed a messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state funded media, third-party intermediaries, and paid social media users, or 'trolls.' "[53] In the case of the 2016 election, Russian propaganda easily meshed with right-wing

networks known as the "alt-right" and also with supporters of Senator Bernie Sanders in the left wing of the Democratic Party. Hillary Clinton had been a target of conservative groups since she first came into the national spotlight as first lady in the 1990s.[54] Thus, groups on the left and right presented strong opposition to her candidacy in 2016, which meant Russian trolls already had a narrative to build upon and a network of true believers on social media to spread their propaganda.

In a September 2016 speech, Clinton described half of candidate Trump's supporters as "deplorables." She went on to say that the other half of Trump's supporters were just people who felt the system had left them behind, who needed support and empathy. Clearly, she was not referring to all of Trump's supporters as deplorable, but the narrative quickly changed after social media users began referring to themselves as "Deplorable" in their screen names.

Before the "basket of deplorables" comment, the trolls primarily used an algorithm to rapidly respond to a tweet from Donald Trump. Those tweets were prominently displayed directly under Trump's tweet if a user clicked on the original. Those users became powerful voices with large followings; Trump himself frequently retweeted many of those users.[55] However, after the Clinton speech, a "people search" on Twitter for "deplorable" was all one needed to suddenly gain a network of followers numbering between 3,000 and 70,000. Once again, FanFan's name changed—this time to "Deplorable Lucy"—and the profile picture became a white, middle-aged female with a Trump logo at the bottom of the picture. The FanFan follower count went from just over 1,000 to 11,000 within a few days. His original network from the Mizzou and European campaigns changed as well: tracing his follower trail again led to the same groups of people in the same network, and they were all now defined by the "Deplorable" brand. In short, they were now completely in unison with a vast network of other Russian trolls, actual American citizens, and bot accounts from both countries on Twitter. With a large network consisting of Russian trolls, true believers, and bots, it suddenly became easier to get topics trending with a barrage of tweets. The Russian trolls could employ the previously used tactics of bot tweets and hashtag hijacking, but now they had the capability to create trends.

Besides creating trends, the trolls could relay strategy under the radar using Twitter. That is to say, a message could be delivered in the form of a picture that did not include any words. The lack of words would

spread the message to the followers in a timeline, but retweets would not develop any trends—only that network of followers or someone actively observing the network saw the messages. Often, anonymous users discussed the tactics behind the trend creation on the social media site 4Chan or on the bulletin board called "/pol/" and subsequently coordinated the trend within the Deplorable Network on Twitter. The most effective trends derived from this strategy came in the days following the release of the "Access Hollywood" tape from 2005 in which Trump had made vulgar remarks.[56] The Deplorable Network distributed the corresponding strategy throughout the network to drown out negative attention to Trump on Twitter. Coinciding with the implementation of the strategy to mask anti-Trump comments on Twitter, WikiLeaks began releasing Clinton campaign chairman John Podesta's stolen emails.[57] The emails themselves revealed nothing truly controversial, but the narrative that the trending hashtag created was powerful. First, the issue of hacked emails developed into a narrative conflating Podesta's emails to the issue of Clinton's use of a private email server while she was secretary of state. The Clinton server was likely never hacked, but the problem of email loomed over her candidacy.

Secondly, the Podesta email narrative took routine issues and made them seem scandalous. The most common theme: bring discredit to the mainstream media. Podesta, like any campaign manager in modern politics, communicated with members of the press. Emails communicating with reporters were distributed via trending tweets with links to fake news websites. The fake news distorted the stolen emails into conspiracies of media "rigging" of the election to support Hillary Clinton. The corruption narrative also plagued the Democratic National Committee (DNC), which experienced a hack earlier in the year, by Russian sources and revealed by WikiLeaks.[58]

A month after the election, a man drove from his home in North Carolina to Washington, DC, to uncover the truth behind another news story he read online. He arrived at Comet Ping-Pong, a pizza restaurant, with an AR-15, prepared to free children from an underground child sex trafficking ring in the restaurant. After searching the store, he found no children. The story was a hoax. One of the emails stolen from John Podesta was an invitation to a party at the home of a friend that promised good pizza from Comet Ping Pong and a pool to entertain the kids. Fake news sites reported the email as code for a pedophilic sex party; it

was widely distributed via the trending #PodestaEmail hashtag and an associated new hashtag, #PizzaGate.

The #PizzaGate hoax, along with all of the other false and quasi-false narratives, became common within right-wing media as another indication of the immorality of Clinton and her staff. Often, the mainstream media would latch onto a story with unsavory backgrounds and false pretenses, thus giving more credibility to all of the fake news; however, the narrative from the #PizzaGate hoax followed the common propaganda narrative that the media was trying to cover up the truth and that the government failed to investigate the crimes. Ultimately, that is what drove the man to inquire into the fake news for himself.[59]

Finally, the stolen emails went beyond sharing on social media. The trend became so sensational that traditional media outlets chose to cover the Podesta email story, which gave credibility to the fake news and the associated online conspiracy theories promulgated by the Deplorable Network. The WikiLeaks release of the Podesta emails was the peak of Russian command of the trend during the 2016 election. Nearly every day #PodestaEmail trended as a new batch of supposedly scandalous hacked emails made their way into the mainstream press.

By analyzing the followers of a suspected Russian troll, a picture emerges regarding the structure of the network that was active during the 2016 election. The core group in the Deplorable Network consisted of Russian trolls and popular American right-wing accounts like Jack Posobiec, Mike Cernovich, and InfoWars editor Paul Joseph Watson. The Network also consisted of two bot accounts while the remaining nodes are individual accounts likely consisting of human-managed accounts. In total, the Deplorable Network was approximately 200,000 Twitter accounts consisting of Russian trolls, true believers, and bots. Based on my analysis, the bot network appeared to be between 16,000 and 34,000 accounts.[60] The cohesiveness of the group indicates how a coordinated effort can create a trend in a way that a less cohesive network could not accomplish. To conduct cyberattacks using social media as information warfare, an organization must have a vast network of bot accounts to take command of the trend. With unknown factors like the impact of fake news, the true results of the Russian influence operation will likely never be known. As Ellul said, experiments undertaken to gauge the effectiveness of propaganda will never work because the tests "cannot reproduce the real propaganda situation."[61] The concept itself

is marred by the fact that much of the social media support Trump received was through real American true believers tweeting. However, two numbers will stand out from the 2016 election: 2.8 million and 80,000. Hillary Clinton won the popular vote by 2.8 million votes, and Donald Trump won the electoral vote via a combination of just over 80,000 votes in three key states. One could easily make the case—as many on the left have done—that Clinton lost because of the Russian influence.[62] Conversely, one could also argue she was destined to lose because of a botched campaign combined with a growing sense of disenchantment with the American political system. However, one cannot dispute the fact that Russia launched a massive cyberwarfare campaign to influence the 2016 presidential election.[63]

For the most part, the Russian trolls became savvier with their techniques as they adapted to the influence operation in the United States. However, some users, like FanFan, were sloppy with their tradecraft and were obvious to anyone monitoring. The trolls were occasionally sloppy with their IP address locations as well. Following the first presidential debate, the #TrumpWon hashtag quickly became the number one trend globally. Using the TrendMap application, one quickly noticed that the worldwide hashtag seemed to originate in Saint Petersburg, Russia. Russian trolls gave obvious support to Donald Trump and proved that using social media could create chaos on a massive scale, discredit any politician, and divide American society.

Adrian Chen, the *New York Times* reporter who originally uncovered the troll network in Saint Petersburg in 2015, went back to Russia in the summer of 2016. Russian activists he interviewed claimed that the purpose of the trolls "was not to brainwash readers, but to overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space."[64] The troll farm used similar techniques to drown out anti-Putin trends on Russian social media in addition to pumping out disinformation to the United States.

A Congressional Research Service Study summarized the Russian troll operation succinctly in a January 2017 report: "Cyber tools were also used [by Russia] to create psychological effects in the American population. The likely collateral effects of these activities include compromising the fidelity of information, sowing discord and doubt in the

American public about the validity of intelligence community reports, and prompting questions about the democratic process itself."[65]

For Russia, information warfare is a specialized type of war, and modern tools make social media the weapon. According to a former Obama administration senior official, Russians regard the information sphere as a domain of warfare on a sliding scale of conflict that always exists between the US and Russia.[66] This perspective was on display during a Russian national security conference "Infoforum 2016." Andrey Krutskih, a senior Kremlin advisor, compared Russia's information warfare to a nuclear bomb, which would "allow Russia to talk to Americans as equals," in the same way that Soviet testing of the atomic bomb did in 1949.[67]

Table 3. Russia case study analysis in 2016 election

Types	Examples
Propaganda narratives	• Anything discrediting to Hillary Clinton • News media hides information • Politicians are rigging the system • Global elite trying to destroy the world • Globalism is taking jobs and destroying cultures • Refugees are terrorists • Russian foreign policy is strong on antiterrorism • Democrats and some Republicans want WWIII with Russia
True believers	Alt-right, some Bernie Sanders supporters, followers of InfoWars and Breitbart, 4Chan and /pol/ users.
Cyber warriors	Hackers and professional trolls
Bot network	Large, sophisticated network that leveraged cyber warriors and true believer accounts to create the "Deplorable Network."

From 2015 to 2016, Russian trolling modus operandi took a logical path from small stories designed to create panic and sow seeds of doubt to a social media machine that IS could only imagine. In warfare strategy, narrative manipulation through social media cyber operations is the current embodiment of taking the fight directly to the people. The 2016 election proved that using social media to influence political outcomes, as opposed to violence or Cold War–like posturing, is a highly effective strategy in modern information warfare—a strategy that will likely continue as technology continues to develop and adapt to the ever-growing social media landscape as more actors gain the ability to take command of the trend.

The Future of Weaponized Social Media

Smear campaigns have been around since the beginning of politics, but this article illustrated novel techniques recently employed by a terrorist group and foreign state actor, with each attack gaining popularity and credibility after trending on Twitter. The attacks, often under the guise of a "whistleblower" campaign, make routine political actions seem scandalous. Additionally, WikiLeaks advertises that it has never published anything requiring retraction because everything it posts is supposedly authentic stolen material. Just like the Podesta email releases, several politicians and business leaders around the world have fallen victim to this type of attack.

Recall the 2015 North Korean hacking of Sony Studios. Lost in the explosive nature of the hacking story is that the fallout at the company was not because of the hacking itself but from the release of embarrassing emails from Sony senior management, as well as the salaries of every employee at Sony. The uproar over the content of the emails dominated social media, often fed by salacious stories like the RT headline: "Leaked Sony emails exhibit wealthy elite's maneuvering to get child into Ivy League school." Ultimately, Sony fired a senior executive because of the content of her emails.[68]

In another example from May 2017, nine gigabytes of email stolen from French presidential candidate Emmanuel Macron's campaign were released online and verified by WikiLeaks. Subsequently, the hashtag #MacronLeaks trended to number one worldwide. It was an influence operation resembling the #PodestaEmail campaign with a supporting cast of some of the same actors. During the weeks preceding the French election, many accounts within the Deplorable Network changed their names to support Macron's opponent, Marine LePen. These accounts mostly tweet in English and still engage in American political topics as well as French issues.[69] Some of the accounts also tweet in French, and a new network of French-tweeting bot accounts uses the same methods as the Deplorable Network to take command of the trend.

In his book *Out of the Mountains*, David Kilcullen describes a future comprising large, coastal urban areas filled with potential threats, all connected.[70] The implications of his prediction are twofold. First, networks of malicious nonstate actors can band together to hijack social media using a template similar to IS. Although these groups may not have the power to create global trends, they can certainly create chaos

with smaller numbers by hijacking trends and creating local trends. With minimal resources, a small group can create a bot network to amplify its message. Second, scores of people with exposure to social media are vulnerable to online propaganda efforts. In this regard, state actors can use the Russian playbook.

Russia will likely continue to dominate this new battlespace. It has intelligence assets, hackers, cyber warrior trolls, massive bot networks, state-owned news networks with global reach, and established networks within the countries Russia seeks to attack via social media. Most importantly, the Russians have a history of spreading propaganda. After the 2016 elections in the United States, Russian trolls again worked toward influencing European elections. Currently, Russian trolls are active in France, the Balkans, and the Czech Republic using active measures and coercive social media messages.[71] It is clear that other countries are attempting to build capabilities to match the Russian cyber troll influence.

Already, Turkey, Iran, and Venezuela are noted as having bot networks and cyber warriors similar to Russian trolls.[72] With these other states, a popular use for the trolls in the social media battlespace is to stoke nationalism and control the narrative within their own borders. For example, the fake Twitter followers of Venezuelan president Nicolás Maduro number so many that he is now the "third-most-retweeted public figure in the world, behind only the king of Saudi Arabia and the pope."[73]

With a large enough bot network, states can also control messages outside of social media using similar techniques. Manipulating search engines is called "search engine optimization," which uses bot accounts to increase the number of clicks to a particular web page after performing a search. The search engine algorithm then prioritizes that page in response to subsequent searches using the same keyword. A Google search for "ODNI Report" is illustrative: in March 2017, the top Google results were RT articles lambasting the intelligence assessment that named the Russian government as the perpetrators behind the 2016 election interference.

Techniques like search engine optimization and command of the trend will become common in future wars to sow discord and spread false information, with the aim of causing the other side to change its course of action. These online weapons should frighten every leader in a democracy. Perhaps most frightening is the Oxford Internet Institute Unit for Propaganda discovery that "hundreds of thousands of 'sleeper bots' exist

on Twitter."[74] These bots are accounts that are active but have not yet started tweeting. Researchers do not know who owns the accounts or what will trigger them. The ease of use and large numbers of active bots and sleeper bots indicate a high likelihood of social media continuing to be used for propaganda, especially as more and more state and nonstate organizations realize the impact they can make on an adversary.

Thus far, the United States response has been relatively weak. For one, the US government does not prioritize information operations the way it once did during the Cold War. When President Eisenhower started the United States Information Agency (USIA), the objective was to compete with Soviet propaganda around the world. The mission statement of USIA clarified its role: "The purpose of the United States Information Agency shall be to submit evidence to peoples of other nations by means of communication techniques that the objectives and policies of the United States are in harmony with and will advance their legitimate aspirations for freedom, progress, and peace."[75]

Knowing what we know now about Russian disinformation active measures, USIA was never truly equipped to fight an information war. The agency became a public diplomacy platform with a positive message rather than a Soviet-style campaign of negative smear tactics. Accordingly, several questions arose: should USIA spread propaganda? Should it seek out and attempt to remove negative publicity about the US? Should it slander opponents? Most importantly: should it do any or all of these things when the American public could be influenced by a message intended for an international audience?[76]

Those problems persist today because the government lacks a centralized information authority since the mission of USIA was relegated to the Department of State. Several failed attempts to counter IS on Twitter show the US government's weakness when trying to use social media as a weapon. One example is the Center for Strategic Counterterrorism Communications, created in 2010, which started the program "Think Again, Turn Away." The State department awarded a $575,046 contract to a Virginia-based consulting firm to manage the project.[77] The intent was to curb the appeal of IS by creating a counternarrative to the IS message on social media. Unfortunately, the Twitter campaign had undesirable consequences after the account sent tweets arguing the finer points of the Islamic faith with IS sympathizers. Rita Katz best summarized the failure: "In order to counter a problem, one must first study it

before adopting a solution. Had the people behind 'Think Again, Turn Away' understood jihadists' mindsets and reasons for their behavior, they would have known that their project of counter-messaging would not only be a waste of taxpayer money but ultimately be counterproductive."[78]

In the end, the "Think Again, Turn Away" campaign was almost comical as it could not communicate effectively with any audience and severely discounted the importance of its message. Jacques Ellul noted that democracies were prone to having problems with outward communication through propaganda. Because democracies rely on presenting an image of fairness and truth, "propaganda made by democracies is ineffective, paralyzed, mediocre."[79] The United States was ill equipped to combat Soviet active measures during the Cold War, and it remains unable to compete using social media as an influence operation.

Unfortunately, countering Russian influence operations has taken a partisan slant within the United States. Many downplay the Russian role in the 2016 election while others appear to be so blinded by the Russian operation that they cannot see the underlying conditions that allowed for the spread of that narrative in the first place.[80] With the two parties unable to reach a consensus on what happened or the impact of the operation, they fail to realize that as technology improves and proliferates around the world, disinformation campaigns and influence operations will become the norm. The attack in a future information war could be toward either political party and come from any of the several countries attempting to build an online army in the mold of Russia's trolls and bot network.

Conclusion

In the 1987 book *Truth Twisters*, Richard Deacon laments the future of independent thinking, as computers "could become the most dangerous hypnotic influence in the future. . . . [T]he effect of a reliance on computerology, of allowing oneself to be manipulated and controlled by it, is certainly hypnotic in that the mind allows itself to accept whatever the computer tells it."[81] He believed that such technology could lead one to commit treason without realizing any manipulation. Propaganda is a powerful tool, and, used effectively, it has been proven to manipulate populations on a massive scale. Using social media to take command of the trend makes the spread of propaganda easier than ever before for both state and nonstate actors.

Fortunately, social media companies are taking steps to combat malicious use. Facebook has been at the forefront of tech companies taking action to increase awareness of fake news and provide a process for removing the links from the website.[82] Also, although Facebook trends are less important to information warfare than Twitter trends, the website has taken measures to ensure that humans are involved in making the trends list. Furthermore, Twitter has started discreetly removing unsavory trends within minutes of their rise in popularity. However, adversaries adapt, and Twitter trolls have attempted to regain command of the trend by misspelling a previous trend once it is taken out of circulation. Still, even if the misspelled word regains a spot on the trend list, the message is diminished.

The measures enacted by Facebook and Twitter are important for preventing future wars in the information domain. However, Twitter will also continue to have problems with trend hijacking and bot networks. As demonstrated by #PrayforMizzou and #WorldCup2014, real events happening around the world will maintain popularity as well-intending users want to talk about the issues. In reality, removing the trends function could end the use of social media as a weapon, but doing so could also devalue the usability of Twitter. Rooting out bot accounts would have an equal effect since that would nearly eliminate the possibility of trend creation. Unfortunately, that would have an adverse impact on advertising firms that rely on Twitter to generate revenue for their products.

With social media companies balancing the interests of their businesses and the betterment of society, other institutions must respond to the malicious use of social media. In particular, the credibility of our press has been put into question by social media influence campaigns—those groups should respond accordingly. For instance, news outlets should adopt social media policies for their employees that encourage the use of social media but discourage them from relying on Twitter as a source. This will require a culture shift within the press and fortunately has gathered significant attention at universities researching the media's role in the influence operation. It is worth noting that the French press did not cover the content of the Macron leaks; instead, the journalists covered the hacking and influence operation without giving any credibility to the leaked information.

Finally, our elected officials must move past the partisan divide of Russian influence in the 2016 election. This involves two things: first, both parties must recognize what happened—neither minimizing nor overplaying Russian active measures. Second, and most importantly, politicians must commit to not using active measures to their benefit. Certainly, the appeal of free negative advertising will make any politician think twice about using disinformation, but the reality of a foreign influence operation damages more than just the other party, it damages our democratic ideals. Senator John McCain summarized this sentiment well at a CNN Town Hall: "Have no doubt, what the Russians tried to do to our election could have destroyed democracy. That's why we've got to pay . . . a lot more attention to the Russians."[83]

This was not the cyber war we were promised. Predictions of a catastrophic cyberattack dominated policy discussion, but few realized that social media could be used as a weapon against the minds of the population. IS and Russia are models for this future war that uses social media to directly influence people. As technology improves, techniques are refined, and internet connectivity continues to proliferate around the world, this saying will ring true: He who controls the trend will control the narrative—and, ultimately, the narrative controls the will of the people. SSQ

Notes

1. Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, 11 October 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?mcubz=0/.

2. Jeremy Scott-Joynt, "What Myspace Means to Murdoch," BBC News Analysis, 19 July 2005, http://news.bbc.co.uk/2/hi/business/4697671.stm.

3. Sitaram Asur, Bernardo A. Huberman, Gabor Szabo, and Chunyan Wang, "Trends in Social Media: Persistence and Decay" (unpublished manuscript, submitted to Cornell University Library arXiv 7 February 2011), 1, https://arxiv.org/abs/1102.1402?context=physics.

4. "Blog" is short for "web log." A blog is a way to share your thoughts via the internet. A microblog is a blog with a character limit to the text.

5. Rani Molla, "Social Studies: Twitter vs. Facebook," *Bloomberg Gadfly*, 12 February 2016, https://www.bloomberg.com/gadfly/articles/2016-02-12/social-studies-comparing-twitter-with-facebook-in-charts.

6. Carole Cadwalladr, "Robert Mercer: The Big Data Billionaire Waging War on the Mainstream Media," *Guardian*, 26 February 2017, https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage.

7. Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation* (Washington, DC: Woodrow Wilson Center Press, 2015), 138.

8. Alex Lubben, "Twitter's Users Are 15 Percent Robot, but That's Not Necessarily a Bad Thing," VICE News, 12 March 2017, https://news.vice.com/story/twitters-users-are-15-percent-robot-but-thats-not-necessarily-a-bad-thing.

9. Jacques Ellul, *Propaganda: The Formation of Men's Attitudes* (New York: Knopf, 1965), 6.

10. Eric Hoffer, *The True Believer: Thoughts on the Nature of Mass Movements* (New York: Harper and Row, 1951), 105.

11. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), 132.

12. Ellul, 85.

13. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 87.

14. Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model*, RAND Report PE-198-OSD (Santa Monica, CA: RAND, 2016), 4, https://www.rand.org/pubs/perspectives/PE198.html.

15. Garth Jowett and Victoria O'Donnell, *Propaganda & Persuasion*, 5th ed. (Thousand Oaks, CA: SAGE, 2012), 159.

16. Katerina Eva Matsa and Kristine Lu, "10 Facts about the Changing Digital News Landscape," Pew Research Center, 14 September 2016, http://www.pewresearch.org/fact-tank/2016/09/14/facts-about-the-changing-digital-news-landscape/.

17. Jowett and O'Donnell, *Propaganda & Persuasion*, 300.

18. Tom Hashemi, "The Business of Ideas Is in Trouble: Re-injecting Facts into a Post-truth World," *War on the Rocks*, 9 December 2016, https://warontherocks.com/2016/12/the-business-of-ideas-is-in-trouble-re-injecting-facts-into-a-post-truth-world/.

19. Asur, Huberman, Szabo, and Wang, "Trends in Social Media," 1.

20. *Merriam-Webster Dictionary Online*, s.v. "lede," accessed 10 October 2017, https://www.merriam-webster.com/dictionary/lede. "The introductory section of a news story that is intended to entice the reader to read the full story."

21. Tess Townsend, "The Bizarre Truth behind the Biggest Pro-Trump Facebook Hoaxes," Inc.com, 21 November 2016, https://www.inc.com/tess-townsend/ending-fed-trump-facebook.html.

22. Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook," BuzzFeed News, 16 November 2016, https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.qwWdA0G8G#.fcEv1Qono.

23. Art Swift, "Americans' Trust in Mass Media Sinks to New Low," Gallup, 14 September 2016, http://news.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx.

24. Andrea Peterson, "Three Charts that Explain how U.S. Journalists Use Social Media," *Washington Post*, 6 May 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/05/06/three-charts-that-explain-how-u-s-journalists-use-social-media/?utm_term=.9cdd82cb8fa7.

25. Weimann, *Terrorism in Cyberspace*, 138.

26. Audrey Kurth Cronin, "ISIS Is Not a Terrorist Group," *Foreign Policy* (March/April 2015), https://www.foreignaffairs.com/articles/middle-east/isis-not-terrorist-group.

27. Stephen M. Walt, "ISIS as Revolutionary State," *Foreign Policy* (November/December 2015): 42, https://www.belfercenter.org/publication/isis-revolutionary-state.

28. Caliphate is defined as "a form of Islamic government led by a—a person considered a political and religious successor to the Islamic prophet, Muhammad, and a leader of the entire Muslim community. Source: Wadad Kadi and Aram A. Shahin, "Caliph, caliphate," in *The Princeton Encyclopedia of Islamic Political Thought*, ed. Gerhard Bowering, Patricia Crone, Wadad

Kadi, Devin J. Stewart, Muhammad Qasim Zaman, and Mahan Mirza (Princeton, NJ: Princeton University Press, 2013), 81–86, http://www.jstor.org/stable/j.ctt1r2g6m.8.

29. Graeme Wood, "What ISIS Really Wants," *Atlantic*, March 2015, 3, https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/.

30. Dabiq is also the name of the ISIS magazine, which is available electronically and spread via social media.

31. Walt, "ISIS as Revolutionary State," 43.

32. J. M. Berger, "How ISIS Games Twitter," *Atlantic*, 16 June 2014, https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

33. Ibid.

34. "Terrorist Use of Social Media: Policy and Legal Challenges," roundtable forum (Washington, DC: Council on Foreign Relations, 14 October 2015).

35. Berger, "How ISIS Games Twitter."

36. Carleton English, "Twitter Continues to Wage its Own War against ISIS," *New York Post*, 21 March 2017, http://nypost.com/2017/03/21/twitter-continues-to-wage-its-own-war-against-isis/.

37. United States Department of State, report, *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–87* (Washington, DC: Bureau of Public Affairs, 1987), viii.

38. Natasha Bertrand, "It Looks Like Russia Hired Internet Trolls to Pose as Pro-Trump Americans," *Business Insider*, 27 July 2016, http://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7.

39. Vladimir Isachenkov, "Russia Military Acknowledges New Branch: Info Warfare Troops," AP News, 22 February 2017, https://www.apnews.com/8b7532462dd0495d9f756c9ae7d2ff3c.

40. Richard Gonzalez, "CIA Director Pompeo Denounces WikiLeaks as 'Hostile Intelligence Service,' " NPR, 23 April 2017, http://www.npr.org/sections/thetwo-way/2017/04/13/523849965/cia-director-pompeo-denounces-wikileaks-as-hostile-intelligence-service.

41. Malcolm Nance, *The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election* (New York: Skyhorse Publishing, 2016), Kindle edition, 1,839.

42. Adrian Chen, "The Agency," *New York Times Magazine*, 2 June 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html. On 11 September 2014, the small town of St. Mary Parish, Louisiana, was thrown briefly into a panic when residents began hearing reports through text, social media, and on local television stations that a nearby chemical plant fire was spreading toxic fumes that would soon endanger the whole town. The entire narrative was based on falsified—but very real looking—online news stories, hashtag manipulation, and mass texts (SMS) to various numbers with the local area code and dialing prefix. The actual source for the news was not the chemical factory; it was a nondescript building in St. Petersburg, Russia, where an army of online cyber-warrior trolls seeks to distribute false information.

43. Statement of Clint Watts, Foreign Policy Research Institute fellow, in "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," testimony before the Senate Intelligence Committee, 115th Cong., 1st sess., 30 March 2017, https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf.

44. Chen, "The Agency."

45. Because of the Adrian Chen article, I observed particular tweeting patterns of certain individuals involved in a hoax on the campus of the University of Missouri that seemed to match the methods of the Russian trolls interviewed by Chen. I mention only one particular user in this article, but I also monitored a dozen or so accounts that contributed to that hoax. Each account followed a pattern that also happened to align with noted Russian influence operations in Europe and eventually in the US presidential election. I describe that transition in the article. From those accounts, I built a database of suspected Russian bot accounts to build a network map. The

Mizzou hoax was a trend hijacking effort launched by actors who later proved to match the Russian modus operandi of using cyber trolls originally observed by Adrian Chen and confirmed by the Office of the Director of National Intelligence (ODNI) report and Foreign Policy Research Institute fellow Clint Watts in his testimony before the Senate Intelligence Committee (note 43).

46. Nadine Schmidt and Tim Hume, "Berlin Teen Admits Fabricating Migrant Gang-Rape Story, Official Says," CNN, 1 February 2016, http://www.cnn.com/2016/02/01/europe/germany-teen-migrant-rape-false/index.html.

47. Judy Dempsey, "Russia's Manipulation of Germany's Refugee Problems," Carnegie Europe, 28 January 2016, http://carnegieeurope.eu/strategiceurope/?fa=62611.

48. Schmidt and Hume, "Berlin Teen Admits Fabricating Migrant Gang-Rape Story."

49. Barbara Tasch, "'The Aim Is to Weaken the West': The Inside Story of How Russian Propagandists Are Waging War on Europe," *Business Insider*, 2 February 2017, http://www.businessinsider.com/russia-propaganda-campaign-weakening-europe-2017-1?r=UK&IR=T.

50. Harriet Sherwood, "Polish Magazine's 'Islamic Rape of Europe' Cover Sparks Outrage," 18 February 2016, https://www.theguardian.com/world/2016/feb/18/polish-magazines-islamic-of-europe-cover-sparks-outrage.

51. Chen, "The Agency."

52. Robinson Meyer, "War Goes Viral: How Social Media Is Being Weaponized across the World," *Atlantic*, 18 October 2016, https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/.

53. Office of the Director of National Intelligence (ODNI), Intelligence Community Assessment Report, *Assessing Russian Activities and Intentions in Recent US Elections*, 6 January 2017, ii, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

54. Hanna Rosin, "Among the Hillary Haters," *Atlantic*, 1 March 2015, 63, https://www.theatlantic.com/magazine/archive/2015/03/among-the-hillary-haters/384976/.

55. K. Thor Jensen, "Inside Donald Trump's Twitter-Bot Fan Club," *New York Magazine*, 15 June 2016, http://nymag.com/selectall/2016/06/inside-donald-trumps-twitter-bot-fan-club.html.

56. David A. Farenthold, "Trump Recorded Having Extremely Lewd Conversation about Women in 2005," *Washington Post*, 8 October 2016, https://www.washingtonpost.com/politics/trump-recorded-having-extremely-lewd-conversation-about-women-in-2005/2016/10/07/3b9ce776-8cb4-11e6-bf8a-3d26847eeed4_story.html.

57. "The Podesta Emails," Politico LiveBlog, accessed 6 December 2016, http://www.politico.com/live-blog-updates/2016/10/john-podesta-hillary-clinton-emails-wikileaks-000011.

58. ODNI Report, 2.

59. Faiz Siddiqui and Susan Svrluga, "N.C. Man Told Police He Went to D.C. Pizzeria with Gun to Investigate Conspiracy Theory," *Washington Post*, 5 December 2017, https://www.washingtonpost.com/news/local/wp/2016/12/04/d-c-police-respond-to-report-of-a-man-with-a-gun-at-comet-ping-pong-restaurant/?utm_term=.c33057f66007.

60. This count is based on analysis of the followers of followers of suspected troll accounts and bots. The study was conducted 15 March 2016. The number of accounts appears to have reduced dramatically since May, following the French election, implying that Twitter suspended some of the accounts. Unfortunately, software limitations prevent this analysis from being more accurate. Additionally, it is nearly impossible to derive the exact number of Russian accounts from that network using my available resources.

61. Ellul, *Propaganda*, 6.

62. Many on the left have mischaracterized the attack as "Russian hacking of the election," which has in turn conflated the issue of the John Podesta email theft with a hacking of the

actual election systems. To be clear: there is no evidence of any sort of hack on any ballot-counting systems, only evidence outlined in this paper of two hacks (Democratic National Committee and Podesta) combined with an influence/information operation.

63. ODNI Report, 1.

64. Adrian Chen, "The Real Paranoia-Inducing Purpose of Russian Hacks," *New Yorker*, 27 July 2016, https://www.newyorker.com/news/news-desk/the-real-paranoia-inducing-purpose-of-russian-hacks.

65. Catherine Theohary and Cory Welt, "Russia and the U.S. Presidential Election," CRS Report no. IN10635 (Washington, DC: Congressional Research Service, 2017).

66. David Ignatius, "Russia's Radical New Strategy for Information Warfare," *Washington Post*, 18 January 2017, https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/?utm_term=.da53e31d7aaa.

67. Ibid.

68. "Ex-Sony Chief Amy Pascal Acknowledges She Was Fired," NBCNews.com, 12 February 2015, https://www.nbcnews.com/storyline/sony-hack/ex-sony-chief-amy-pascal-acknowledges-she-was-fired-n305281.

69. The political left in the United States seems to have a large group of bot accounts forming around the "Resist" movement. It is unclear whether those accounts are foreign cyber warriors or bots, but external actors can certainly feed off the underlying narratives and tap into existing networks of true believers.

70. David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (New York: Oxford University Press, 2013), 231.

71. Anthony Faiola, "As Cold War Turns to Information War, a New Fake News Police Combats Disinformation," *Washington Post*, 22 January 2017, https://www.washingtonpost.com/world/europe/as-cold-war-turns-to-information-war-a-new-fake-news-police/2017/01/18/9bf49ff6-d80e-11e6-a0e6-d502d6751bc8_story.html?utm_term=.7c99cc2fadd5.

72. Meyer, "War Goes Viral."

73. Ibid.

74. Cadwalladr, "Robert Mercer: The Big Data," 1.8.

75. Malcolm Mitchell, *Propaganda, Polls, and Public Opinion: Are the People Manipulated?* (Englewood Cliffs, NJ: Prentice-Hall, 1977), 12.

76. Ibid., 13.

77. Rebecca Carroll, "The State Department Is Fighting with ISIL on Twitter." Defense One, 25 June 2014, http://www.defenseone.com/technology/2014/06/state-department-fighting-isil-twitter/87286/.

78. Rita Katz, "The State Department's Twitter War with ISIS Is Embarrassing," *Time*, 16 September 2014, http://time.com/3387065/isis-twitter-war-state-department/.

79. Ellul, *Propaganda*, 241.

80. Adrian Chen, "The Propaganda about Russian Propaganda," *New Yorker*, 1 December 2016, https://www.newyorker.com/news/news-desk/the-propaganda-about-russian-propaganda.

81. Richard Deacon, *The Truth Twisters* (London: Macdonald, 1987), 95.

82. Michelle Castillo, "Facebook Found Fake Accounts Leaking Stolen Info to Sway Presidential Election," CNBC.com, 27 April 2017, https://www.cnbc.com/2017/04/27/facebook-found-efforts-to-sway-presidential-election-elect-trump.html.

83. Eric Bradner, "At CNN Town Hall, McCain and Graham Give Their View of Trump's Presidency so Far," CNN, 2 March 2017, http://www.cnn.com/2017/03/01/politics/john-mccain-lindsey-graham-town-hall/index.html.

Overcoming the Cyber Weapons Paradox

Maj Timothy M. Goines, USAF

Abstract

To increase the effectiveness of its cyber deterrence policy, a US Department of Defense official recently called for "loud" cyber weapons: cyber weapons that could be easily discovered and traced to the United States. These weapons, if employed, could offer unique advantages for US deterrence policy. However, the prospect of employing cyber weapons creates a paradox between overt factors of deterrence and the covert nature of offensive cyber operations—and the paradox of cyber weapons themselves. The current processes in place for using cyber weapons are not adequate to ensure such employment avoids the cyber-weapons paradox. A better process is to use interagency coordination that provides for a whole-of-government approach. The results of this evaluation demonstrate that, by using an interagency coordination process, the United States will be better positioned to employ an effective cyber deterrence policy.

✳ ✳ ✳ ✳ ✳

With thousands of malicious cyber acts occurring daily, the United States appears to be rather unsuccessful at deterring bad actors from attempting to infiltrate its networks and do damage.[1] For example, the Department of Defense (DOD) reported in 2008 that it was probed hundreds of thousands of times each day, and the problem has only grown.[2] One reason for the lack of success stems in part from the covert nature of cyber operations.[3] Under current policy, US cyber operations are highly classified; operations may be conducted in response to cyber acts, but the operations and the specific actor are obscured. Recently,

---

Maj Timothy M. Goines serves as an assistant professor of law, at the US Air Force Academy, Colorado Springs, Colorado. He is a judge advocate and has earned a master of arts degree from the Air Command and Staff College in 2017 as well as a master of laws degree from the University of Nebraska in 2016.

however, the commander of US Cyber Command (USCYBERCOM) stated the command is looking for attributable or "loud" cyber weapons that can be used by the DOD and definitively traced to the US military. As proposed, when using these new cyber weapons, the United States would not obscure the operation or actor from being discovered by the victim and attributed to the United States. It would broadcast US use of cyber weapons, making them easily discoverable. The logic is that by using loud cyber weapons, the United States gains a deterrent advantage. First, it allows the United States to signal its intent to defend specified domestic assets and its willingness to engage in aggressive cyber operations against an adversary.[4] Second, it informs the cyber adversary of US cyber capabilities—something that is suspected but not known. Finally, it increases the credibility of the US deterrence program by demonstrating that the United States is capable and committed to responding to malicious cyber acts. Upon consideration, this appears to be a rather simple and effective solution to the current problems with US cyber deterrence policy. Making cyber weapon use easily discoverable and allowing actors to trace the use back to the United States will open a line of communication, albeit rather indirect. Nevertheless, this line of communication allows the United States to indicate which targets it is willing to defend as well as its capabilities, its commitment, and the credibility of its future threats. In other words, this solution meets the requirements of deterrence, allowing the United States to communicate its system of rules and signal its commitment and credibility in the cyber environment.

However, two US government communities concurrently conduct cyber operations: the intelligence community and the DOD. These two communities have complementary capabilities, resources, and staff but often conflict with each other because of exclusive planning, unknown vulnerabilities or exploits, uncoordinated timing, and detrimental targeting. As the DOD starts to employ loud cyber weapons, these operations could render future missions ineffective or substantially degraded. While some overt offensive cyber use adds to deterrence, at the same time it creates a sort of cyber weapons paradox between overt cyber deterrence and covert cyber usefulness because any overt use can render the weapon useless. The paradox also exists because of the nature of cyber weapons themselves.

In addressing the paradox, this article explores the following question: How can the United States most effectively employ offensive cyber weapons to achieve maximum deterrent effect without foreclosing the US ability to conduct covert offensive cyber operations? The article begins by defining deterrence and discussing the essential factors for effective cyber deterrence. Next it analyzes the paradox that emerges within current offensive cyber processes and the existence of a paradox within cyber weapons themselves. Following this, the article proposes overcoming the cyber weapons paradox through interagency working groups that focus on prioritizing cyber weapons.

Unfortunately, the employment of these weapons raises a slew of other concerns. First, there are policy concerns. For example, what are the potential consequences of using these weapons? If employed against certain actors, what are their likely responses? Does responding to these actions result in the escalation of conflict? If so, is that advisable? What would the threshold be for potential responses? Is the United States willing to accept these potential responses? By revealing its hand, the United States exposes itself to scrutiny from the international community and potential cyber responses from the actor. Given the significant policy considerations, this article cannot adequately address and resolve them all. Instead, it assesses the more practical concerns associated with employing attributable cyber weapons—specifically, the paradox that results from loud versus covert and used versus useless cyber weapons.

Essentials of Cyber Deterrence

A thorough history and analysis of deterrence theory is provided by deterrence scholars Alexander L. George and Richard Smoke.[5] They have noted that deterrence theory traces its roots back to Thucydides and the Peloponnesian War, but its most significant employment was far later, during the Cold War between the United States and the Soviet Union. As both parties attempted to avoid a nuclear war during this period, many theorists studied deterrence theory in its various forms: strategic (thermonuclear), limited, and "sublimited" deterrence.[6] From these studies, deterrence theory across all forms was reduced to a goal of affecting the decision-making calculus in the mind of the actor: "In its simplest form, deterrence is merely a contingent threat: 'If you do x I shall do y to you.' If the opponent expects the costs of y to be greater than the benefits of x, he will refrain from doing [x]; he is deterred."[7]

While the practice of deterrence is rarely this simple, the heart of the theory is logically sound. If the potential costs of a particular action outweigh the potential benefits of that action, the actor should rationally choose not to pursue that action. More accurately, if the actors believe the deterring state will defend itself and the actors believe the costs of such a response will exceed the benefits of their proposed action, they will not conduct the action.[8] Thus, the goal of any viable deterrence policy should be to raise the credibility of the potential response. From this, we can extract important requirements of a successful deterrence policy.

Rules, Signals, Commitment, and Credibility

The deterring state must develop a clear policy that contemplates qualifying actions (such as threshold questions), qualifying targets, qualifying actors, and the corresponding responses, which this article will term a *system of rules*.[9] By developing these rules, the deterring state fully forms its intent to protect certain aspects of the nation (such as national infrastructure, institutions, and territory) and develops the corresponding responses to any of these threats. Nuclear deterrence is a prime example, whereby the United States declared that any launch of a nuclear weapon by an adversary would result in a retaliatory strike.

After a system of rules is created, the rules must be communicated to the actor to be deterred; if that actor does not know about the potential consequences, the actor is not likely to change his actions.[10] This is commonly completed through *signaling*, where the deterring state declares its intent and the consequent actions.[11] For example, in conventional operations, if states want to deter an adversary from invading their territory, they can "signal" their intent to resist an invasion by amassing troops along the border. Similarly, if states want to demonstrate their global reach, they may send naval squadrons to a particular area.

Next, the deterring states must be *committed* to carrying out their prescribed consequences.[12] If deterring states are or appear unable or unwilling to employ their system of rules, they would do little to impact the decision calculus of the other actor. With nuclear deterrence example, if the United States were unwilling to resort to nuclear war, adversaries would not be affected by the threat of a strike. Similarly, if the United States were incapable of launching a retaliatory strike (due to monetary or deployment constraints), the adversary would not likely be deterred. Thus, this requirement has two components: the state must

have the will to employ the system of rules, and it must also have the "acquisition and deployment of capacities to back up the intent."[13]

Finally, the deterrence policy, as a whole, must be *credible*.[14] This requirement is related to both the commitment by the deterring states and the capability of the deterring states to carry out the actions within their system of rules. For example, if the response threat were (or appeared to be) outlandish or unreasonable, an adversary would likely not believe the potential threat and likely not be deterred.

It is important to note that the general goal is to deter, but this is by no means an all-or-nothing theory; in other words, deterrence theory considers that it may succeed at times and it may fail at times.[15] This especially applies in the cyber environment, where deterrence of every malicious cyber act is an unrealistic goal. Although this might seem to be a drawback with deterrence strategy, it is not exclusive to deterrence—after all, military operations can and do fail, as do other political attempts. Thus the goal of any deterrence policy should be to designate actions we want to deter and then coordinate operations to maximize our ability to deter those acts.

From general deterrence theory, the United States has formulated its deterrence policy. The most recent version was articulated in the 2006 publication *Deterrence Ops, Joint Operating Concept, Version 2.0.*[16] More recently, in 2015, the *DOD Cyber Strategy* was issued, which also addresses deterrence (specifically, cyber deterrence) and reinforces the concepts in *Deterrence Ops*.[17]

The stated goal of the DOD deterrence policy is "to decisively influence the adversary's decision-making calculus in order to prevent hostile actions against US vital interests."[18] As such, an adversary's decision-making calculus consists of weighing three factors: (1) the benefits of a course of action, (2) the costs of a course of action, and (3) the implications of restraint.[19] Deterrence operations, therefore, seek to affect adversary decision-making calculus by providing the basic framework for all deterrence operations to build upon, including cyber deterrence.

Denying Benefits

The first way to deter an adversary is by denying the benefits of a course of action. In the cyber domain, the primary method through which a state denies benefits is through a robust and effective cybersecurity system, reducing the number of vulnerabilities within its network and

preventing infiltration and exploitation. This method of denying benefits is a purely defensive operation.[20] As a result, this article will not discuss denying benefits in great detail since its primary focus is offensive cyber operations, which are more appropriately categorized under cost imposition and encouraging adversary restraint.

Imposing Costs

The second way to deter an adversary is to credibly threaten to impose costs as a consequence of an aggressive cyber act. Examples of cost imposition range from criminal prosecution to offensive cyber operations to conventional military operations.[21] It is worth highlighting the distinction between cost imposition and the threat of cost imposition. In essence, once costs have to be imposed, the act has occurred and deterrence has failed. Therefore, the goal of a deterrence strategy should be to effectively threaten cost imposition such that an actor chooses not to engage in the act in the first place. DOD policy reflects this logic, stating one of its goals is "to declare or display effective *response* capabilities to deter an adversary from initiating an attack" (emphasis in original).[22]

Implications of Restraint

The third and final way to deter an adversary—to encourage restraint—is accomplished primarily through voluntary agreements to restrain, such as multilateral and bilateral agreements in the form of arms control treaties or conventions. For example, in September 2015, the United States and China agreed to stop all economic espionage in cyberspace against one another.[23] While this effort has been somewhat successful, most efforts have been rather unsuccessful at achieving adversary restraint.[24] Fortunately, a state looking to deter actors can also encourage restraint through general deterrence, demonstrating its ability to deny benefits (through defensive operations) and impose costs (through offensive operations) by interacting with other countries. Upon seeing the capability of the deterring state, an adversary is more likely to see a greater benefit and less cost in *not* attempting a cyber act against the deterring state.

Underlying this DOD deterrence policy is the concept (borrowed from deterrence theory) that the decision to act is made by individuals based on their perception of these factors, given their values and perceived probabilities of alternate outcomes.[25] So the DOD's policy recognizes

that deterrence is not a one-size-fits-all approach; to be effective, it must be tailored to specific adversaries within their specific contexts.[26] For example, knowing why an actor carried out a cyber act offers insight into its decision-making calculus (motive and what it stands to lose or gain from an act) and can help in creating an effective deterrence strategy, whether criminal prosecution or responding with offensive cyber operations is more appropriate.[27]

The Paradox of Cyber Processes

As with most things relating to cyber operations, the current US government process used to approve offensive cyber operations is classified. While the unclassified instruction Joint Publication (JP) 3-12, *Cyberspace Operations*, does provide general information on the employment of offensive cyber operations, it fails to provide much, if any, description of the current process for employment and approval.[28] JP 3-12 discusses the employment of offensive cyber operations, where it highlights valid concerns including transregional effects, conflict probability, and foreign policy implications.[29] Unfortunately, it does not specify how to account for these concerns within an established process. Instead, it appears to endorse an ad hoc approach, requiring initiation, planning, coordinating, deconflicting, and executing each operation, one at a time. This requires any offensive cyber operation to start from ground zero instead of being able to use an established process.

Beyond that, there is very little description of the approval process for offensive cyber operations. The lone reference to any approval process simply states that approval for offensive cyber operations requires "national level approval."[30] What can reasonably be assumed is that "national level approval" requires authority beyond the hierarchy of any one US agency (the DOD, the National Security Agency [NSA], the Department of Justice [DOJ], the Department of Homeland Security [DHS]). This would likely put the approval level at the National Security Council (NSC), the president, or vice president.

Although more information is likely contained within classified documents, there is no evidence that it extends beyond an ad hoc nature and the approval authority is at the "national level." For example, there is no evidence of an established interagency process within the NSC or outside of it. In fact, JP 3-12 is a DOD-specific instruction and only applies to DOD operations. Furthermore, given the covert nature of

cyber operations and the historical desire to keep operations classified, having a process that crosses multiple agencies, especially when it comes to the employment of offensive cyber operations, is not likely to exist.

Therefore, given the limited access to classified information, it is a reasonable assumption that the current process to approve and employ offensive cyber operations begins solely within the DOD, funneled through the secretary of defense, and approved by someone at the national level.[31] When evaluated under the specific factors outlined earlier, there are a number of concerns with this process.

Limited Visibility of Other Operations

With national-level approval, the current process allows offensive cyber operations to be a smaller piece in the larger deterrence policy. Unfortunately, the responsibility to assess the effectiveness of every operation falls on the DOD chain of command and the national level approval authority, without the assistance of knowledgeable outside organizations, experts, and technicians. This is a significant stress on the process, since the responsibility of maximizing each offensive operation's deterrent effect is left to one authority.

Second (and related to the first concern since it originates solely within the DOD community), the particular vulnerability and exploit are not vetted through each organization for past use, current use, or potential future use. It is highly unlikely that the single national-level approval authority would know each vulnerability and exploit previously, currently, and intended to be employed by all the disparate agencies with cyber capabilities. Furthermore, it is even more unlikely that the national-level authority would have a system in place to consult with these organizations, consolidate the vulnerabilities and exploits in a unified database, and set rules and priorities for their employment. The likely consequence is that, unless the authority is informed of other operations, he or she is likely to approve an offensive cyber operation that could conflict with current or future operations.

No Whole-of-Government Approach

The current process also does not use a whole-of-government approach. There are a number of agencies that either possess or could easily possess offensive cyber capabilities, for instance USCYBERCOM, the NSA, the DOJ, and the Central Intelligence Agency. Each has access

to certain vulnerabilities and exploits, and each has a mission they are attempting to accomplish. Currently, these agencies do not work in concert. Instead, they are segregated from one another to ensure the secrecy of their operations. These disparate missions likely contribute to the paradox.

Moreover, cyber threats come from various types of individuals, including state actors, state-sponsored actors, organized criminal groups, individual hackers, and extremist groups with radical ideologies. Each of these actors can and must be deterred in different ways, through different mechanisms. Achieving deterrence is not exclusive to offensive cyber operations. Rather, a cyber operation is just one of many possible alternatives for a deterring state; other options include criminal prosecution, sanctions, public condemnation, and conventional military operations. Each of these alternatives can be effective at deterring future actors, depending on the circumstances.

As noted above, offensive cyber operations originate solely within the DOD and its chain of command. They are only elevated beyond the DOD when they are seeking approval to conduct the specific cyber operation on the specific target. Not only does this result in a lack of vetting the specific cyber vulnerabilities and exploits with other cyber-capable agencies, but it also does not consider other response options from other agencies. It is conceivable that an offensive cyber operation could be used where prosecution of a conventional military operation would have a greater deterrent effect.

From a practical perspective, it is not likely that the DOD self-initiates the process for employing an offensive cyber operation in response to a cyber act. Rather, it is more likely that the national-level authority requests a proposed offensive cyber operation when weighing all the response options. Unfortunately, much like the vetting process, this puts a significant strain on the approval authority to determine which action is likely to be the most effective, especially considering the various political factors. This is aggravated by the ad hoc nature of the current process.

Slow Decision Timelines

Under the current process, when a cyber response is desired, an offensive cyber operation is planned, reviewed, and elevated throughout the DOD. This process likely includes reviews for viability, legality, conflict escalation, and policy concerns. It is then sent forward to the national-

level authority for consideration. This process, like any process requiring multiple reviews within multiple layers of bureaucracy, takes time. Also, because each offensive cyber operation must start from ground zero, unfamiliarity with the process can produce unnecessary delays. As a result, the ad hoc nature of the current process can produce slow operation timelines, leaving more time for the adversary to find and patch vulnerabilities.

Stress on Decision Maker

With the designation of the national-level authority for the approval of offensive cyber operations, there appears to be a single authority deciding which vulnerabilities and exploits to employ for which purpose. As noted with the previous factors, the current process puts a tremendous amount of strain on the decision maker. This is due to the lack of a vetting process, the lack of a whole-of-government approach, and the ad hoc nature of the current approval process. As a result, even though a final authority is designated, the process does not have the intended effect of creating a cooperative environment and avoiding the potential for multiple agencies employing the same cyber weapon for two different purposes.

For these reasons, the current processes for offensive cyber operations are not adequate to ensure their employment is conducted to avoid the paradox and mission conflict. This situation creates problems for the use of loud cyber weapons—which are paradoxical themselves.

The Paradox of Cyber Weapons

Before discussing the paradox inherent in cyber weapons, it is important to first consider some of the unique aspects of cyber weapons that undergird the paradox.

Perishability and Obsolescence

Cyber weapons (both attributable and covert) are perishable and rendered obsolete over time. A cyber operation is composed of two parts, a vulnerability and an exploit. A vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."[32] The

prototypical example of a vulnerability is a zero-day vulnerability, which is a hole in the software that is unknown to the author.[33]

The upside with vulnerabilities is that the operator of the system is unaware of them, providing another actor the ability to access their system. The downside is that, once the vulnerabilities are discovered, they are often fixed by the vendor, manufacturer, or owner quickly. For example, Microsoft has historically released security patches to fix holes in its Windows Operating System (OS) on the second Tuesday of each month.[34] So, a vulnerability has a window from the time it is known to a potential actor to when it is discovered and fixed by the operator. Using the Windows OS schedule as an example, a vulnerability could be fixed in as little as 30 days after its discovery; the time could be longer or shorter depending on a number of factors (the nature of the vulnerability, how prevalent it is, and so forth). The greatest factor in determining a vulnerability's lifetime is discovery. The longer it can remain undiscovered, the longer an actor can exploit it.

Vulnerabilities are discovered through self-initiated examinations, through notices from government or cybersecurity organizations (such as the United States Computer Emergency Readiness Team or the Symantec Corporation), or in response to an exploit. Thus vulnerabilities suffer from perishability (fixed once discovered through its use with an exploit) and obsolescence (fixed once discovered by self-initiated examinations or discovery by other organizations).[35]

Exploits are "operations [or] intelligence collection capabilities conducted . . . to gather data from target or adversary information systems or networks."[36] Essentially, the exploit is the code, worm, virus, or Trojan horse that is inserted via the vulnerability to do damage, collect information, or complete another operation. Perhaps the most famous example of this is the Stuxnet worm, which was inserted into the Iranian nuclear material enrichment facility and caused many of the centrifuges to spin out of control.[37]

Similarly to vulnerabilities, exploits also suffer from perishability and obsolescence; once they are used, the operator can develop a patch that can render the exploit ineffective (although this is less effective than patching the vulnerability). For example, once Stuxnet was discovered, the author of the targeted devices' OS developed a patch that rendered the code useless.[38] Additionally, certain exploits can be rendered ineffective if they are sophisticated, only becoming active once specific condi-

tions exist. For example, Stuxnet depended on the specific conditions to exist (a certain version of the OS, a certain type of logic controller, and a certain type of centrifuge).[39] This was a positive thing, since it limited the impact it would have on other computers if it propagated outside of the nuclear facility. However, the negative of this was that, if any of these conditions changed, Stuxnet would have been rendered useless.

Reusability and Forensic Data

Another attribute of an exploit that can lead to problems is that, once discovered, exploits can be replicated and forensically studied. Once the "code" is out in the world, nothing can be done to erase or destroy it. This leads to two potential problems. First, any discovered exploit could be studied, modified, and then used again, potentially against the creator. For example, Stuxnet was a very sophisticated exploit with thousands of lines of code.[40] Once discovered, Stuxnet was widely distributed throughout the internet, allowing many to study its tactics and its ability to avoid detection.[41] It has since been replicated hundreds of times, possibly serving as the foundation for many new cyber weapons.[42] Granted, many of these variants would likely be ineffective given the widespread knowledge of Stuxnet's code, but many devices may remain vulnerable to its methods. In any event, cyber operators must be cognizant of the reusability of cyber exploits before employing certain code within an attributed cyber weapon.

Second, any discovered exploit can be studied and compared to other exploits for similarities in methods and organization. This may lead to the conclusion that two exploits came from the same organization. For example, Stuxnet was studied extensively by many organizations around the world. Within the code, information was discovered that allegedly tied Stuxnet to certain countries, although no one has officially confirmed these suspicions.[43]

This particular attribute of cyber weapons can be disastrous for cyber operations—each discovered cyber weapon gives the target forensic evidence that can expose other (more covert) operations. Consequently, any misuse of these vulnerabilities and exploits could result in either the DOD or intelligence community (IC) compromising the effectiveness of the other. For example, if the DOD deployed a cyber weapon that exploited a vulnerability that the IC was using for intelligence gathering, the vulnerability could be fixed quickly by the target, and the IC's operation

would be degraded. Similarly, if the IC developed an exploit and it was discovered, the target could adapt its system to be immune from future exploits of this nature. In another scenario, the DOD could develop an exploit and deploy it, and once discovered, it could bear similarities to other covert operations by the IC. This could link the two operations and expose covert operations to the international community.

As the DOD starts to employ attributable cyber weapons, it is easy to imagine how its operations could conflict with those of the intelligence community, rendering one or both of the missions ineffective. Fortunately, it does not appear that this paradox as played out has resulted in any disastrous effects thus far. However, as loud cyber weapons are employed more frequently, the potential for these operations to conflict increases. Thus, the United States should anticipate the potential problems and be proactive in overcoming the paradox.

Perishability and obsolescence make deployment of cyber weapons unlike that of other weapons in the US arsenal. Once a vulnerability or exploit is used, future use is foreclosed; however, waiting too long to use a vulnerability or exploit provides the target time and opportunity to discover the flaws, also resulting in the foreclosure of its future use. Thus, offensive cyber operations must strike a balance between waiting for the best opportunity to employ a particular weapon and not waiting too long such that the exploit or vulnerability is rendered obsolete.[44]

The problem this paradox poses is made more significant by the fact that the number of vulnerabilities and exploits are somewhat limited. While these are theoretically unlimited (a computer system is manmade, so it will likely never be without a flaw, and there are always creative ways to code an exploit), the discovery of vulnerabilities and development of exploits is increasingly expensive. Accordingly, available vulnerabilities and exploits must be closely guarded and cautiously used.

The large majority of cyber operations conducted by the United States are classified. Therefore, the following discussion is limited to the unclassified information available. As detailed below, however, this does not detract from the conclusions. Instead, the covert nature of US cyber operations hits on a major problem for cyber deterrence: the inability to communicate the deterrence policy. This inability prevents the United States from communicating its system of rules, signaling, and commitment—all necessary for effective deterrence.

Lack of a Clear System of Rules

While current US deterrence policy does specifically identify certain protected targets, it leaves ample ambiguity surrounding potentially protected targets.[45] While this may appear to allow leeway as technology changes and the protected targets shift, it works both ways. The potential actors are unclear as to what targets will generate a response and what targets will not. What qualifies as the "DOD network" and "DOD data"? Since the majority of DOD traffic flows over civilian networks, where does the United States draw the line between the civilian network and the DOD network?[46]

Perhaps in an effort to clear up some of this confusion, in July 2016, President Obama approved a Presidential Policy Directive (PPD), which directly addressed the federal government's classification and response to cyber acts.[47] Along with this PPD, the president also released a Cyber Incident Severity Schema (CISS), which identified "targets" and sought to establish a framework through which the severity of cyber incidents would be classified.[48] Identified targets include critical infrastructure, national security, public health, civil liberties, and the lives of US persons. Unfortunately, the CISS did little to clear up the confusion. What qualifies as an act targeting US national security, critical infrastructure, or civil liberties? If it is unclear to those who execute the PPD, it is definitely unclear to potential foreign actors who lack familiarity with US culture and internal operations.

While in certain categories of deterrence ambiguity can be a benefit, this is not necessarily the case in cyber operations. For example, in nuclear deterrence, being unclear as to what targets would provoke a retaliatory strike has been beneficial. A nuclear strike is on the highest end of the escalation ladder, so the prospective response is extreme. A potential adversary would not want to chance a debilitating retaliatory strike to see whether the United States would respond. Instead, the adversary would avoid any action that may provoke a response. In cyber operations, this relationship is reversed: cyber operations are on the lower end of the escalation ladder, so a prospective response would also be low. Given this scenario, adversaries are more willing to "poke and prod" US networks to determine what they can do and what provokes a US response; the worst response is still very low on the escalation ladder. Thus, ambiguity in what would provoke a response ostensibly serves to tempt adversaries to probe US networks and see where the United States will draw the line.

The more clearly the United States defines what will generate a response and draw the line proactively, the less likely an adversary will be tempted to test the waters. Until the United States develops a comprehensive system of rules, the confusion that results only reduces the effectiveness of the current deterrence policy.

Also, the current DOD policy completely ignores civilian targets and civilian infrastructure. The CISS attempts to include some civilian aspects, but they are framed in vague generalizations. While the reluctance to incorporate specific civilian targets under the umbrella of already overworked DOD cyber operators is understandable, their exclusion is noteworthy. If anything, the absence of specific civilian targets creates confusion over what targets would generate a response and what targets would not.

Inability to Signal

Signaling is the method by which deterring states communicate their intent to defend certain targets or areas.[49] In conventional operations, the United States communicates its intent to defend a particular target and expresses a commitment to the defense with a show of force, lending credibility to the threat. However, with the covert nature of cyber operations, the United States is unable to signal potential actors. Consequently, the United States does not effectively communicate which targets it is committed to defend and the credibility of its potential response is not confirmed, at least not in any meaningful way. Furthermore, even if adversaries suspect certain capabilities and assume that a target is one that the United States will defend, they do not know what actions will result in a US response.

Unacknowledged Responses

Moreover, the covert nature of operations prevents effective communication after an offensive cyber act. Even if the United States responds with an effective cyber operation, the target of the response may not discover the response and, if discovered, may never know that the United States was the responsible party. This is another area where cyber deterrence contrasts significantly with nuclear deterrence. In nuclear deterrence, not only would a response be easily recognizable (e.g., a launched missile), but the source of the response would also be easily identifiable.

However, in cyber operations, there is considerable ambiguity, and the ambiguity actually hurts the effectiveness of deterrence. Many adversaries may suspect the United States could and would respond, but they may not be able to confirm the response or the source. This can be a lost opportunity, where an adversary is left with the perception that he "got away with it." That perception can render a deterrence policy wholly ineffective.

To be fair, there are certainly scenarios where the United States may prefer ambiguity or to mask the source of the operation. For example, US operators may desire to monitor the actor's activities for intelligence-gathering purposes or to prevent confirmation of the source of the response. However, it must be acknowledged that these types of operations have little to no deterrent effect; if an actor does not know of the monitoring or the source of the response, it is very unlikely to impact his decision-making calculus—the primary goal of deterrence.

Another side effect of this ambiguity is that it puts too much power into the hands of potential adversaries. As an adversary "pokes and prods" US networks and as the United States seemingly ignores those actions, the adversary continues to push the boundary. If the United States has not clearly articulated its system of rules (and communicated them), this can actually allow the adversary to define the threshold for a response. In other words, until the United States draws a line in the sand, the adversary is empowered to do so—to the detriment of US interests.

Overcoming the Cyber Weapons Paradox

Overcoming the cyber weapons paradox means balancing a number of factors relating to cyber operations and national security. Any process or system employed to overcome the paradox must be empowered to work within the existing national deterrence framework in two ways. First, it will necessarily be a smaller piece of a larger deterrence policy that meets the characteristics of deterrence: rules, signals, commitment, and credibility. Obviously, as framed here, the paradox specifically addresses offensive cyber operations with the advent of attribution, which is a narrow issue in relation to a national deterrence policy. While this article does not specifically address the larger deterrence policy, it recognizes the need that any proposed solution must work within it. Determining when to employ one of the many different options should be the main responsibility of the larger deterrence policy, which high-

lights the need for a whole-of-government approach in that component as well. But, more specifically for the purposes of this article, any process or system must funnel its work product into the larger deterrence policy to inform it of the potential offensive cyber responses available for each situation. Additionally, there must be a final authority to make the decision on what response to employ in every scenario. This decision maker is critical for offensive cyber weapons, where it is important to have a single authority deciding which weapons to employ for which purpose. Channeling this decision to a single authority creates a cooperative environment and avoids the potential for multiple agencies employing the same cyber weapon for two different purposes.

Second, the process or system must be given the necessary authority and scope to manage offensive cyber operations in a manner that maximizes their effectiveness. This authority must include the authority over US government organizations that possess cyber capabilities or authorities (IC, DOD, DOJ, DOS, and DHS). In other words, the process or system must have the authority to gather the various vulnerabilities and exploits across all relevant organizations and set the rules for their employment, by which these organizations must abide. This authority should be distinguished from the decision maker having the power to authorize the employment of an offensive cyber weapon, which is not a prerequisite for overcoming the paradox. Rather, the process or system is only required to consult with US government organizations regarding offensive cyber weapons, consolidate these weapons in a unified database, and set binding rules and priorities for their employment. Without this authority, the prioritization serves as guidance, which can seemingly be ignored and produce the very paradox it is meant to prevent. The process must also recognize time is a significant factor in cyber operations where some vulnerabilities only last 30 days. Therefore, overcoming the paradox requires a process or system that accounts for time, using a streamlined process that minimizes the time from discovery of the vulnerability or exploit to its employment.

Proposed Interagency Working Groups

The approach to overcome the paradox requires establishing two interagency working groups.[50] The first will be the cyber interagency working group (CIWG) comprising the government agencies with cyber capabilities. Membership of the group would include all government agencies

with cyber capabilities, both offensive and defensive; this membership will ensure all past, present, and future operations are considered. This interagency working group will have the mission to consolidate all the known vulnerabilities and exploits into a unified list and set rules and priorities for their employment. It will also have the authority to require compliance with the rules and priorities they determine.

Given the disparate nature of the missions of the organizations in the CIWG, a lead agency should be appointed to ensure that progress is made at a sufficient rate. USCYBERCOM is currently delegated responsibility for planning and conducting cyber operations for the DOD.[51] Due to the significant role it plays in US cyber operations, the lead agency for the CIWG should be USCYBERCOM.

It should be noted that private technical (tech) companies are not included as members of the CIWG. While having private tech companies participate in the consolidation and prioritization process would appear to be an advantage due to their technical capabilities, their participation would create a conflict of interest. Private companies aspire to create software that is secure from potential penetration by hackers and other governments. In addition, they currently sell their software worldwide, to allies and adversaries. By disclosing the known vulnerabilities in their software and the potential exploits to these civilian tech companies, we would create a potential conflict of interest, whereby these companies would be tempted, if not obligated by their shareholders, to find and fix the vulnerabilities as soon as possible.

The concern was recently highlighted by the president of Microsoft, Brad Smith, who declared that civilian tech companies should proclaim their neutrality in the cyberspace battlefield.[52] A neutral party would clearly not endeavor to assist any government in finding vulnerabilities and developing exploits. Furthermore, as Smith added, private tech companies must be committed to "100% defense and zero percent offense."[53] Therefore, it appears that at least some tech companies recognize this conflict of interest and do not wish to participate in planning or executing offensive operations.

To ensure the effectiveness of larger deterrence policy, the second interagency working group will be the deterrence interagency working group (DIWG). This deterrence working group will serve as a component of the NSC, be responsible for assembling the various agencies that can impose costs on cyber adversaries, and advise the NSC on the courses

of action that maximize the deterrent effect. The CIWG would be subordinate to the DIWG. A representative from the cyber working group would participate in discussions of cyber policy and serve as the subject-matter expert within the DIWG.

The placement of the sub-working group under the DIWG may appear to limit its deconfliction responsibilities and usefulness to deterrence purposes only; however, loud cyber weapons have utility outside of deterrence effects. Therefore, while the sub-working group is placed under the DIWG, it will provide deconfliction services for all cyber operations, including covert cyber operations. Given that the majority of loud cyber operations will be for deterrence purposes, the placement under the DIWG provides the most logical supervisory structure.

Once again, given the disparate nature of the missions of DIWG members, a lead agency should be appointed. The DHS is an executive agency with the mission to "ensure a homeland that is safe, secure, and resilient against terrorism and other hazards."[54] This mission specifically includes preventing terrorism, enhancing security, and securing cyberspace.[55] Considering the effects that cyber acts have on the United States and its citizens, the lead agency for this larger working group should be DHS. However, the final authority for any action taken would be the NSC.

Practically, the process would begin with the sub-working group, which would be a standing committee, meeting regularly to discuss, consolidate, and prioritize cyber vulnerabilities and exploits. As individual vulnerabilities and exploits are employed, perish, or are rendered obsolete, the list would be updated to account for the changes. Given the nature of cyber operations, this would likely be a continuous process. In the event an act occurred, the proposed DIWG would determine what response would provide the maximum deterrent effect, consulting the representative of the cyber sub-working group for potential options. If the best course of action is a cyber response, the representative from the cyber sub-working group would reference the current list of priorities and designate a vulnerability and exploit for employment. When evaluated under the specific criteria outlined above, these working groups offer a number of benefits for overcoming the cyber weapons paradox.

Benefits of the Integrated Working Groups

With the DIWG serving as an advisor to the NSC, it would be empowered to advise on the response that would result in the greatest

deterrence effect. As a component of the DIWG, the sub-working group on cyber operations would similarly be empowered. It would have the necessary authority and scope to manage offensive cyber operations in a manner to maximize their effectiveness. Part of this empowerment would come from the sub-working group's position within the NSC and the authority given by the president; the other part would come from the fact that all the cyber-capable agencies would be members and part of the prioritization process. So, not only would the agencies be required to follow the prioritization scheme, but they would also be shareholders of the process.

The DIWG and the sub-working group on cyber would both be made up of agencies that have parts to play in the larger deterrence policy and cyber capabilities. These agencies include the DOD, DOJ, DOS, NSA, and DHS—all agencies that can offer the NSC response options. For the DIWG, these agencies can work together; sort through the various options, consequences, and policy limitations; and select the most appropriate response option to maximize deterrence. This process helps provide comprehensive advice to the NSC and ensures all options are appropriately considered.

A similar construct would exist for the sub-working group on cyber. It would be made up of similar agencies, but the membership would largely be the technical experts within these agencies. By working together to prioritize the various cyber vulnerabilities and exploits, the working group ensures that each vulnerability or exploit is used discriminately, ensuring that loud operations do not conflict with current or future operations or expose covert options. In addition, the prioritization ensures that each cyber vulnerability and exploit is used in the most effective way.

As proposed, the CIWG will be a standing committee, meeting regularly to consolidate, prioritize, re-prioritize, develop, and designate cyber weapons for employment. Given the membership and the organization of the sub-working group, this proposal appears to add a layer (or layers) of bureaucracy, which can potentially lead to delay. However, as proposed, this sub-group employs two mechanisms to avoid delay. First, it appoints a lead agency, USCYBERCOM, to consolidate and prioritize the process. This gives the NSC and the larger DIWG a designated agency to assign duties and define timelines, ensuring the process is accomplished in a timely manner.

Second, instead of an ad hoc arrangement, the CIWG meets well before a cyber act occurs and continually prioritizes available cyber responses. Once a malicious cyber act occurs, the prioritized list allows the DIWG to review and select a cyber response in a timely manner. This greatly reduces the likelihood that a vulnerability or exploit will be kept past the window of usability. Also, by speeding up the timeline between approval and execution, the US signals "this action and others like it will not be tolerated."

The final authority for the employment of all cyber weapons would be the NSC. Positioning the DIWG as a component of the NSC and utilizing a whole-of-government approach alleviates some of significant strain on the final authority to account for the numerous variables within foreign relations. Instead of relying on the final authority to consider the numerous factors at play, this process allows the final authority to consult with the DIWG, consider the guidance, and make the final call.

Drawbacks and Limitations

While the interagency process provides for an improved practice, certain drawbacks exist. For example, anytime a number of different agencies with disparate missions and unique cultures attempt to work together, the likelihood of disagreement is high, which can introduce deadlock and delay. Additionally, there will be an initial period when the member agencies adjust to the procedure and the proposed hierarchy. However, the goal of the proposed process is not to design cyber operations by committee; rather, the goal is to foster a collaborative environment for all agencies to have a voice in the selection and employment of offensive cyber operations. Unfortunately, this requires the various agencies to buy in to the process and cede some of their power and independence. Therefore, the proposed process may suffer from an initial lack of cooperation and collaboration.

Another limitation with the proposed interagency process is that it exposes US cyber operations to more vulnerabilities—specifically, human vulnerabilities. Those who have access to the system with certain privileges or those who know of US cyber operations are vulnerable to exploitation. For example, a malicious cyber actor can access information on a particular person, which can be used as threats or other tactics to gain intelligence about potential cyber operations. Under the current

process, the covert nature of cyber operations reduces the number of people with access, thereby reducing the number of human vulnerabilities.

Another limitation is the vulnerabilities equities process (VEP), a classified procedure by which the US government determines when to publicly disclose discovered software and hardware vulnerabilities.[56] Some of the documents detailing the process were made public in 2010 in response to a Freedom of Information Act lawsuit.[57] In short, the VEP has existed within the US government, in some form, since 2008; it also went through a "reinvigoration" in 2014, when the administration made some changes to the process. The goal of the VEP is to identify vulnerabilities and then determine whether to share them with the US public for their security or to retain the vulnerability for offensive use. Unfortunately, the VEP has been a source of frustration for both civil liberty groups arguing that the US government should disclose all known vulnerabilities and government agencies arguing that the VEP serves to frustrate cyber operations.

The interagency process proposed in this article is not a substitute for the VEP. Instead, the interagency working group would work in concert with the VEP. In this regard, the proposed interagency process differs from the VEP in two significant ways. First, the VEP focuses on the disclosure or retention of vulnerabilities. On the contrary, the interagency working group does not consider the disclosure of vulnerabilities but rather the most effective use of vulnerabilities (regardless of the decision of the VEP) and exploits. Additionally, the VEP's goal is the privacy of the US public and the security of its devices and network, whereas the proposed interagency working group is focused on criminals and US adversaries.

It is possible that employment of loud cyber weapons can and will result in disclosure of vulnerabilities. Therefore, it is critical that the CIWG work with the VEP to ensure the exploited vulnerability has been quietly and properly disclosed prior to its employment—particularly for critical infrastructure and the defense industrial base.

Finally, the main criticism of the VEP has been the tension between the strategic disadvantages of disclosure and the risks to security and privacy due to retention. That same tension does not exist within the interagency process. While the CIWG must consider the strategic disadvantages of disclosure, it would be less concerned with security and privacy; any vulnerability will be shared prior to employment.

Conclusion

This article touches on but does not discuss at length the various other concerns raised by loud offensive cyber weapons. Opportunities exist for further research in this area on questions such as: What are the potential consequences? What are their likely responses? What is the threshold for potential responses? Is the United States willing to accept these potential responses? These concerns are significant and would benefit from more consideration. In addition, although the proposed solution discusses a framework for developing and selecting offensive cyber operations, it does not discuss the specific methods and means to consider when implementing this framework; further research is needed regarding specific cyber adversaries and how best to deter them. For example, what are the best cyber techniques to deter terrorist organizations, cyber armies, and cyber criminals? How do these techniques differ from state actors? Regardless, the proposal here represents a viable solution to the cyber weapons paradox. In short, this process ensures the United States can employ offensive cyber weapons to most effectively achieve maximum deterrent effect without foreclosing the US ability to conduct clandestine offensive cyber operations. SSQ

Notes

1. Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, 2008), 11–13.
2. Ibid.
3. For the purposes of this article, a cyber operation is considered to have two necessary pieces: a "vulnerability," which is a flaw in the target system's security, and an "exploit," which is the software (or code) that uses a vulnerability. Both vulnerabilities and exploits are perishable and rendered obsolete over time. Perishability defines the characteristic of a cyber weapon when it is no longer effective after being used due to the identification and subsequent elimination of the vulnerability or exploit. Obsolescence refers to a cyber weapon becoming ineffective because time has afforded the opportunity to identify (and subsequently eliminate) the vulnerability. These two characteristics of cyber weapons are unique among the US arsenal since any *discovered* use of a cyber weapon can foreclose the ability to use it again.
4. Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), 60.
5. Ibid.
6. Ibid., 1.
7. Ibid., 48.
8. Ibid., 60.
9. Ibid.

10. Ibid.
11. Ibid.
12. Ibid.
13. Ibid., 64.
14. Ibid., 60.
15. Ibid., 93.
16. Department of Defense (DOD), *Deterrence Ops Joint Operating Concept, Version 2.0* (Washington, DC: Office of the Secretary of Defense, December 2006), http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf.
17. DOD, *Department of Defense Cyber Strategy* (Washington, DC: Office of the Secretary of Defense, April 2015).
18. DOD, *Deterrence Ops*, 5.
19. Ibid. Presented another way, an adversary may consider the relative benefits and costs of action versus restraint.
20. While other methods for denying benefits are available outside of the cyber domain (i.e., refusing to relent to an adversary's demands), they are not the primary focus of this article.
21. Matthew J. Sklerov, "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent," *Military Law Review* 201 (Fall 2009): 1–85, https://www.jagcnet.army.mil/DOCLIBS/MILITARYLAWREVIEW.NSF/20a66345129fe3d885256e5b00571830/d471dd1e07eb949d85257672004463bc?OpenDocument.
22. DOD, *Cyber Strategy*, 11.
23. Ellen Nakashima and Steven Mufson, "The U.S. and China Agree not to Conduct Economic Espionage in Cyberspace," *Washington Post*, 25 September 2015, https://www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html?utm_term=.a31d532717a5.
24. Joseph Menn and Jim Finkle, "Chinese Economic Cyber-Espionage Plummets in U.S.: Experts," Reuters, 21 June 2016, https://www.reuters.com/article/us-cyber-spying-china/chinese-economic-cyber-espionage-plummets-in-u-s-experts-idUSKCN0Z700D; and Michael A. Vatis, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010), 207–24, https://www.nap.edu/read/12997/chapter/14.
25. DOD, *Deterrence Ops*, 11.
26. Ibid., 44.
27. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 75.
28. Joint Publication (JP) 3-12(R), *Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, 5 February 2013), http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
29. Ibid., II-7.
30. Ibid., II-7–8.
31. While other agencies may have cyber capabilities, only the DOD, as the military cyber force, would have the role of employing offensive cyber operations.
32. Committee on National Security Systems Instruction (CNSSI) 4009, "Committee on National Security Systems Glossary," 6 April 2015, 131, https://www.cnss.gov/CNSS/openDoc.cfm?LlSjfKedpJ/cVMi+7zozig==.
33. PC Tools, "What Is a Zero-Day Vulnerability?" PC Tools by Symantec, accessed 17 February 2017, http://www.pctools.com/security-news/zero-day-vulnerability/.

34. Microsoft Security Tech Center, "Microsoft Security Bulletins," Microsoft.com, accessed 17 February 2017, https://technet.microsoft.com/en-us/security/bulletins.aspx.

35. Christopher A. Bartos, "Cyber Weapons Are Not Created Equal," *Proceedings* 142 (June 2016), https://www.usni.org/magazines/proceedings/2016-06/cyber-weapons-are-not-created-equal.

36. CNSSI 4009, "Glossary," 25.

37. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, 3 November 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

38. Ibid.

39. Ibid.

40. Ibid.

41. Ibid.

42. Ibid.

43. Ibid.

44. Robert Axelrod and Rumen Iliev, "Timing of Cyber Conflict," *Proceedings of the National Academy of Sciences of the United States of America* 111, no. 4 (January 2014): 1298–1303, http://doi.org/f5q64n.

45. DOD, *Cyber Strategy*.

46. Eric Talbot Jensen, "Cyber Deterrence," *Emory International Law Review* 26, no. 2 (2012): 773–824, http://law.emory.edu/eilr/_documents/volumes/26/2/symposium/jensen.pdf.

47. The White House, *Fact Sheet: Presidential Policy Directive on United States Cyber Incident Coordination* (Washington, DC: Office of the Press Secretary, 26 July 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

48. Ibid.

49. George and Smoke, *Deterrence in American Foreign Policy*, 60.

50. It should be noted that this proposal is not without a precedent. In 2015, the DOD established the Joint Interagency Combined Space Operations Center (JICSpOC), which assembles representatives from the DOD, the intelligence community, and other agencies in the national security space enterprise. The JICSpOC serves as an example for implementation of the interagency process. *See* "New Joint Interagency Combined Space Operations Center to Be Established," news release, DOD, 11 September 2015, https://www.defense.gov/News/News-Releases/News-Release-View/Article/616969/new-joint-interagency-combined-space-operations-center-to-be-established/. Also see Colin Clark, "JICSPOC Morphs to 'National Space Defense Center'; What It Means," *Breaking Defense*, 4 April 2017, http://breakingdefense.com/2017/04/jicspoc-morphs-to-national-space-defense-center-what-it-means/.

51. United States Strategic Command (USSTRATCOM), accessed 17 February 2017, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/; and "About," USSTRATCOM, accessed 17 February 2017, http://www.stratcom.mil/About/.

52. Elizabeth Weise, "Microsoft Calls for 'Digital Geneva Convention,'" *USA Today*, 14 February 2017, http://www.usatoday.com/story/tech/news/2017/02/14/microsoft-brad-smith-digital-geneva-convention/97883896/.

53. Ibid.

54. Department of Homeland Security (DHS), "Our Mission," DHS, accessed 17 February 2017, https://www.dhs.gov/our-mission.

55. Ibid.

56. Dave Altel and Matt Talt, "Everything You Know about the Vulnerability Equities Process Is Wrong," *Lawfare*, 18 August 2016, https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong.

57. Ibid.

Fighter Jets, Supercars, and Complex Technology

Ian MacMillan

Abstract

The history of America's joint fighter programs is one marred by cost overruns, late deliveries, and cancellations. A neoliberal component of American political culture provides rhetoric to argue these are symptoms of public-sector management; furthermore, private-sector models offer greater efficiency standards. However, the public-private distinction is largely hyperbole. Especially with complex technological projects, neither sector is invulnerable to inflated costs and schedule slippage. Through a "Most Different Systems Design" method, this article compares the Joint Strike Fighter program to Honda's arduous journey to design a second-generation Acura NSX supercar. As a "plausibility probe," the findings in this article offer a starting point for further research examining public- and private-sector commonalities. There are problems with the F-35, but this should come as no surprise. Like modern supercars, complex weapons are not designed and built overnight. With patience, there can be a silver lining. Years of redesigns, cancellations, and more redesigns can eventually lead to revolutionary new capabilities. Many close to the Joint Strike Fighter agree that something special will emerge. Although the impatience directed toward the JSF program is politically effective, it is a poor basis for sound policy making. Given the strategic imperativeness of the F-35, patience is essential. The financial sacrifice is a modest trade-off necessary to maintain US airpower competitiveness.

✷ ✷ ✷ ✷ ✷

"It's been a scandal and the cost overruns have been disgraceful."[1] Heavily critical of the Joint Strike Fighter (JSF) program's expensive,

Ian MacMillan is a PhD candidate in strategic studies at the University of Calgary, Canada. His primary research interests include defense procurement, international relations, and culturally based analysis of government decision making. MacMillan's background in political science is complemented by his years as a media and policy analyst with Canada's federal public service.

15-year development schedule, Sen. John McCain has led a chorus seeking to eliminate the F-35's program office. In December 2016, accusing the JSF program of being "out of control," president-elect Donald Trump Tweeted a Boeing alternative was being considered.[2] In January 2017, the president suggested Boeing's Super Hornet could be equipped with stealth capabilities and replace the F-35.[3] Impatience with the JSF is understandable, but forgoing the capabilities of the F-35 may harm America's national interest.

The situation is not unique. Specifically, the history of America's joint fighter programs is one marred by cost overruns, late deliveries, and cancellations.[4] Condemnation of complex military programs like the JSF reflects a neoliberal political culture, critical of public spending in general. [5] Neoliberal proponents would argue JSF problems are symptomatic of poor public-sector management. Moreover, private-sector models would mitigate America's chronic problem with defense procurement.[6] Flowing from neoliberalism—an ideology with roots in American culture but which primarily emerged in the 1980s—New Public Management was envisioned as a system to "reconfigure the state along more cost-efficient (and effective) lines."[7] Henceforth, public spending habits were generally characterized as wasteful, and they continue to be held in sharp contrast to private-sector efficiency. *Prima facie*, this characterization is satisfying. It is easily understood and appeals to a critical mass of middle-class voters. However, the historical record shows that private-sector projects can also experience problems with delays and cancellations.

One example of a private-sector counterpart to the JSF is the Honda Motor Company's Acura NSX project. Through a comparative approach known as the "Most Different Systems Design," this article helps demonstrate that both public and private sectors can experience setbacks with complex technological projects.[8] The Honda case is appropriate because it is a private-sector company with multiple decades of success as an automobile manufacturer, especially its revolutionary first generation NSX. In spite of being a skilled and experienced company, designing an innovative and cutting-edge next-generation NSX led to schedule delays, redesigns, cancellations, and more redesigns before any success. There are other examples of private-sector companies experiencing design problems. But, before extensively researching additional private-sector cases, this "plausibility probe" acts as an effective method for exploring the suitability of the hypothesis: private-sector companies like

Honda experience design setbacks.[9] The strength of neoliberal political culture helps us forget that, especially with complex technology designs, both public and private sectors can be burdened by ambitious goals and ambitious delivery schedules.

To begin, this article will examine the main problem neoliberalism poses, for the public sector and for the JSF more specifically. To clarify the outlook toward delayed public-sector projects, a short history of neoliberalism in the US must be provided. The two case studies and results will follow. Although the impatience directed at the JSF program is politically effective, it is a poor basis for sound policy making. Given the strategic imperative of the F-35, patience is essential.

The Problem of Neoliberalism in American Politics

In spite of considerable literature pertaining to American military procurement, as well as how culture shapes military doctrine and innovation, yet to be addressed is the problem neoliberal politics poses for military procurement in the United States.[10] The neoliberal proposition is so classically American in logic and assertion, and comes up so frequently, that it must be addressed to move on to a more factual and fully analytic debate that can lead to better outcomes in the future.

The neoliberal tone in which the JSF program is criticized is not new or particular to American military procurement. Neoliberal political culture emerged several decades ago, henceforth providing rhetoric designed to reduce government spending and shift remaining programs toward private-sector type business practices.[11] Although there is a certain noble quality in serving the national interest through efficient government spending—especially in an era in which the American national debt has reached a critical phase—the JSF criticism is a problem. It perpetuates an oversimplified perspective that public-sector programming should somehow meet a set of unrealistic efficiency standards attained in the private sector. As John A. Alic notes, a private-sector approach toward military procurement began before President Ronald Reagan with Robert McNamara's attempt to enforce the use of business planning to support national security objectives. It was largely unsuccessful. Emulating private-sector practices may work with routine contracts, but it fails to effectively approach the complexity of major acquisition programs like the JSF.[12] In the particular case of military technological production, the private-sector practices lauded by neoliberal political culture do not

necessarily improve program efficiency. Rather, they may serve to strain further an industry already operating under challenging conditions.[13]

Between 1960 and 2010, 27 studies on defense procurement in the United States were completed. In 2011, Harvard professor J. Ronald Fox reviewed these studies; he concluded major defense programs require more than 10 years to deliver less capability than planned, at two to three times the initial cost. It could be argued that scheduling and cost goals established, generally in the beginning stages of military technology programs, are overly ambitious.[14] Private-sector practices will not necessarily alleviate the challenges posed by inventing complex military technology. Delays are a common reality. However, the inveterate quality of neoliberal politics in American political culture consigns alternative perspectives to a position of anathema.

The distinction between public and private organizations is embedded in the social fabric of American culture.[15] The country's collective imagination is one characterized by self-reliance, entrepreneurship, and private enterprise. Emphasizing a limited and accountable government from its point of inception, the United States instilled Lockean classical liberalism.[16] In an ironic twist, the continued operationalization of America's entrepreneurial spirit necessitated greater public institutional involvement. In tandem with a creeping reliance on public services, stronger federal control continued throughout the better part of the twentieth century. Governmental involvement became a matter of course in both domestic and international arenas.

The end of the Second World War gave rise to the welfare state, strengthening the position of public-sector involvement in society. Through a comprehensive tax system and a burgeoning bureaucracy, the American government—and other western governments for that matter—were able to ensure unprecedented economic development, employment, and social security. This creation of a "social domain" was a hedge against the risks of an industrial economy, pooling collective responsibility to ensure individual reimbursement. But during the late twentieth and early twenty-first centuries, socially oriented programs came under attack for supposed inefficient government spending.[17] As Donald Warwick notes, "Critics claim that governmental organizations become the master rather than the servant of the people, stifle initiative, inculcate fear, multiply reporting requirements, circumscribe action, waste time, and deplete the federal treasury."[18] There was a growing concern that,

in addition to draining public resources, social programming interfered with free market expansion, stifled entrepreneurialism, and encouraged dependency on the government at the cost of individual autonomy.[19]

In step with economist Milton Friedman, the 1980s saw western leaders such as Ronald Reagan and Margaret Thatcher endorse a neoliberal governmental approach, one that downplayed the value of large, public-sector projects.[20] Stated simply, the idea was that national economic prosperity was linked to attaining smaller fiscal deficits by decreasing public-sector reliance through privatization, thus containing government spending.[21] Self-reliance, entrepreneurship, and private enterprise returned as the thematic lodestars of future prosperity. Reagan argued against the idea that big business and big labor required big government.[22]

Of course, total abolishment of public-sector responsibility never occurred. But the idea that the public sector was inefficient gained a foothold. Stressing the utility of a private-sector management style, neoliberal proponents argued a New Public Management system would enable governments to achieve parsimony in resource use by, among other things, the cutting of direct costs and the enhancement of labor discipline via the resistance of union demands.[23] The one-dimensional characterization of the private enterprise as the harbinger of fiscal efficiency generated a narrative still used to undermine public-sector spending. Programs falling behind schedule and accruing unanticipated costs are characterized as a product of government mismanagement.[24] Sometimes these assessments are correct, but there are exceptions.

America's Joint Strike Fighter Program

Speaking at an April 2016 Senate Armed Services Committee meeting, Republican Sen. John McCain led a withering critique of the JSF program. Indeed, the F-35 has been plagued by several notable development problems, causing delivery delays since its inception in 2001.[25] However, it stands to reason that fighter-jet technology is complex, not to mention short take-off and vertical landing (STOVL) as a necessary component in the creation of a stealthy, multi-role fighter.

The JSF program emerged in the restrictive budgetary environment at the end of the Cold War. Individual fighter programs were incongruent with other political goals. Although the United States Navy (USN), the United States Air Force (USAF) and the United States Marine Corps (USMC) had differing aircraft objectives, fiscal frugality imposed a mar-

riage of convenience. Whereas the USMC wanted a STOVL enhanced aircraft, the USAF desired stealth. The USN predominantly wanted something with a robust airframe. The outcome of these disparate desires was the Pentagon establishing the JSF program in March 1996 and issuing a request for proposal for a design prototype shortly thereafter.[26] In a winner-takes-all competition, Boeing and Lockheed Martin were selected to construct the JSF prototypes and compete to build the production aircraft. The initial deadline to submit their prototypes was 2000 so a winner could be selected in March 2001.[27]

Problems designing and testing the STOVL component postponed the submission of flight test data until July 2001. Delayed slightly by the 9/11 attacks, Pentagon Acquisition Chief Pete Aldridge's announcement of the winner was made in October 2001.[28] Lockheed Martin was granted a 126-month, $13 billion contract.[29] What emerged over the course of a decade and a half was the F-35 family, composed of three single-seat variants with unique and complex characteristics to match the requirements of the USAF, USMC, and USN. Designed for the USAF, the most basic variant is the F-35A. Because it operates from conventional runways, it only requires conventional take-off and landing capabilities. However, unlike the USMC and USN versions, the F-35A was designed to carry an internally housed cannon to provide close air support for ground troops. This also means it can hold less fuel.[30]

The F-35B was designed for the Marines. In desperate need of a Harrier replacement, the USMC required an aircraft capable of providing STOVL so it could operate from austere, short-field bases and a range of air-capable ships operating near frontline combat zones. STOVL was made possible through a Rolls Royce–patented, shaft-driven "LiftFan" propulsion system and an engine that can swivel 90 degrees when in STOVL mode. Including this LiftFan required the variant to have a smaller internal weapon bay and even less internal fuel capacity than the F-35A.[31]

The F-35C was designed to be the Navy's first ever fifth-generation, radar-evading stealth aircraft, capable of long-range missions and built explicitly for aircraft carrier operations. It was also designed to be the Navy's first-day-of-the-war strike fighter, capable of overcoming a variety of threats (such as surface-to-air and air-to-air missiles), thereby opening up the battlefield for non-stealth aircraft. To enhance survivability and mission success, the F-35C combined stealth, advanced jamming, and threat system destruction. This variant has a larger wingspan and more

robust landing gear than the other variants, making it suitable for catapult launches and fly-in arrestments. Its wingtips also fold to allow for more room on the carrier's deck. Accommodating nearly 20,000 pounds of fuel internally, the F-35C has the greatest internal fuel capacity of the three variants, giving it longer range than any other fighter in a combat configuration. Like the F-35B, the F-35C uses probe and drogue refueling; this allows the USN to operate its carriers a safe distance from the threat while its fighters reach remote targets.[32]

That the Pentagon's JSF program constitutes an egregious mismanagement of public money is a false assumption. A program of this magnitude—a single airframe that operates across services and mission sets—is not a simple undertaking, and it is well known that military technology takes time to perfect. Furthermore, if the past is any indication of future events, current problems (such as software deficiencies, F-35B fuel tank redesign, lightning strike vulnerability, flight control problems, helmet display issues, component unreliability) are not insurmountable. When Lockheed Martin was contracted to develop a stealth fighter, completing the task was not a foregone conclusion. As the makers of the F-117 Nighthawk and B-2 Spirit know all too well, stealth technology presents a considerable challenge in aeronautical design. A problem faced early on by the JSF program was designing an aircraft that could evade radar, while carrying sufficient payloads and fuel for mission proficiency, and still reach supersonic speed. Different from most previous fighters (for example, F-14 Tomcat, F-16 Falcon, and F/A-18 Super Hornet), a stealthy F-35 required a larger and heavier airframe, one capable of storing all necessary weapons and fuel internally. The entire F-35 had to be scaled up to make room for a weapon bay able to carry a 5,000-pound payload. Since carrying drop tanks was out of the question, the plane had to include enough room for large internal fuel tanks. With a maximum takeoff weight of 60,000 pounds, the F-35 is considerably heavier than its non-stealthy predecessors.[33] To ensure the F-35 could both fly at a reasonable pace as well as deliver its payload, it was equipped with the Pratt & Whitney F135 engine. With a maximum thrust of over 50,000 pounds, this engine became the most powerful ever installed in a fighter aircraft as of 2010.[34]

Developing this engine took many years, and success in its creation was by no means guaranteed. For instance, the Pratt & Whitney F135-400 engine used for carrier-based operations faced issues with "pop stalls."[35] A

pop stall is when an aircraft's engine stops working as a result of hot gas ingestion. USN aircraft carriers use something called a launch catapult system to get aircraft airborne. The steam emitted from this system can cause a pop stall. Since the F-35 was designed as a single-engine aircraft, a pop stall created considerable risk as far as losing the aircraft and even the pilot during takeoff. To solve this, a risk-reduction team was assembled to evaluate the pattern of steam during an aircraft launch. Engineers from Lockheed Martin, Pratt & Whitney, General Electric, and NAVAIR cooperated to test and reduce the risk for the F135 engine. An additional problem occurred in June 2004 when the Pratt & Whitney F135-600 engine used for the STOVL F-35B variant experienced an "erosion problem" caused by the size of the restrictor plate that regulates the flow of cooling air to certain parts of the engine. The plate was undersized and was therefore not allowing enough cool air to reach the second-stage vanes of the turbine section. A revised restrictor plate was put in place, and the engine was permitted to rejoin testing.[36]

In January 2016, the Pentagon's Office of the Director of Operational Test and Evaluation (DOT&E) released its annual report for fiscal year 2015. Regarding the JSF program, the report listed a variety of problems and technical glitches and was largely viewed as a testimony to the program's supposed failure.[37] For instance, in 2011 it became clear that Rockwell Collins—the company contracted to build the F-35's Helmet Mounted Display System—was experiencing technical setbacks. Problems with "jitter," "alignment," the ability to set "symbology intensity," "latency in imagery projections," and performance of the night vision camera convinced Pentagon officials to hire BAE Systems to build a back-up helmet. Two years later, improvements in the helmet led the Pentagon to continue with Rockwell Collins. The DOT&E report noted that following Generation III testing, developmental test pilots reported significant improvements in the helmet.[38]

In spite of overall improvements, the Senate Armed Services Committee submitted a bill to disband the F-35 program office after the F-35 reaches full-rate of production in April 2019. Notwithstanding President Trump's Twittersphere campaign to drive down the cost of the F-35, McCain's bill was a dramatic move. Responsibility for follow-on modernization of the three F-35 variants—estimated to cost more than $8 billion for the first block upgrade—would be taken from the Department of Defense (DOD) and given to the Navy and Air Force, to be

treated as separate defense acquisition programs.[39] A summary of the bill states, "Devolving this program to the services will help ensure the proper alignment of responsibility and accountability the F-35 program needs and has too often lacked. . . . Given the Department of Defense's poor track record on upgrade programs like this one, a separate program will enable rigorous oversight by the Congress to protect taxpayers."[40] As one journalist argued, "The move is a shot across the Pentagon's bow."[41] John Alic argues the major lesson of the past half century is sensible military acquisition begins with increased power of civilian officials, not increased influence of the military services or even emulation of private sector practices.[42]

Discussing neoliberalism was a way for this article to bring a degree of clarity to McCain's and Trump's reactions to JSF program delays. Although neither are necessarily strictly neoliberal guided politicians, their words and demeanour toward the JSF program echoed that brand of ideology. Criticizing government programs for running over budget is effective political maneuvering but not necessarily an approach that translates into sound public policy. Shifting responsibility from the DOD to the Air Force and Navy—or choosing the older Super Hornet over the JSF—is more of a punishment than an optimal policy decision. There is no reason to believe the service branches will improve any aspect of a program that is more or less on track. And in spite of Boeing's 2013 Advanced Super Hornet concept, which generated a 50 percent improvement in stealth, the Super Hornet is still a fourth-generation fighter—same axe head, new handle.[43]

Although it is important to hold programs to account—and McCain and Trump are likely doing a good job of that—there is a balance to strike between demanding a return on an investment and showing patience with an especially complicated piece of technology. It is not as though program management acted irresponsibly with public money. As evidenced by their testimony at the Senate Armed Services Committee, the JSF management team—Frank Kendall, Lt Gen Christopher Bogdan, and Dr. Michael Gilmore—publicly acknowledged production schedule shortfalls and took steps to correct them. Impatience therefore demonstrated a degree of myopic, short-term thinking. Despite the propensity for setbacks when designing new technology, it is a necessary investment—a factor the private sector is familiar with.

Honda's Acura NSX

In January 1984, Japan's Honda Motor Company began research to develop an underfloor, midship-engine, rear-wheel drive sports car. Generally characterized as a practically oriented, front-engine/front-wheel drive, economical car company, Honda had returned to Formula One (F-1) racing just one year earlier. According to Honda engineer Shigeru Uehara, the company's aspiration in building a sports car was to bridge its mass production models with its F-1 cars. In addition, plans were being made to launch an Acura Division at American Honda, and the company needed a car that would serve as its flagship. After five years in design and development, the Acura NSX was unveiled at the 81st Chicago Auto Show in February 1989. With an elegant Pininfarina exterior that Honda claims was inspired by the F-16 fighter jet, the NSX was an instant success.[44] Many praised the car as revolutionary in that it irreversibly changed the supercar world. According to Motor Trend Channel's Johnny Lieberman, the 1989 Ferrari 348 represented a low point in Ferrari craftsmanship. Not only did the NSX perform better, it cost much less, did not break, and was easier to drive on a daily basis. "The NSX, in fact, blew people's minds. The entire industry sat up and took notice."[45]

A testament to the car's true original quality, between 1990 and 2005, only minor upgrades were made to keep the NSX popular. Unfortunately, in that time, the NSX was surpassed by many of its competitors, including a sedan by the Ford Motor Company: the 24-valve, double-overhead cam, V-6 Taurus.[46] Honda returned to the drawing board and in January 2007 unveiled the Acura Advanced Sports Car Concept. Boasting a powerful, front-mounted 5.0-liter V-10 engine, many assumed this to be the NSX successor. Later that year, Honda confirmed these assumptions and stated a possible introduction date of 2010. But the car was not well received.[47] Many did not like the exterior design, and supercar purists felt a front-mounted engine on an all-wheel drive car neglected Acura's powerful NSX lineage. Honda executives decided a second supercar concept would headline for Acura at the Tokyo auto show in October 2007, and not a production NSX as promised.[48]

In spite of making considerable advancements in a short period of time, by December 2008, CEO Takeo Fukui announced Honda would cancel the costly next-generation NSX program due to poor economic conditions. A strong Japanese yen caused US sales to plummet, and

Fukui cited a 67 percent drop in operating profits. But by early 2011, rumors of an NSX project revival were circulating. In April that year, Honda's president Takanobu Ito told Automotive News that an NSX successor was being developed but that it would be considerably different from previous designs. The difference Ito was alluding to was the pairing of Honda's 3.5-liter V-6 gasoline engine with a series of electric motors, making the car a hybrid.[49] This made the next generation NSX unique in the 2011 supercar world. But by mid-2012, new problems emerged. Needing to confront an era in which horsepower levels were increasing, NSX project leader Ted Klaus changed the performance targets and asked Honda's Japanese research and development executives for permission to add turbos. Permission was granted, but the problem Klaus soon discovered was that it is difficult to cool turbos on a transversely mounted V-6 engine. So Klaus scrapped the design again and started over, this time mounting the engine longitudinally.[50]

Honda finally unveiled its next generation NSX supercar at the North American International Auto Show in 2015. Although it received mixed-reviews, overall, the NSX was recognized as a complex masterpiece of modern engineering. In addition to a twin-turbo V-6 augmented by three electric motors for a total output of 573 horsepower, the NSX is host to computer software that changes everything from the drive mode to the electrohydraulic brakes. An additional piece of complex technology is the rapid torque vectoring system. The basic objective with torque vectoring is to enhance traction to improve high-speed handling by way of a computer that controls each of the front wheels individually: one can push forward while the other pushes back; they can both push forward; or they can both push back. This allows the computer to steer the NSX without the steering wheel moving.[51]

Honda's second generation NSX exemplifies the commonality of risk in developing new technology. SpaceX CEO Elon Musk anticipated the possibility of his Falcon 9 rockets crashing in the multiple attempts to execute mid-ocean landings on a robotic landing pad.[52] The company's fourth attempt in February 2016 ended in a fourth consecutive crash. Quick to determine the problem, SpaceX followed that crash with three successful landings in April and May 2016. Yet, problems persisted for Musk's ambitious plans.[53] Like the Falcon 9, the NSX required experimentation. Sometimes experiments pay off. As with the NSX, cancellations and redesigns were part of the process required to get it right. In

executing their vision for a new and profitable supercar, Honda executives had to be willing to scrap designs, wait for the right moment and start over. This required patience.

Results and Conclusions

The idea that public sector–led projects are slow and expensive is not incorrect, though it is often overstated. The meaning we attribute to a measurement is often the product of an exercise in comparison. Though this comparison would benefit from additional cases in both public- and private-sector production, a plausibility probe works as an effective starting point before additional research is undertaken. Especially with new and complex technological projects, problems—regardless of sector—should be expected. This is not to say problems should be accepted out-of-hand. Just as a company's shareholders are owed a return on their investment, a nation's citizens are owed efficient output in exchange for their tax-dollars; one set of concerns is commercially oriented, the other affects the national interest. The US government spends several trillion dollars a year.[54] Although it is beyond the scope of this article to develop a broader understanding of those expenses, a sizable portion of the budget covers unanticipated costs in government programs. The mistake is concluding all unanticipated costs qualify as waste. Creating new and innovative technology is complicated and is therefore riddled with unforeseen consequences. It appears neither public- nor private-sector projects are excused from this burden.

The JSF program was given approximately 10 years to deliver three similar, but different, fighter jets; by 2016, the program was five years past its deadline. Each of the three variants had to have stealth capabilities while satisfying a series of branch-specific requirements. Whereas the F-35A had to make room for an internal cannon, the F-35C required a larger wingspan, more robust landing gear, folding wingtips, and a larger internal fuel tank. Even more problematic, the F-35B had to have a STOVL capability. For 15 years, with only minor and mostly cosmetic changes, Honda kept producing the same NSX model it designed in the late 1980s. After 2005, it took an additional decade of cancellations and redesigns to deliver a second-generation Acura NSX. In designing and constructing the NSX, Honda was being squeezed by the pressure of delivering another revolutionary supercar. Honda decided that a new NSX not only had to look different from its Pininfarina predecessor,

but it also had to somehow look as elegant while providing the complex computerized luxuries drivers were becoming accustomed to.

But the primary complication shared by both the JSF program and the Acura NSX project was designing technically sophisticated equipment capable of reaching the speeds required to remain competitive in their relative spheres. Designed to be a stealth fighter, the JSF required all components (e.g. gas tanks and munitions) to be carried internally. Honda's objective of designing a truly modern supercar required including a variety of electronic luxuries and computer systems (e.g. dynamic mode selector, computerized electrohydraulic brakes, and torque vectoring). Whereas the F-35's airframe had to be scaled up to carry its components internally, the NSX required significantly more horsepower than its predecessor in order to hold its new technical components. Both the F-35 and NSX required larger, more powerful engines. Major setbacks in the delivery schedule were the result of complications in designing and accommodating their respective engines.

Honda was able to work through its design problems. These took considerable time and effort, but the result was an exceptionally modern, yet fast and effective supercar. Likewise, technical glitches with the F-35's computerized systems continued to slow delivery. Problems with the helmet system, for instance, drew attention to the project's highly innovative qualities, leading some to ask why the United States required a fighter jet more complex than the F-16 or F/A-18. Although technical glitches caused delays, scathing vitriol proclaiming it a disgrace was unnecessary.

At $400 billion for 2,457 aircraft, the program cost was almost twice the initial estimate.[55] But focusing on the price tag of an essential piece of military equipment distracts from the main issue, namely the F-35 is a vital component in the continuation of American military competitiveness.[56] Generally, "a state with airpower supremacy is in a position to dominate any location of its choosing by suppressing the naval and land forces of the opposing side."[57] The F-35 is an "engineering marvel"; its stealth technology will greatly increase strike capacity and lethality, thus providing the United States with continuing airpower competitiveness.[58] Specifically, the F-35 will not only be necessary in deterring Russian and Chinese aggression, but also it will be crucial to the success of overseas deployments. On the one hand, Russia, for instance, resumed its long-range bomber patrols near North American airspace in 2007.[59]

This concern has only been exacerbated by Russia's construction of a new long-range stealth bomber (the PAK-DA) in addition to resuming production of the Tu-160 Blackjack supersonic strategic bomber.[60] On the other hand, the proliferation of missile technology among irregular forces is increasing the danger of overseas deployments. As there is no compelling reason to believe the United States will altogether stop foreign military action, stealth capabilities will be an essential ingredient in the American airpower mix. In addition, the quantity and variety of American airpower will continue to be reduced, placing increased pressure on the level of sophistication in its remaining arsenal.[61]

There have been technological problems, and these have cost the US government considerably. This is the nature of inventing, designing, and producing complex, revolutionary technology.[62] Like the F-16, the F-4 Phantom, and the V-22 Osprey, examples of aeronautical design problems are the rule and not the exception. Indeed, it is the cost of doing business. But with these examples, we are also reminded that solutions are possible. The F-35 is certainly no exception to that. Congressional testimony from the JSF management team made clear the JSF program is progressing. Experts are solving problems as they arise and meeting evolving objectives, including demands for a lower "flyaway" cost.[63]

Americans, like Honda shareholders, deserve an honest account of how and where their money is spent. They also deserve successful returns. However, they are owed explanations of public spending that account for what the government is trying to achieve on a wider scale. On the surface, a budget-led acquisition approach appears sensible. Applying it to government spending coincides with a neoliberal political ideology that appeals to the millions of middle-class Americans trying to run their households in the face of rising living costs and stagnant wages. But the US government is not a household. It is the most powerful, and by extension the most threatened, nation-state in the system. In their article on the military's responsibility to lead technological development, Newt Gingrich and Ronald Weisbrook argue that to prevent the eclipse of American military supremacy requires a recapturing of the "urgency and capability of past national mobilization efforts."[64] Although "supremacy" may not be attainable or even necessary, US competitiveness is essential.[65] Remaining competitive requires the modest degree of patience necessary to support and complete important military technology programs. Just as late-nineteenth century economic

interests demanded a Mahanian three-link chain approach, twenty-first century security interests necessitate continual investment in sophisticated military technology.[66]

Contrary to neoliberal idealism, public-sector programs are not that different from their private-sector counterparts. Especially when new and innovative technologies are being designed, problems are often imminent. This is the cost of doing business. Honda looked carefully at the future of supercar ingenuity, realized the past's technology was going to be replaced, and decided to reach ahead by engineering something special. Succinctly stated by Seyth Miersma, executive editor at *Motor1*, "Acura's intricately driven NSX is a compelling preview of how sports cars will exist in the years soon to come."[67] The process of reaching ahead was challenging for Honda—but a worthwhile investment. The same can be said for the ongoing JSF program. Despite a number of significant problems, the US DOD has persevered to develop an aircraft that will replace aging equipment, revolutionize the way American fighter pilots conduct air warfare, and reaffirm American airpower capabilities in the emerging multi-polar system. Given the long-term strategic implications of the F-35 family, schedule setbacks constitute a modest sacrifice that deserves patience. In his last speech addressing national reunification following the Civil War, Abraham Lincoln said, "We shall sooner have the fowl by hatching the egg than by smashing it."[68] SSQ

Notes

1. Richard Lardner, "Senator Says Fighter Program Has Been Scandal and Tragedy," *Associated Press*, 26 April 2016, http://bigstory.ap.org/article/5f64228336014b158de3d8b351ec728e/senator-says-fighter-program-has-been-scandal-and-tragedy.

2. Valerie Insinna, "Trump Makes the 'Out Of Control' F-35 His Latest Target," *Defense News*, 12 December 2016, http://www.defensenews.com/articles/trump-makes-the-out-of-control-f-35-his-latest-target.

3. David Pugliese, "Super Hornet Could Face Some Tough Opposition in the Battle against the F-35," *Ottawa Citizen*, 5 April 2017, http://ottawacitizen.com/news/national/defence-watch/super-hornet-could-face-some-tough-opposition-in-the-battle-against-the-f-35.

4. Mark A. Lorell, Michael Kennedy, Robert S. Leonard, Ken Munson, Shmuel Abramzon, David L. An, and Robert A. Guffey, *Do Joint Fighter Programs Save Money?* (Washington, DC: Rand Corporation, 2013).

5. Robert A. Dahl, and Charles E. Lindblom, *Politics, Economics and Welfare* (New York: Harper & Brothers, 1953); Anthony Downs, *Inside Bureaucracy* (Boston: Little, Brown, 1967); Richard E. Boyatzis, *The Competent Manager: A Model for Effective Performance* (New York: Wiley, 1982);

Emanuel S. Savas, *How to Shrink Government: Privatizing the Public Sector* (Chatham, NJ: Chatham House, 1982); Michael Keating, "Quo Vadis? Challenges of Public Administration," *Australian Journal of Public Administration* 48, no. 2 (June 1989): 123–31, http://doi.org/d7shtn; Thomas I. Palley, "From Keynesianism to Neoliberalism: Shifting Paradigms in Economics," *Foreign Policy in Focus* (May 2004), http://fpif.org/from_keynesianism_to_neoliberalism_shifting_paradigms_in_economics/; Jonathan D. Ostry, Prakash Loungani, and Davide Furceri, "Neoliberalism: Oversold?," *Finance and Development* 53 no. 2 (June 2016): 38–41, http://www.imf.org/external/pubs/ft/fandd/2016/06/pdf/ostry.pdf; and Thomas Volscho, "The Revenge of the Capitalist Class: Crisis, the Legitimacy of Capitalism and the Restoration of Finance from the 1970s to the Present," *Critical Sociology* 43 no. 2 (2017): 249–66, http://doi.org/cdb6.

6. John A. Alic, "Managing US Defense Acquisition," *Enterprise & Society* 14, no. 1 (March 2013): 30, http://www.jstor.org/stable/23701646. Alic does not specifically mention neoliberalism, but he does discuss the problem with the assumption private sector models necessarily improve military procurement. He notes there could be an argument emulation of private firms would be appropriate for "relatively straightforward administrative functions, including the five million or so routine contract actions that Department of Defense (DOD) personnel execute each year, not for major acquisition programs." Alic uses the JSF program as an example of a major acquisition program.

7. Rhys Andrews and Stephen van de Walle, "New Public Management and Citizens' Perceptions of Local Service Efficiency, Responsiveness, Equity and Effectiveness" (working paper, Coordinating for Cohesion in the Public Sector of the Future [COCOPS], no. 7, June 2012), http://www.cocops.eu/wp-content/uploads/2012/08/COCOPS_workingpaper_No7-.pdf.

8. Carsten Anckar, "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research," *International Journal of Social Research Methodology* 11, no. 5 (December 2008): 389–401, http://doi.org/drws9g. Because the JSF program and the Acura NSX project are dissimilar in many respects, this article falls under the investigative rubric of the Most Different Systems Design. This method can be used to compare cases that, despite certain dissimilarities, possess the same dependent variable. The basic idea is to show that cases with different structural characteristics can generate similar outcomes.

9. Alexander L. George and Andrew Bennett, *Case Studies in Theory Development in the Social Sciences* (Cambridge, MA: MIT Press, 2005); and Jack S. Levy, "Case Studies: Types, Designs, and Logics of Inference," *Conflict Management and Peace Science* 25 (2008): 1–18, http://doi.org/dd4wfx. George and Bennet define a plausibility probe as a preliminary study on a relatively untested theory to determine whether more intensive testing is warranted. The theoretical purpose of this article is to show that both public- and private-sector technology projects experience delays and setbacks, a factor neoliberal political culture neglects to acknowledge. A plausibility probe is a way of developing this theory before approaching a multi-case analysis.

10. J. Ronald Fox, *The Defense Management Challenge: Weapons Acquisition* (Boston: Harvard Business School Press, 1988); Thomas L. McNaugher, *New Weapons, Old Politics: America's Military Procurement Muddle* (Washington, DC: Brookings Institutions, 1989); Elizabeth Kier, *Imagining War: French and British Military Doctrine between the Wars* (Princeton, NJ: Princeton University Press, 1997); Terry Terriff, "Innovate or Die: Organizational Culture and the Origins of Maneuver Warfare in the United States Marine Corps," *Journal of Strategic Studies* 29, no. 3 (2006): 475–503, http://doi.org/c9xxns; Alic, "Managing US Defense Acquisition"; Donald MacKenzie, *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance* (Cambridge, MA: MIT Press, 1990); Thomas Hone, Norman Friedman, and Mark Mandeles, *American and British Aircraft Carrier Development, 1919-1941* (Annapolis, MD: Naval Institute Press, 1999); and J. Ronald Fox, *Defense Acquisition Reform, 1960-2009: An*

Elusive Goal (Washington, DC: Center of Military History, United States Army, 2011). There is a considerable amount of literature examining American military procurement. As noted by Harvard faculty member J. Ronald Fox, a sizable amount of it includes studies commissioned by presidents, Congress, secretaries of defense, government agencies, studies and analyses organizations, and universities. One such study in particular is Fox's own *Defense Management Challenge*, which deals with the roles of government personnel in procuring military equipment, as well as various other aspects of the acquisition process, such as cost estimating. Other American military procurement literature deals with the interplay of the various organizations and players involved in procurement and suboptimal outcomes such as cost overruns, schedule slippage, and contract cancellations. Thomas McNaugher identifies the complex technical interaction between a military interested in improved weapons systems, a political sector focused on appeasing constituent interests, and a bureaucracy with procedural obsessions and parochial budgetary concerns. Despite this and other literature describing the bureaucratic political aspects of military procurement, the research dealing with American acquisitions has not yet addressed the effects neoliberal political cultural has on acquisitions.

There is of course, a more than sufficient amount of literature examining the role culture plays in shaping the military, both in terms of the doctrines they pursue as well as the weapons acquired to pursue these doctrines. For example, Elizabeth Kier examines the role French and British political values played in forming interwar defense policy. Budget choices of course affected the doctrinal and military capabilities of the French and British forces, as well as what type of weapons they could afford, which largely dictated what they could do. Terry Terriff argues that following the Vietnam War the US Marine Corps was forced to adapt its mystical amphibious marine warfare culture by innovating towards a total mechanized force, emphasizing mobility and maneuver warfare.

John Alic notes there has been a modest number of works dealing with military technological innovation. Donald MacKenzie's book considers both technical and political-organizational issues of the nuclear missile age. He tries to show that continued innovation in missile technology is a product of institutional structures, not a natural course of evolution. Take away those structures, and nuclear missile innovation crumbles. Seeking to understand why the Royal Navy and US Navy went in different and unique directions with regard to aircraft carrier innovation, Thomas Hone, Norman Friedman, and Mark Mandeles examine the interaction between strategy, technological alternatives, and organizational politics. Alic's 2013 article argues the business models used in major DOD investments in innovation, such as the F-35 Joint Strike Fighter, are not necessarily compatible with major private-sector investment models. Reform, Alic states, would begin with legislation further limiting the influence of individual services over weapons choice, augmented by greater civilian control.

Alic carries his argument into his review of Ronald Fox's 2011 book on defense acquisition reform in the US. In analyzing 27 studies on defense procurement in the United States, Fox argues what the DOD requires is better trained defense acquisition managers, proficient in the complex and continuing negotiations between government departments and large industrial firms—moreover, managers that emulate private sector practices. Based on his own extensive research, Alic argues there is no evidence to suggest emulating private-sector management practices would guarantee better organizational performance.

Alic reminds us that following World War II, as civilian control over military procurement was slowly reasserted, elements of private-sector managerial practices followed close behind. As secretary of defense, beginning in 1961, Robert McNamara instituted administrative procedures, along with the planning, programming, and budgeting system, that evoked practices widespread in private industry. In spite of best efforts, procurement schedules remained

lengthy, and budgets continued to grow to cover their costs. It is here where this article on the JSF proceeds. The misconception that efficiency is intrinsic to private-sector practice and that if only the public sector could emulate such practice, programs would be delivered on time and on budget, is reflection of a neoliberal political culture. This article seeks to examine this contention through the JSF and NSX cases.

11. Palley, "From Keynesianism to Neoliberalism."

12. Alic, "Managing US Defense Acquisition," 30.

13. Robert Perry, Giles K. Smith, Alvin J. Harman, and Susan Henrichsen, *System Acquisition Strategies* (Santa Monica, CA: United States Air Force Project Rand and Advanced Research Projects Agency, June 1971): 39, http://www.dtic.mil/dtic/tr/fulltext/u2/730921.pdf.

14. Fox, *Defense Acquisition Reform*.

15. Bruce Buchanan II, "Red-Tape and the Service Ethic: Some Unexpected Differences between Public and Private Managers," *Administration and Society* 6 no. 4 (February 1975): 423–44, http://doi.org/ft3thf. Also see Elizabeth Kier, *Imagining War: French and British Military Doctrine between the Wars* (Princeton, NJ: Princeton University Press, 1997), 28. Kier defines culture as "a set of basic assumptions, values, norms, beliefs and formal knowledge that shape collective understandings."

16. Eva Brann, "A Reading of the Gettysburg Address," in *Abraham Lincoln, The Gettysburg Address, and American Constitutionalism*, ed. Leo Paul S. de Alvarez (Irving, TX: University of Dallas Press, 1976), 15–53; Walter R. Mead, *Special Providence: American Foreign Policy and How It Changed the World* (New York: Alfred A. Knopf); and John Locke, *Two Treatises of Government* (New York: Cambridge University Press, [1689] 1988). Thomas Jefferson, who composed the original draft of the Declaration of Independence, borrowed from seventeenth-century English political theorist John Locke. Locke's *Two Treatises of Government* argued that although people in the state of nature transferred some of their rights to a central authority in exchange for a stable society, government not only requires the consent of the governed but also must be restricted to a minimal role in society. Because individuals are rational and self-interested and therefore in the best position to care for themselves, classical liberals like Locke argued for limited state power, primarily ensuring the right to liberty and protection of property. Governments that failed in these duties or acted tyrannically—as in the case of British Monarch George III toward the Thirteen Colonies—had to be overthrown. This suspicious mindset exists to this day in the United States, sometimes to the benefit of the country, but not always.

17. Suzan Ilcan, "Privatizing Responsibility: Public Sector Reform under Neoliberal Government," *Canadian Review of Sociology* 46, no. 3 (August 2009): 207–34, http://doi.org/cw3f29.

18. Donald P. Warwick, *A Theory of Public Bureaucracy: Politics, Personality, and Organization in the State Department* (Cambridge, MA: Harvard University Press, 1975), 3.

19. Ilcan, "Privatizing Responsibility," 211.

20. Thomas Volscho, "The Revenge of the Capitalist Class: Crisis, the Legitimacy of Capitalism and the Restoration of Finance from the 1970s to Present," *Critical Sociology* 43, no. 2 (2017): 18, http://doi.org/cdb6.

21. Ostry, Loungani, and Furceri, "Neoliberalism: Oversold?." Also see Campbell Parker Jones and Rene Martin ten Bos, "For Business Ethics" (New York: Routledge, 2005).

22. Volscho, "Revenge of the Capitalist Class," 17; Gérard Duménil and Dominique Lévy, *The Crisis of Neoliberalism* (Cambridge, MA: Harvard University Press, 2011), 17; and John A. Alic, *Trillions for Military Technology: How the Pentagon Innovates and Why It Costs so Much* (New York: Palgrave MacMillan, 2007), 2, 10, 50. Although Duménil and Lévy refer to President Ronald Reagan as one of the "emblematic figures" of neoliberalism, Alic points out Reagan presided over a major defense buildup, even though the Cold War was coming to a close.

Cancelled by the Carter administration, the B1-bomber entered production when Reagan took office. Designed to outpace Soviet fighter technology, design work on the F-22 began in the early years of Reagan's presidency. By 1989, the defense budget had reached $300 billion, a figure that was not increased until 2002. The irony is not lost. However, in politics, actions do not always reflect rhetoric. Sometimes circumstances change, and campaign promises get ignored. But other times, rhetoric can catch on with voters, requiring a president to follow through on a promise, even if it no longer makes sense to do so.

23. Christopher Hood, "A Public Management for All Seasons?," *Public Administration* 69, no. 1 (Spring 1991): 5, http://doi.org/bdwbfj.

24. See note 5.

25. Mia De Graaf and Mark Prigg, "John McCain Slams F-35 Striker Jet Project as "a Scandal,'" *Daily Mail Online*, 27 April 2016, http://www.dailymail.co.uk/news/article-3562189/John-McCain-slams-F-35-striker-jet-project-scandal-disgraceful-aircraft-s-development-stretches-15th-year-costing-Pentagon-nearly-400-BILLION.html.

26. Lorell, et al., *Do Joint Fighter Programs Save Money?*, 1. The US DOD has started numerous joint tactical fighter programs since the 1960s. The conventional wisdom behind these programs was that one common airframe could be used to support the needs of the USAF, USN, and USMC, with reduced costs. Savings would be found by "eliminating duplicate research, development, test, and evaluation (RDT&E) efforts and by realizing economies of scale." According to Lorell et al., this approach towards commonality and integration complicates already sizable technical challenges leading to cost growth that could negate potential savings. What these authors fail to acknowledge are the minor successes that emerged from ambitious joint programs like the Tactical Fighter, Experimental (TFX), and the Air Combat Fighter. In spite of a failure to achieve 100 percent commonality between a variety of service aircrafts, the TFX produced the highly successful F-111A as well as the incredibly successful A-10 from the close air support portion of the project. These projects are meant to supply American military needs, but they are also acknowledged to some degree as experimental. It is well known ahead of time there will be problems. Acting astonished after schedule slippage is asinine.

27. Bill Sweetman, *Ultimate Fighter: Lockheed Martin F-35 Joint Strike Fighter* (Saint Paul, MN: Zenith Press, 2004), 22–47.

28. Ibid., 94. Interestingly, Pentagon acquisition chief Pete Aldridge's announcement stated the incorrect designation. The previous fighter in the US designation system was Northrop's YF-23A. The JSF should have therefore been the F-24. At the conference, a reporter asked Aldridge about the designation. Not knowing the answer off-hand, Aldridge turned to Program Director General Mike Hough. "Momentarily confused, Hough said 'X-35.'" Aldridge misheard him and stated the designation as F-35. Instead of the Pentagon admitting a mistake, the JSF office officially requested F-35 under the Mission Design Series, on the grounds that it was consistent with Aldridge's statement.

29. Gerard Keijsper, *Lockheed F-35 Joint Strike Fighter: Design and Development of the International Aircraft* (South Yorkshire, UK: Pen & Sword Aviation, 2007), 34.

30. "Conventional Takeoff and Landing Variant, F-35A Lightning II," Lockheed Martin, 2016, accessed 24 January 2017, https://www.f35.com/about/variants/f35a.

31. "Short Takeoff/Vertical Landing, F-35B Lightning II," Lockheed Martin, 2016, accessed 24 January 2017, https://www.f35.com/about/variants/f35b.

32. "Carrier Variant, F-35C Lightning II," Lockheed Martin, 2016, accessed 24 January 2017, https://www.f35.com/about/variants/f35c.

33. Andy Nativi, "F-35 Air Combat Skills Analyzed," *Aviation Week*, 5 March 2009, http://aviationweek.com/awin/f-35-s-air-combat-skills-analyzed.

34. Guy Norris, "Pratt Raises Stakes in JSF Engine Battle," *Aviation Week*, 27 August 2010, http://aviationweek.com/awin/pratt-raises-stakes-jsf-engine-battle-0.

35. Keijsper, *Lockheed F-35 Joint Strike Fighter*, 199.

36. Ibid., 200–2.

37. Reuven Ben-Shalom, "Cultural Prism: Supremacy, Lethality and Transparency," *The Jerusalem Post*, 16 June 2016, http://www.jpost.com/Opinion/Supremacy-lethality-and-transparency-457023. Also see Director of Operational Test and Evaluation, *FY 2015 Annual Report* (Washington, DC: Department of Defense, 2016), http://www.dote.osd.mil/pub/reports/FY2015/pdf/other/2015DOTEAnnualReport.pdf.

38. Christian Davenport, "Meet the Most Fascinating Part of the F-35: the $400,000 Helmet," *Washington Post*, 1 April 2015, https://www.washingtonpost.com/news/checkpoint/wp/2015/04/01/meet-the-most-fascinating-part-of-the-f-35-the-400000-helmet/. Also see Director of Operational Test and Evaluation, *FY 2015 Annual Report,* (Washington, DC: Department of Defense, 2016), http://www.dote.osd.mil/pub/reports/FY2015/pdf/other/2015DOTEAnnualReport.pdf.

39. Loren Thompson, "Why Sen. McCain Is Right in Trying to Put the Military Services in Charge of Buying Weapons," *Forbes*, 28 September 2015, http://www.forbes.com/sites/lorenthompson/2015/09/08/why-sen-mccain-is-right-to-put-the-military-services-in-charge-of-buying-weapons/#3e056c692933.

40. US Senate Committee on Armed Services, *National Defense Authorization Act for Fiscal Year 2017: Bill Summary* (Washington, DC, 2016), 11, http://www.armed-services.senate.gov/imo/media/doc/FY17%20NDAA%20Bill%20Summary.pdf.

41. Dave Majumdar, "US Senate Proposes to Disband F-35 Joint Program Office," *The National Interest*, 13 May 2016, http://nationalinterest.org/blog/the-buzz/us-senate-proposes-disband-f-35-joint-program-office-16206.

42. Alic, "Managing US Defense Acquisition."

43. Eric Tegler, "Could Trump Really Replace the F-35 with a Super Hornet? No. But also Yes," *Popular Mechanics*, 10 January 2017, http://www.popularmechanics.com/military/aviation/a24682/f-35-vs-super-hornet/.

44. "Let's Build a Sportscar!," Honda Corporation, 2005, http://world.honda.com/history/challenge/1990thensx/index.html.

45. Johnny Lieberman, "Lexus LFA versus Acura NSX!," 25 July 2012, in Motor Trend Channel's Head 2 Head, episode 13, video, 17:07, https://www.youtube.com/watch?v=zLJ2lw0bCkk&index=9&list=PLXooetYap97WexVvxqJQs0zCsPySCYhDh; and Jason Cammisa, "2017 Acura NSX: The Slowest Supercar in the World?," 7 December 2015, in Motor Trend Channel's Ignition, episode 143, video, 13:35, https://www.youtube.com/watch?v=GUDLUSqfqxg.

46. Lieberman, "Lexus LFA versus Acura NSX!"

47. Jake Holmes, "2010 Acura NSX: No Longer a Design Study, the New NSX Shows its Face," *Car and Driver*, June 2008, http://www.caranddriver.com/spy-shots/2010-acura-nsx-spied-1.

48. Alissa Priddle, "Acura Supercar Concept, Part 2," *Car and Driver*, September 2007, http://www.caranddriver.com/news/acura-supercar-concept-part-2-auto-shows.

49. Jake Holmes, "Revival, Part Deux: Honda President Dishes on New NSX Successor," *Automobile*, 25 April 2011, http://www.automobilemag.com/news/revival-part-deux-honda-president-dishes-new-nsx-successor-42779/.

50. Aaron Robinson, "2016 Acura NSX Dissected: Powertrain, Chassis, and More," *Car and Driver*, April 2015, http://www.caranddriver.com/features/2016-acura-nsx-dissected

-powertrain-chassis-and-more-feature; and Cammisa, "2017 Acura NSX: The Slowest Supercar in the World?"

51. Cammisa, "2017 Acura NSX."

52. Maya Kosoff, "Elon Musk Wants You to Know His Rocket Will Probably Crash," *Vanity Fair*, 23 February 2016, http://www.vanityfair.com/news/2016/02/elon-musk-wants-you-to-know-his-rocket-will-probably-crash.

53. Ali Sundermier, "Here's Why SpaceX Crash Landed its Most Recent Rocket," *Business Insider*, 17 June 2016, http://www.businessinsider.com/why-spacex-crash-landed-falcon-9-rocket.

54. Jeanne Sahadi, "U.S. Deficit Now Lowest since 2007," *CNN Money*, 15 October 2015, http://money.cnn.com/2015/10/15/news/economy/budget-deficit/.

55. Ryan Browne, "John McCain: F-35 Is 'A Scandal and A Tragedy,' " *CNN Politics*, 27 April 2016, http://www.cnn.com/2016/04/26/politics/f-35-delay-air-force/.

56. Given the re-emergence of sophisticated Russian and Chinese weaponry, the rational cost of remaining competitive is continued weapons experimentation and development, an expensive proposition. Congressional anxiety based on cost overruns and schedule slippage not only reflects neoliberal ideals, but it also qualifies as a nonrational response because complex military technology like the JSF program is inherently risk oriented. Congress wants primacy but does not always accept the trade-offs necessary to at least remain competitive.

57. Rob Huebert, "The Future of Canadian Airpower and the F-35," *Canadian Foreign Policy Journal* 17, no. 3 (September 2011): 229, http://doi.org/cdb8.

58. Ben-Shalom, "Cultural Prism." It is predicted bi-static radar and infrared will impair stealth aircraft success more than in the past.

59. Reuters, "Russia Restores Bomber Patrols," CNN, 17 August 2007, http://www.cnn.com/2007/WORLD/europe/08/17/russia.airforce.reut/index.html?iref=newssearch.

60. Dave Majumdar, "Russia to Build Lethal PAK-DA Stealth Bomber—with Hypersonic Weapons?," *The National Interest*, 18 April 2016, http://nationalinterest.org/blog/the-buzz/russia-build-lethal-pak-da-stealth-bomber%E2%80%94-hypersonic-15821.

61. Huebert, "Future of Canadian Airpower and the F-35," 232–4.

62. The term "revolutionary" is used here to describe something that irreversibly changes the nature of its respective field. For instance, a revolutionary piece of military technology irreversibly changes the nature of warfare. Also see Lorell, et al., *Do Joint Fighter Programs Save Money?* The TFX program had a similar problem providing maximum system commonality while meeting important individual service requirements. What began in June 1961 as a joint fighter program between the Air Force and Navy eventually led to a split in which the Air Force procured the F-111A and the Navy procured the F-14A Tomcat, a fighter with 20 per cent commonality to the F-111A. In spite of the split, the program led to two success stories. Given time, something good will come of the Joint Strike Fighter program.

63. Ben-Shalom, "Cultural Prism"; and Marcus Weisgerber, "The Price of an F-35 Was Already Falling. Can Trump Drive it Lower?," *Defense One*, 27 January 2017, http://www.defenseone.com/business/2017/01/f-35s-price-has-been-falling-can-trump-lower-it-even-more/134919/.

64. Newt Gingrich and Ronald E. Weisbrook, "Adapt or Die: The US Military's Responsibility to Protect America by Leading the Transformations in Science and Technology," *Strategic Studies Quarterly* 1, no. 2 (Winter 2007): 25, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-01_Issue-2/Winter07.pdf.

65. Stephen Walt, "American Primacy: Its Prospects and Pitfalls," *Naval War College Review* 55, no. 2 (Spring 2002): 9–28, https://usnwc2.usnwc.edu/Publications/Naval-War-College-Review/2002---Spring.aspx; Robert Farley, "Yes, America's Military Supremacy Is Fading (And

We Should Not Panic)," *The National Interest*, 21 September 2015, http://nationalinterest.org/feature/yes-americas-military-supremacy-fading-not-its-superiority-13885?page=3; and Kenneth Waltz, "Why Iran Should Get the Bomb," *Foreign Affairs* 91, no. 4 (July/August 2012): 2–5, https://www.foreignaffairs.com/articles/iran/2012-06-15/why-iran-should-get-bomb. Others have argued perpetual US military primacy is not necessary. For instance, neorealist Stephen Walt questions whether "increasing the US lead" is worth the effort. He acknowledges the value of maintaining US strength in both relative and absolute terms but is hesitant to argue primacy is a long-term necessity.

Robert Farley argues the advantages of unipolarity and military supremacy the US enjoyed in the 1990s were ephemeral and an anomaly in the broader history of global politics. The shrinking gap between the United States, China, and Russia indicates a return to a more normal balance of power. Farley makes the distinction that while "superiority" is possible, "supremacy" is not a practical nor even a necessary goal.

Kenneth Waltz applies a similar logic to concerns over Iranian nuclear ambitions. Flowing primarily from the United States and Israel, concerns are partly based on the notion the Middle East and the world would be safer without a nuclearized Iran. Waltz argues this is simply not true. Israel would not be destroyed by an irrational Iranian first strike attack, and the world would not descend into chaos as an emboldened Iran supplied Shia terrorist groups with nuclear materials, and every state with a reasonable chance of building nuclear weapons would proliferate and attack one another.

As the twenty-first century continues to reveal a slightly more proportional balance of power, neither Israel nor the United States should expect continued supremacy. However, while superiority is possible, competitiveness is essential. The United States is in no way entitled to rely solely on complex interdependence. It must buttress its use of international institutions and trade relations with investments in key strategic assets such as the JSF.

66. Alfred Thayer Mahan, *The Influence of Sea Power upon History, 1660-1805* (Boston: Little, Brown, & Co., 1890; reprinted together with extracts from *The Influence of Sea Power upon the French Revolution and Empire, 1793–1812* [London: Hamlyn Publishing Group; A Bison Book, 1980]), 57. Greatly concerned the United States was squandering its opportunity to secure a piece of global economic dominance, nineteenth-century naval historian Alfred Thayer Mahan argued the undeniable relationship between commercial success and naval power required protection of America's coastal approaches, harbors, and inlets; Mahan also emphasized home industrial production, shipping of industrial goods with naval protection and foreign bases, and colonies to provide material resources and marketplaces.

67. Seyth Miersma, "After an Interminable Wait, Acura's Second NSX Is Here, and It's Brought the Future with It," Motor1.com, 23 May 2016, http://www.motor1.com/reviews/62927/first-drive-2017-acura-nsx/.

68. "Last Public Address, April 11, 1865," Abraham Lincoln Online, accessed 11 January 2017, http://www.abrahamlincolnonline.org/lincoln/speeches/last.htm.

Rethinking the US Nuclear Triad

Darius E. Watson

Abstract

For over 50 years, the structure of the US nuclear triad has remained the same. Relying on strategic bombers, intercontinental ballistic missiles (ICBM), and submarine-launched ballistic missiles (SLBM), the United States has sought to deter strategic threats from a variety of sources. The current threat environment, however, is radically different from what was being considered when the triad was created. From the continued evolution of terrorism to the increasing threat of cyberattacks, both the nature of the threats facing the United States and the deterrence frameworks necessary to counter them have changed. The United States needs to critically reassess the current triad with an eye toward eliminating redundant or potentially ineffective delivery systems such as the strategic nuclear bomber.

✳ ✳ ✳ ✳ ✳

The US nuclear triad has been the foundation of the country's strategic deterrence framework since the mid-1960s. Comprising strategic bombers, intercontinental ballistic missiles (ICBM), and submarine launched ballistic missiles (SLBM), the triad has been the backbone of US efforts to deter threats from other states. From an analytical perspective, proving the effectiveness of deterrence is highly problematic. "After all," wrote noted strategy scholar Colin Gray, "episodes of successful deterrence are recorded as blanks in the pages of history books."[1] However, from the policy perspective, the US "victory" in the Cold War has come, for many, to represent clear evidence that the nuclear triad, and US strategic deterrence in general, have been successful. As a result, the United States continues to maintain the same general framework developed over 60

Darius Watson is a professor of political science and security studies as well as a senior consultant at Watson Consulting & Analysis, LLC. He earned a doctorate in international relations from the State University of New York–Albany.

years ago to combat an aggressive Soviet Union that no longer exists. There are undoubtedly still traditional state-level nuclear threats that require a robust and dynamic nuclear component to US strategic deterrence. But changes in the international threat environment since the end of the Cold War now require the United States to reevaluate that framework critically. From the evolution of terrorism to the rapid rise of cyber and space threats, traditional state-level nuclear attack no longer represents the primary threat to be deterred by the United States. Thus, it is time the US strategic deterrent reflect this new reality.

To begin the debate, this analysis specifically considers the continuing utility of the strategic bomber leg of the nuclear triad. As the first component of the US nuclear triad, the strategic bomber fleet represents both the historical and practical foundations of US strategic deterrence. For the entirety of the Cold War, strategic bomber forces were the primary component of the triad due to the wide variety of basing options offered vis-à-vis both strategic and extended deterrence policies.[2] As a result, bombers also became the central method through which the United States conducted "signaling" as a component of the threat-response framework associated with strategic deterrence. For many, their greatest asset was their flexibility relative to doctrine and planning due to their ability to be recalled.[3] Finally, they represent the long-standing central importance of the Air Force in the development of US strategic deterrence policy. It is the strategic bomber that created historical and contemporary perceptions of the "vital" role of airpower for US nuclear deterrence and stood as a symbol of US power in general.

The decline in the potential applicability and relative effectiveness of the strategic bomber is at the core of the current debate.[4] The argument offered here is that these underlying rationales for continuing investment and development of strategic nuclear bomber forces are either outdated regarding the threat environment, ineffective due to technological advancements, or increasingly inefficient because of the relative unit cost for nuclear deterrence attained through ICBMs and SLBMs. The United States must begin to consider eliminating the strategic bomber leg of the nuclear triad to both streamline the nuclear deterrent and permit strengthening deterrence within the cyber and space domains.

Why the Triad?

One of the most important things to consider regarding the current structure of the US nuclear triad is that it was never planned. The current reliance on strategic bombers, ICBMs, and SLBMs is the direct result of an intertwined evolution of nuclear weapon and delivery system technologies, changes within the global strategic environment, and "because each of the military services wanted to play a role in the US nuclear arsenal."[5] Thus, the rationale for the nuclear triad was never based on a clear and consistent understanding of US strategic threats, interests, and needed capabilities. Instead, it is the result of sometimes ad hoc responses to a wide variety of often disconnected technological, political, military, and bureaucratic considerations. This in turn has led to an enormous commitment to maintain the triad despite long-standing questions regarding both its effectiveness and efficiency.

In examining the continued utility of the strategic bomber as a leg of the nuclear triad, it is important to examine two specific arguments behind its perceived importance to US strategic deterrence: its historical position as a nuclear delivery system and the symbol of US global power and its flexibility relative to nuclear doctrines and geostrategy. These two considerations have created a commitment to the strategic bomber leg of the nuclear triad that hinders further development and improvement of other US strategic deterrence capabilities in general. The doctrinal focus on a "flexible nuclear response" that was created under the Kennedy administration in early 1960s would become the foundation of the belief in the need for a nuclear triad—and strategic bombers specifically.[6] However, the continued use of World War II–era perspectives on strategic bombing in conjunction with conventional conflicts such as the Vietnam War obscured necessary questions regarding its utility as a nuclear delivery system. Over time, this leg of the nuclear triad also came to represent the primary signaling mechanism toward the Soviet Union, as it was considered "the only portion of the triad that provides the ability for signaling of alert readiness changes (signs of escalation)."[7] Both considerations in turn served to reinforce the long-standing historical perception of airpower as the primary illustration of strategic power and thus the logical foundation of US strategic deterrence. The result has been a commitment to the strategic bomber leg of the nuclear triad driven by outdated arguments and perspectives, rather than a comprehensive understanding of its value to contemporary US strategic deterrence efforts.

Nuclear Deterrence and Nuclear Bombers

The strategic bomber has enjoyed a unique position within the nuclear triad and US deterrence efforts precisely because it was the first (and still the only) delivery method that has been used. This position has assured that regardless of the rhetoric and reality associated with the various developments of US nuclear doctrine, the bomber has always assumed an unquestioned role in the nuclear triad. Prior to development of the ICBM (and later the SLBM), "concepts of strategic bombing that had emerged before and during the Second World War [continued] to provide an adequate framework for thinking about how atomic war would be fought."[8] This meant that the highly quantified and sterile examinations of strategic bombing during World War II then became the foundation of US nuclear doctrine well into the 1960s. This is typified by the widely held belief during much of the Cold War that the problem of creating a nuclear doctrine that satisfied deterrence and war-making requirements in the thermonuclear age "was in essence an economic problem—and thus the kind of problem that professional economists were best equipped to deal with."[9] While there was recognition of an increase in the level of destructiveness associated with the new weapon, there was a more general assumption that the nature of war had not really changed. But the development of the hydrogen bomb in 1952 was the first of many technological advancements that would challenge this assumption and as a result affect US nuclear policy. It certainly played a role in the development of the policy of massive retaliation under the Eisenhower administration, as well as in the growing concerns and resistance to it as US nuclear policy.[10] The exponential increase in the destructive capability of thermonuclear weapons for many threatened to undermine traditional relationships between political goals and war. This in turn would lead to deeper questions regarding the very morality of nuclear weapons and the use of various deterrence strategies. Regardless of the problems associated with exactly how and when thermonuclear weapons would be used, there was little question during the majority of the 1950s that the strategic bomber would be the primary weapon of the next war.

During the early 1960s the strategic bomber was still the unquestioned central pillar of US deterrence strategies. Although ICBM technologies were rapidly improving the viability of US second-strike capabilities, it was commonly understood that US bomber forces still represented the

primary strategic deterrent for the United States. A significant part of this psychology was directly related to the US experience with strategic airpower during World War II and the clear belief that it had played a decisive role in the defeat of Germany and Japan.[11] With the advent of nuclear weapons, this perception of strategic airpower as the central component of US global power was strengthened. The combination of US victory in World War II and its nuclear dominance in the immediate postwar period created a psychology in which critical evaluation of the role of bombers in nuclear deterrence seemed unnecessary. According to airpower historian Richard R. Muller, "the advent of nuclear weapons was seen initially as a quantitative, though not necessarily qualitative, change in the means of conducting aerial warfare."[12] Not only did this serve to ensure the role of bombers in the nuclear triad would not be questioned later, but it also cemented the Air Force and the doctrine of massive retaliation as the cornerstones of US deterrence policy.

In the early 1950s, Air Force bombers were the nation's primary means for delivering strategic nuclear weapons, and the Air Force also had the lead in developing missile technology. Its budget authority went from $11.5 billion in 1954, in the wake of the Korean War, to $18.6 billion in 1960—about a 25 percent increase adjusting for inflation.[13]

The result was the unquestioned commitment to strategic bombers as part of the US nuclear triad, despite growing evidence that both ICBM and SLBM technologies were potentially more effective vis-à-vis US deterrence and strike strategies.[14] The advances in both delivery systems were, however, overshadowed by improvements in the design of strategic bombers and the lethality of thermonuclear weapons. With the development of both the B-52 and the first USAF supersonic bomber, the B-58, the arguments regarding the potential advantages for US deterrence stemming from ICBM and SLBM technologies were defeated relatively easily by the continued perception of the dominance of the strategic bomber fleet. This was reinforced by resistance from the Air Force to any significant changes in its dominance of the US nuclear arsenal and deterrence policy, noted as far back as this history from 1967: "The Air Force's hesitation resulted from its devotion to the concept of strategic bombing, its belief in the application of maximum military power to important targets, and its desire to retain a monopoly of nuclear weapons."[15] By the time the US policy of flexible response was in place in the late 1960s, the Air Force had established firm control of US nuclear deterrence

policy. In turn, this guaranteed that the role of strategic bomber as part of the nuclear triad would remain generally unquestioned.

The 1960s represented the development of several potential threats to the role of the bomber within the US strategic deterrence framework. After a decade of development, the first nuclear ICBMs became operational in 1959. When combined with the hydrogen bomb, the ICBM's advantages in both range and delivery immediately led to questions regarding the future structure of the US nuclear deterrent. These questions manifested most directly in doctrinal, and subsequently policy, disagreements between the Air Force and the Army and Navy. Against the Air Force's continued promotion of the strategic air offensive as the foundation of US strategic doctrine and nuclear policy, "the other services flatly denied that strategic airpower alone could insure victory. While they generally agreed that Soviet aggression presented the greatest threat to US security . . . they argued that the conflict would be much more complex than the Air Force expected and that no single kind of military force could decide the issue."[16] The result was a disagreement between the branches that focused on what a future war would look like and what role nuclear weapons would most likely play in that war. The impact on policy showed in debates throughout the 1960s at places like RAND between those who supported the "stability doctrine" or mutually assured destruction (MAD), versus those who believed US deterrence structures could be formed around the concept of limited war.[17]

By the early 1970s, the US Army had relented in its attempts to develop its own nuclear capability. The Navy, however, increasingly began to challenge both the Air Force and its doctrinal assumptions relative to the continued evolution of the nuclear triad. Through successful development of the Polaris program, the Navy could now substantively add to the US nuclear deterrent framework. More importantly, the debates that surrounded the program throughout the 1950s and early 1960s were portents for the same discussions had today. First, they exposed "the nuclear weapon dominance that the newly created Air Force had in the early years the Cold War."[18] By the end of the Eisenhower administration, the Air Force was in control of three of the four primary ballistic missile projects, with the lone Jupiter missile project controlled by the Army. Without development of its own delivery system, the Navy was relegated to secondary status to the development of the country's nuclear posture. It had focused initially on development of so-called

super carriers able to service nuclear capable long-range bombers. But Truman, "citing budget constraints, canceled the program in favor of increased investment in the Air Force's B-36 strategic bomber."[19] This defeat led to a shift from the super carrier to the fleet ballistic missile as the primary nuclear delivery system for the Navy.

A second connection between nuclear force structure debates during the Cold War and today is the importance of technology for understanding capability—and thus policy and strategy. Combined with significant advances in submarine technology, shifting from an air-based to a missile-based focus in the late 1950s was an obvious and ultimately effective change in strategy for the Navy. But it also served to insulate strategic bombers from broader considerations of how to develop (and fund) the evolving nuclear triad. This is because the focus on missile technologies tended to make ICBMs the natural comparative weapon system for the new SLBMs, and neither seemed capable of fully supplanting the perceived advantages of the strategic bomber at the time. Potential advancements in missile defense systems (such as "Star Wars") and a growing faith in stealth technology to enhance the effectiveness of strategic bombers created a short debate.[20] The practical aspects of questions regarding the future of strategic nuclear bombers were symbolized by the development, cancellation, and subsequent reinvigoration of the B-1 bomber program in 1985. In the end, development of the B-1 and subsequent B-2 strategic bomber programs seemed to close the door on lingering questions. Indeed, the future role of the nuclear bomber seemed secure with deployment of the stealth-capable B-2 bomber in 1997. The Cold War was won, US strategic power was unchallenged, and both seem to be directly related to the development and maintenance of the nuclear triad as the foundation of the nation's deterrence framework. What was less considered was how the new global threat environment would once again raise questions regarding the most appropriate framework for US nuclear deterrence.

Signaling the Soviets

Aside from their role in the delivery of nuclear weapons, strategic bombers' most important use has been as a tool for signaling within the US deterrence framework. Few questioned the capability of the United States to follow through on the various threats associated with its deterrence policies. Instead, most of the academic- and policy-driven

examinations of US deterrence policy have focused on the ability to communicate intentions to use that capability in a credible manner. The primary means of signaling during the Cold War involved stationing nuclear weapons on an ally's territory or within potential striking distance of an adversary. With the development and expansion of extended deterrence, the United States found itself in an increasing number of situations where it had to send nuclear signals to potential adversaries for both its own and its allies' interests.[21] The use of signaling was not aimed solely at adversaries like the Soviet Union or China, "it aimed also to discourage allies from seeking nuclear arms of their own."[22] As the role of signaling evolved relative to changes in the US nuclear doctrine, there was an ever-increasing need for flexibility and graduation within US response options. Because bombers offered more flexibility than the stationing of ICBMs, they increasingly became the preferred method for signaling US deterrence policy. The B-52 in particular became the symbol of US nuclear strength and deterrence policy, a role that it continues to play to this day.[23]

The use of bombers as the primary signaling method was an essential component of the US-Soviet deterrence framework during the Cold War. Interestingly, they played less of a role in Europe than they did in Asia for a variety of reasons. From a general perspective, ICBMs are the most static component of the nuclear triad and thus offer few options as a method of signaling intentions in individual crises. There are no spare missiles or extra silos, the missiles cannot be moved, and they remain constantly ready. ICBMs were useful for more general and long-term signaling in the European context precisely because US deterrence was intertwined with the regional security framework (i.e., NATO).[24] This aside, bombers offered flexibility in terms of deployment and control. Even the possibility of using low yield or tactical nuclear weapons was part of an escalation ladder. This is most clearly summarized by one supporter's claims that "nothing demonstrates American resolve better than putting fully loaded strategic bombers on alert or deploying them to a forward base as the spy satellites of a target nation pass overhead. The ability to signal in a nuclear crisis is a characteristic found only in the bomber force."[25] This flexibility was evident not only against the Soviets but also following the successful development of nuclear weapons by China in 1964. In both instances, however, this was at least partially

due to the differing structures of deterrence that developed within Asia relative to Europe.

The reality is that most of the direct conflict associated with the US-Soviet rivalry during the Cold War took place in Asia. If the US-Chinese rivalry is added to the equation, nuclear doctrine and strategy were tested far more often in the Asian theater than they were in Europe. In addition to (or perhaps because of) the almost constant existence of conflict in Asia, the United States also had the problem of potentially unstable or ill-equipped allies who were considering development of their own nuclear arsenals. At one point or another, the United States engaged Taiwan, South Korea, Japan, and Australia in quiet but firm efforts to convince them that pursuit of nuclear weapons was unnecessary due to US extended deterrence.[26] Due to a variety of factors, including the Japanese adoption of its antinuclear principles and questions regarding the stability of some allies, the United States had no real opportunities to use missile deployments as a signaling method in the same way the strategy developed in Europe from the 1960s onward. The need for signaling within the Asian context, however, increased dramatically with the nuclearization of China. The difference between the two contexts involved more than just the signaling utility of missile basing, however.

The US nuclear deterrent in Europe is embedded in the American commitment to the NATO alliance, particularly Article V of the Washington Treaty. By contrast, the United States has no parallel multilateral alliance structure in East Asia. The US extended deterrent there is based on bilateral relationships and agreements, so any nuclear debate there would be viewed mainly through a bilateral lens.[27]

Through its membership in NATO, the United States used a single signal (the basing of theater and intermediate range nuclear weapons throughout Western Europe) to illustrate extended deterrence to all of its allies in the region at the same time.[28] The need to rely on bilateral relationships in the Asian context meant that the United States often found itself demonstrating its commitments more frequently, and in a much more specific manner. Rather than potentially defending Europe from a general Soviet threat, the United States had to engage its bilateral deterrent relationships within individual, often crisis-laden contexts. This only further limited the utility of missile deployments as a method of signaling, a reality that was finalized when the George H. W. Bush administration removed all tactical nuclear weapons from the region in

the early 1990s. The more critical takeaway, however, was that the signaling role of the strategic bomber was being affirmed in the post–Cold War era, if only because it was the only option.

It could be argued that the stationing of nuclear-capable submarines represented a potential form of signaling for US deterrence policy similar to the basing of missiles, especially as it related to extended deterrence.[29] One of the reasons for this was the development of multiple independently targetable reentry vehicle (MIRV) technology and its impact on the deterrence value of SLBMs. The ability to mount three warheads on each individual SLBM, and survivability aspects of the submarine platform, quickly increased its importance in the nuclear triad and thus as a potential source of signaling. Combined with the Soviet rejection of the US proposed ban on MIRV technologies in 1970, "the Navy's deterrent and retaliatory capabilities increased multifold."[30] The stationing of nuclear submarines could represent a significant message to both allies and adversaries of the US commitment to extended deterrence in a region. In recent attempts to deter North Korea from further developing its nuclear capabilities, nuclear submarine forces have played a prominent role in US signaling.[31]

Despite the limited use of both ICBMs and SLBMs to signal US intentions and deterrence capabilities, the strategic bomber has remained the dominant method of nuclear signaling into the post–Cold War period. There is little to suggest that the relationship between the three legs of the nuclear triad will ever change the relative utility of strategic bombers for signaling. What should be considered, however, is the contemporary need for nuclear signaling within the US framework of deterrence. Like other aspects of US nuclear doctrine and strategy, it may be the case that the need for nuclear signaling has diminished in combination with the decline of state-level nuclear crises. With changes in the international threat environment have come changes to the application of US deterrence strategies. In those instances where there have been state-level nuclear threats to US security, the threats have come from rogue states like Iran and North Korea. As will be discussed, traditional frameworks of deterrence are less useful in these instances precisely because rogue states already indicate their willingness to ignore attempts to deter their nuclear ambitions or policies. This means that while the strategic bomber continues to be the primary signal, both the instances for and effectiveness of its use have declined in the post–Cold War era.

The Declining Utility of Nuclear Bombers

To this point, this analysis has sought to clearly explain the foundations of the US reliance on strategic bombers as an essential component of the country's deterrence policy and nuclear doctrine. The underlying reason for this discussion has been the desire to assess the continuing value of strategic bombers as part of the nuclear triad. The current position is firmly grounded in the historical value of strategic airpower for US hegemony, the practical need to have both a flexible response and dynamic signaling options, and in the general dominance of the Air Force within the area of US nuclear policy. The argument offered here is that these points no longer justify the continuing maintenance of the US strategic nuclear bombing option. First, whatever the historical value of strategic airpower for US geostrategy, technology has steadily eroded and perhaps eliminated that advantage. Although the Air Force argues that stealth technology represents a path to overcoming problems in this area, it is precisely the costs of producing an entirely new line of stealth-capable strategic bombers that has reduced the relative value of the strategic bomber leg of the triad. A second point to consider is the sea change that has taken place in the international threat environment since the end of the Cold War and since 9/11 in particular. Because of the general transition from states to nonstate actors as the primary threat and the associated transition in focus from nuclear conflict to terrorism and cyberwar, the utility of the US nuclear deterrent has diminished. There is no doubt that the global war on terrorism has illustrated the continued essential need of strategic bombing capabilities within conventional theaters. It is when one considers their decreasing effectiveness as a delivery platform, in conjunction with increasing costs relative to the other platforms, that the overall viability of the strategic bomber must be questioned.

Too Much "Buck"

The strategic bomber leg of the nuclear triad has consistently represented the most expensive component of the US nuclear arsenal. According to one study, "The annual cost of maintaining this fleet of aircraft ranges from $3.1 to $3.5 billion across the FYDP [Future Years Defense Program] (2014–18) for a total of $16.5 billion."[32] There were several years when this cost was double that associated with the deployment of ICBMs, and even with the associated cost of the development and support of submarine forces it still outpaced those expenses as well.

During that same period, for instance, the cost of ICBM maintenance ranged from $1.7 to $1.9 billion per year, with the cost of maintaining the nuclear submarine fleet resting at around $2.9 billion a year.[33] The key is understanding the costs associated with delivery platforms, that is, the bombers themselves. Other examinations, such as the Harrison-Montgomery study conducted for the Center for Strategic and Budgetary Assessments, project much lower costs for maintaining the airborne components of the nuclear triad precisely because they do not include the full costs of the B-2 or the proposed B-21. The previously mentioned success of strategic bombers in the conventional context allows for rationalizing part of the cost as a "dual-use system."[34] There is, however, some mathematical judo taking place as the cost of development, deployment, and support of strategic bomber forces is extremely high for anyone solely considering the need to maintain nuclear capabilities. "In the minds of detractors, bombers are overkill and the costs associated with maintaining nuclear capable bombers are no longer justifiable."[35] This has not deterred supporters from continuing to promote the strategic bombing leg as untouchable during budget negotiations or reviews of US nuclear doctrine.

The primary responses offered rest on the belief that the bombers offer significant levels of flexibility for US deterrence efforts, flexibility that more than makes up for its expense relative to other legs of the triad. One aspect of this perspective rests on the nature of the weapon system itself. Incorporation of the human element into the bomber leg as represented by the crews of the bombers offered this component of the nuclear triad a higher level of responsiveness to changing conditions and contexts. This was most directly represented by the argument that bombers and their crews represented the only nuclear weapon system that could be both scrambled and recalled. This made them much more useful than the other two legs of the triad relative to "escalation/de-escalation during a conflict"—that is, signaling.[36] In the post–Cold War context, it has been their flexibility relative to the sudden increase in the conventional role for long-range bombers that offers evidence of their continued importance to the nuclear triad. What has been interesting is that the overall justification for the contemporary costs of maintaining a strategic bomber fleet often has been justified more by "the need for long-range strike capabilities . . . than an interest in maintaining the nuclear role for bombers."[37] This recognition has been reinforced by

US combat experiences in Afghanistan, Iraq, and elsewhere. The role and utility of long-range bomber forces continue to be fully justified by the wide variety of combat requirements facing conventional US forces today. But the dominance of nonstate actors and the threat of terrorism within that framework require a separation of the role of bombers in the conventional sense versus their position and usefulness as part of the nuclear triad. On their own, long-range bombers represent an enormous investment of state resources and capabilities. The additional requirement of making the weapon system dual capable relative to the delivery of nuclear weapons adds a significant level of cost. It is for this reason that some cost projections have development and maintenance of the new long-range strategic bomber reaching $8 billion a year by 2030.[38] In the end, acceptance of the significant and steadily increasing costs associated with maintaining strategic nuclear bombers is not justified by its diminishing role within the nation's deterrence framework.

Too Little Bang

The primary argument offered here against the continuation of the strategic bomber leg of the nuclear triad is its vulnerability and relative weaknesses when compared to ICBMs and SLBMs. These are not new concerns as they represent consistent themes in the recurring debates regarding the structure of the triad. Ever since the establishment of the strategic bomber, a primary consideration for its effectiveness has been its ability to penetrate enemy airspace. This practical issue dominated analyses of strategic bombing during World War II, and its importance did not diminish with the advent of nuclear weapons. One of the more significant rationales behind the development of the Polaris SLBM system in the early 1960s was the recognition that the effectiveness of strategic bombers depended almost totally upon the degradation of Soviet air defenses.[39] For this reason the emphasis on the flexibility and responsiveness of strategic bombers is much more applicable with regard to signaling than it is to the practical planning of a nuclear strike.

The potential weaknesses of strategic bombers as nuclear delivery systems are well documented and have been scrutinized since World War II. They are slow and vulnerable to air defenses as well as to surprise attacks on their bases, and they "provide only minimal second-strike capability."[40] When combined with the increasing ability to utilize ICBM and SLBM forces to satisfy both extended deterrence and counterforce

requirements, there is (for some) a steadily decreasing role in deterrence to be played by strategic bombers. One way in which the Air Force has attempted to address these criticisms is through the development of stealth technology. Unfortunately, experiences with the B-2 bomber indicates problems that call into question its overall effectiveness, especially as air defense technologies continue to improve.[41] Even though current plans for the development of the new stealth B-21 bomber are in the works, there is no indication that their potential to defeat or evade enemy air defenses has improved relative to the problems that existed in the immediate post–Cold War era. What is important to understand is that the costs of developing and maintaining new replacement bombers in conjunction with upgrading existing B-52 and B-2 weapon systems is estimated to drive the overall cost of the strategic bombing leg of the triad to more than $8 billion a year by 2019.[42] This expense could be justified if strategic bombers represented the most effective and efficient method by which to deliver nuclear weapons. But when the cost is considered relative to evidence that strategic bombers might in fact end up with the lowest success rate among other nuclear delivery platforms, the overall investment in maintaining and further developing them becomes increasingly questionable.

Conclusion

There has been a long-standing acceptance of strategic bombers as an essential component of the US nuclear triad. Its dominance has been based upon historical understandings of the importance of strategic airpower to US hegemony, as well as their practical use in signaling US deterrence strategies. The role of the strategic bomber has been supported further by the long-term dominance of US nuclear doctrine by the Air Force. There have been various instances in which the role of ICBMs was critically reviewed in terms of their continuing importance to US deterrence efforts. Similarly, the Navy encountered an uphill struggle in its attempts to develop the SLBM as the last leg of the nuclear triad. But it is in fact the strategic bomber leg of the triad that has most consistently been a source of concern when the US nuclear posture was under review. During the transition from mutually assured destruction to flexible response, and within the regular reviews of US nuclear doctrine, the role of the strategic bomber has continually been questioned, mostly by those outside the Air Force and beyond the culture of strategic airpower.

It is now time to engage more fully the questions and doubts surrounding the role of the strategic bomber as part of the nuclear triad, especially given the potential doubling of maintenance and support costs over the next decade.

While both the cost and efficiency arguments have value, the history of the debate surrounding the nuclear triad clearly demonstrates that it is the perceptions and influence of the Air Force that will most directly determine the future of strategic bombers. Some indications show their position on the nuclear triad is changing by the steady realization that the threat environment that the nuclear triad was designed to respond to no longer exists. While there is certainly a need to maintain traditional strategic deterrence vis-à-vis states such as Russia and China, the threat of terrorism and irregular warfare, as represented by increasing conflict with weak states and nonstate actors, has changed the dynamic within which the United States promotes its current deterrence policy. This perspective is highlighted further by the rise of both the cyber and space domains as areas in need of significant investments in deterrence capabilities. The United States must begin to recognize that despite its enormous economic strength, the ability to invest in a truly dynamic deterrence framework remains limited. It must begin to recognize that US deterrence efforts need to address new and more dynamic types of threats and attacks. This will mean that during the next nuclear posture review the Department of Defense will need to make hard choices regarding investing in increased cyber and space capabilities versus reinvesting in the increasingly narrow and potentially ineffective strategic bomber leg of the nuclear triad. These choices will require sacrifices in other areas as well, but the suggestion offered here is that the strategic bomber leg of the nuclear triad represents a potential area to start with. SSQ

Notes

1. Colin Gray, *Maintaining Effective Deterrence* (Carlisle Barracks, PA: Army War College Strategic Studies Institute, August 2003), 1, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA417180.

2. Alex Wellerstein, "A Brief History of the Nuclear Triad," *Restricted Data: The Nuclear Secrecy Blog*, 15 July 2016, http://blog.nuclearsecrecy.com/2016/07/15/brief-history-nuclear-triad/.

3. Thomas C. Kirkham, "Modernizing the Nuclear Bomber Force: A National Security Imperative," in *The Strategic Challenge of the US Nuclear Arsenal: AY14 Nuclear Issues Research*

Group, ed. Albert J. Mauroni (Maxwell AFB, AL: US Air Force Center for Unconventional Weapons Studies, 2014), 45–46, http://cpc.au.af.mil/assets/strategicchallenge.pdf.

4. Amy Woolf, *U.S. Strategic Nuclear Forces: Background, Developments, and Issues*, RL33640, Congressional Research Service, 8 August 2017, 37, https://fas.org/sgp/crs/nuke/RL33640.pdf.

5. Ibid., 2.

6. Francis J. Gavin, "The Myth of Flexible Response: United States Strategy in Europe during the 1960s," *International History Review* 23, no. 4 (2001): 847–75, http://doi.org/cx5763.

7. Maj Kenneth Fetters, "The Role of the Long-Range Strategic Bomber," Center for Unconventional Weapons Studies, Trinity Site Papers, March 2014, 4, http://cpc.au.af.mil/assets/trinity_site_paper3.pdf.

8. Marc Trachtenberg, *History and Strategy* (Princeton, NJ: Princeton University Press, 1991), 4.

9. Ibid., 12.

10. Lt Col Keith A. Barlow, *Massive Retaliation*, Research Paper no. AD-764 412 (Carlisle Barracks, PA: US Army War College, 8 March 1972), 12, http://www.dtic.mil/dtic/tr/fulltext/u2/764412.pdf; and Trachtenberg, *History and Strategy*, 6–12.

11. Richard R. Muller, "The Origins of MAD: A Short History of City Busting," in *Getting MAD: Nuclear Mutual Assured Destruction, Its Origins and Practice*, ed. Henry D. Sokolski (Carlisle, PA: Strategic Studies Institute, 2004), 45.

12. Ibid., 6.

13. Benjamin Friedman, Christopher Preble, and Matt Fay, *The End of Overkill? Reassessing US Nuclear Weapons Policy* (Washington, DC: Cato Institute, 2013), 2.

14. Thom W. Ford, *Ballistic Missile Submarines of the United States and the Soviet Union: A Comparison of Systems and Doctrine* (Monterey, CA: Naval Postgraduate School, 1972), 8.

15. George F. Lemmer, "The Air Force and Strategic Deterrence, 1951–1960," USAF Historical Division Liaison Office, December 1967, 14, http://nsarchive.gwu.edu/nukevault/ebb249/doc09.pdf.

16. Ibid., 24.

17. Trachtenberg, *History and Strategy*, 31–32.

18. Harvey M. Sapolsky, "The US Navy's Fleet Ballistic Missile Program and Finite Deterrence," in *Getting MAD*, 124.

19. Ibid., 125.

20. Donald M. Hale Jr., "US Nuclear Triad: Is It Sustaining the Cold War or 21st Century Framework?" (master's thesis, Johns Hopkins University, December 2013), https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/37599/HALE-THESIS-2014.pdf.

21. *See* Matthew Fuhrmann and Todd S. Sechser, "Signaling Alliance Commitments: Hand Tying and Sunk Costs and Extended Nuclear Deterrence," *American Journal of Applied Science* 58, no. 4 (2014): 919–35, http://doi.org/f6m34m; and Steven Pifer, Richard C. Bush, Vanda Felbab-Brown, Martin S. Indyk, Michael O'Hanlon, and Kenneth M. Pollack, "US Nuclear and Extended Deterrence: Considerations and Challenges," *Arms Control Series, Paper 3*, Brookings Institute (May 2010), https://www.brookings.edu/wp-content/uploads/2016/06/06_nuclear_deterrence.pdf.

22. Pifer et al., *Nuclear and Extended Deterrence*, 7.

23. Mike Benitez, "The Nuclear Bomber: Fighting Conflated Deterrence in the 21st Century," *Breaking Defense*, 2016, http://breakingdefense.com/2016/03/the-nuclear-bomber-fighting-conflated-deterrence-in-the-21st-century/.

24. Pifer et al., *Nuclear and Extended Deterrence*, 18–19.

25. Kirkham, *Modernizing*, 46.

26. *See* Pifer et al., *Nuclear and Extended Deterrence*; and Richard C. Bush, "The US Policy of Extended Deterrence in East Asia: History, Current Views and Implications," Brookings Institute, Arms Control Series, Paper 5, 24 February 2011, https://www.brookings.edu/research/the-u-s-policy-of-extended-deterrence-in-east-asia-history-current-views-and-implications/.

27. Bush, "US Policy," 5.

28. Michaela Dodge, "US Nuclear Weapons in Europe: Critical for Transatlantic Security," Backgrounder Report no. 2875, The Heritage Foundation, 18 February 2014, http://www.heritage.org/defense/report/us-nuclear-weapons-europe-critical-transatlantic-security.

29. David J. Trachtenberg, "US Extended Deterrence: How Much Strategic Force Is too Little?," *Strategic Studies Quarterly* 6, no. 2 (Summer 2012): 84, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06_Issue-2/summer12.pdf.

30. Ford, *Ballistic Missile Submarines*, 68.

31. Franz-Stefan Gady, "Trump: Two Nuclear Subs Operating in Korean Waters," *The Diplomat*, 25 May 2017, http://thediplomat.com/2017/05/trump-2-nuclear-subs-operating-in-korean-waters/.

32. Jon B. Wolfsthal, Jeffrey Lewis, and Marc Quint, *The Trillion Dollar Nuclear Triad* (Monterey, CA: The James Martin Center for Nonproliferation Studies, 2014), 18.

33. Ibid., 13.

34. Todd Harrison and Evan Braden Montgomery, *The Cost of New US Nuclear Forces: From BCA to Bow Wave and Beyond* (Washington, DC: Center for Strategic and Budgetary Assessments, 2015), 32–33, http://csbaonline.org/research/publications/the-cost-of-u-s-nuclear-forces-from-bca-to-bow-wave-and-beyond/publication.

35. Kirkham, *Modernizing*, 46–47.

36. Ibid., 51.

37. Woolf, *US Strategic Nuclear Forces 2016*, 32.

38. *See* Congressional Budget Office, *Projected Costs of U.S. Nuclear Forces, 2014 to 2023*, Pub. No. 4618, December 2013, https://www.cbo.gov/publication/44968; and Wolfsthal, Lewis, and Quint, *Trillion Dollar Nuclear Triad*.

39. Friedman, Preble, and Fay, *End of Overkill?*, 10.

40. Kirkham, *Modernizing*, 49.

41. *The U.S. Nuclear Triad: GAO's Evaluation of the Strategic Modernization Program*: *Testimony before the Committee on Governmental Affairs*, 103rd Cong. (1993) (Statement of Eleanor Chelimsky, assistant comptroller general, Program Evaluation and Methodology Division, US Government Accountability Office).

42. Wolfsthal, Lewis, and Quint, *Trillion Dollar Nuclear Triad,* 20.

Book Review

China's Military Transformation by You Ji. Polity Press, 2016, 284 pp.

The United States has a growing and stronger rival in the area of military affairs. It is the People's Liberation Army of China (PLA), and it is changing in many ways, becoming more powerful and influential—and also more autonomous as a leading institution in China. Its connection to the Chinese Communist Party (CCP) also is evolving. In the past, the relationship between the PLA and the CCP was harmonious, but today changes in the military seem to have driven a wedge between these two entities. This seems to be the view of You Ji, a prolific writer and author of a number of works concerning the Chinese military.

The author cites a number of changes in the Chinese military that should be of interest to us. For example, there is no reluctance to spend billions of dollars on improving the capability of the military. The military itself seems to have also changed its posture from one of defense of the homeland to one of preparation for offensive actions. The navy, for example, is now concerned not only with protecting the coastline but also extending its influence into regional waters, which may be of more concern to the United States. In addition, the types of weapons the Chinese are interested in developing are more sophisticated and lethal than in the past, especially those which can reach faraway places. There is also a major US concern with the Chinese military and space warfare development. One effect of this development will be more American monitoring of Chinese military activities so as to prevent a security vulnerability in this country.

It is interesting to discover the motives for such a transformation in the Chinese military. Obviously, perceived threats from other countries in terms of invading Chinese areas of influence seem to be paramount. The United States and Japan may be viewed as the cause of these perceptions in one way or another. For example, American military ships patrolling close to China could result in that country reacting in a more protective manner by building up its military capacity. There may be other factors, such as China's desire to expand its sphere of influence and to create an impression of more power in the world based on military capability. There is no doubt that China is growing in prominence in the world today, and it certainly helps to have a military that can be influential in foreign affairs. Yet the Chinese military has another function noted in the book: quelling dissent. Even though this function could be interpreted as antidemocratic, it could be useful to a government more concerned about unity, progress, international influence, and some type of stability. Hence the role of the Chinese military will still be of great importance in China in the future considering that it has a strong effect on foreign and domestic affairs in many ways.

This book has focused on three major transformations of the PLA. One transformation is the relationship of the military to the Communist Party. It seems as if the military is becoming more of a separate entity with its connection to the party. For example, the author notes, "Today there is no politician in uniform and the minimized PLA representation at the apex of power has become largely functional" (p. 27). This change suggests a difference with previous civil-military personnel situations.

Another transformation is the role of the PLA in domestic politics. Basically, the author suggests that the PLA has less of an effect on who will be the future Chinese political leaders. He notes that the generals are no longer the "kingmakers" who could determine leadership succession (p. 27–28). It seems that the military is moving from unconditional support of the

party to nominal loyalty. Nevertheless, it is evident that cooperation between the two entities is still present and probably will continue for some time.

A third transformation is the modernization of military force. With the huge sums of money being invested in the military, there is an obvious attempt to rival the United States in developing certain types of sophisticated weapons. For example, the Chinese military's attitude toward aerospace power seems to be of paramount concern. The Chinese military does differentiate between airpower and space power but believes that there should be a combination of both to become successful in air warfare. Hence, financial investments in both of these types of powers are recognized as very important to the security of China considering the fact that the United States has developed effective and sophisticated weapon systems in both areas.

It is obvious upon reading this book that there is a growing separation between the CCP and the PLA even though the fact is that the party is the key entity in Chinese foreign policy. Yet the separateness could have important repercussions recognized by many—especially the Chinese. For example, the separateness between these two entities is important to note because it could have serious consequences, such as a decline of influence of China in world affairs, and other countries could take advantage of this change. However, the Chinese will work hard to keep these differences from restricting their rapid growth in power and influence in the worldwide environment.

It is projected by many that China will be a fast rising power in the twenty-first century. Although many factors, including economic growth, will foster this power, certainly the role of its military will be another important reason. One must remember that for China to feel more secure domestically and internationally and to expand its influence further in the world, it needs to have a strong military. Hence, this book becomes a valuable tool in helping us understand this new position of China and the role of its military.

William E. Kelly, PhD
Auburn University Political Science Department

Mission Statement

Strategic Studies Quarterly (*SSQ*) is the strategic journal of the United States Air Force, fostering intellectual enrichment for national and international security professionals. *SSQ* provides a forum for critically examining, informing, and debating national and international security matters. Contributions to *SSQ* will explore strategic issues of current and continuing interest to the US Air Force, the larger defense community, and our international partners.

Disclaimer

The views and opinions expressed or implied in *SSQ* are those of the authors and should not be construed as carrying the official sanction of the US Air Force, the Department of Defense, Air Education and Training Command, Air University, or other agencies or departments of the US government.

Comments

We encourage you to e-mail your comments, suggestions, or address change to: **StrategicStudiesQuarterly@us.af.mil**.

Article Submission

The *SSQ* considers scholarly articles between 5,000 and 15,000 words from US and international authors. Please send your submission in Microsoft Word format via e-mail to:

StrategicStudiesQuarterly@us.af.mil

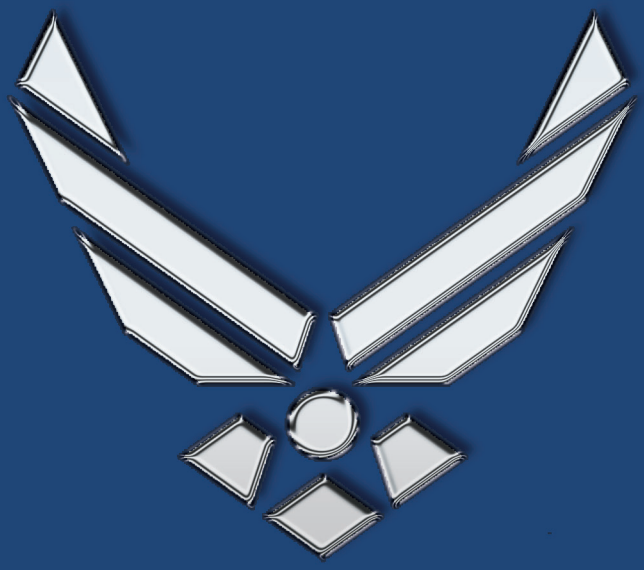
Strategic Studies Quarterly (SSQ)
600 Chennault Circle, Building 1405, Room 143
Maxwell AFB, AL 36112–6026
Tel (334) 953–7311

View *Strategic Studies Quarterly* online at **http://www.airuniversity.af.mil/ssq/**

Free Electronic Subscription

Like *SSQ* on Facebook at https://www.facebook.com/AirUnivPress
and follow us on Twitter at https://www.twitter.com/AirUnivPress

A forum for critically examining, informing, and debating national and international security



"Aim High... Fly-Fight-Win"

http://www.airuniversity.af.mil/SSQ/