Nuclear Deterrence and Cyber

The Quest for Concept

Dr. Stephen J. Cimbala

Nuclear deterrence is not what it used to be. Theorists, policy makers, and military planners have arrived at the place that noted physicist Freeman Dyson referred to as "The Quest for Concept."[1] One aspect of this change is that uses of nuclear weapons for deterrence or other missions will take place in a post-Internet, cyber-ready world. This is the international system defined not only by Hobbes but also by Jobs. Governments and their armed forces will have to adapt their bureaucratic hierarchies to the demands for faster and more flexible decision making and force application. In so doing, they will become progressively more cyber implicated, cyber dependent, and cyber vulnerable.[2]

That this is so is already acknowledged in US military organization. The Department of Defense (DOD) established US Cyber Command (USCYBERCOM) as a subunified command of US Strategic Command, and USCYBERCOM coordinates across the relevant military branches (US Army Cyber Command, US Fleet Cyber Command / US Tenth Fleet, Twenty-Fourth Air Force, US Marine Corps Forces Cyber Command, and US Coast Guard Cyber Command). Colocated with the National Security Agency, USCYBERCOM is headed by the same director.[3] Yet, for the most part, nuclear deterrence and cyber warfare issues are treated as separate and distinct compartments. This cyber-nuclear separatism is understandable as a matter of division of labor among experts, but it casts a shadow over the reality of nuclear deterrence or crisis management under cyber-intensive conditions.

In the discussion that follows, we first examine some of the broader theoretical implications of the nuclear-cyber nexus for students of na-

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

tional security policy and warfare. Second, we comment on the apparent significance of cyber and information wars, albeit with caveats not always recognized. Third, we consider how missile defenses, posing cyber challenges of their own, might complicate US-Russian political relations and nuclear arms reductions. No implication is intended that the US-Russia deterrence relationship is illustrative of other arms control and proliferation issues; indeed, we will see below that just the opposite is true. Nevertheless, some enduring realities of nuclear force exchanges merit recall as we move further away from the precyber and into the postcyber nuclear age. Fourth, we analyze how the combination of nuclear offenses and more advanced missile defenses might play out for deterrence stability, especially within the contentious US-Russian context. Finally, we draw pertinent conclusions about the nuclear-cyber interface insofar as it might pertain to future arms control, nonproliferation, and deterrence.

Nuclear and Cyber: Together or Apart?

What are the implications of potential overlap between concepts or practices for cyber war and for nuclear deterrence?[4] Cyber war and nuclear weapons seem worlds apart. Cyber weapons should appeal to those who prefer a nonnuclear or even a postnuclear military-technical arc of development. War in the digital domain offers, at least in theory, a possible means of crippling or disabling enemy assets without the need for kinetic attack or while minimizing physical destruction.[5] Nuclear weapons, on the other hand, are the very epitome of “mass” destruction, such that their use for deterrence or the avoidance of war by the manipulation of risk is preferred to the actual firing of same. Unfortunately, neither nuclear deterrence nor cyber war will be able to live in distinct policy universes for the near or distant future.

Nuclear weapons, whether held back for deterrence or fired in anger, must be incorporated into systems for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). The weapons and their C4ISR systems must be protected from attacks both kinetic and digital in nature. In addition, the decision makers who have to manage nuclear forces during a crisis should ideally have the best possible information about the status of their own nuclear and cyber forces and command systems, about the forces and C4ISR of possible attackers, and about the probable intentions and risk acceptance of possible opponents. In short, the task of managing a nuclear crisis demands clear thinking and good information. But the employment of cyber weapons in the early stages of a crisis could impede clear assessment by creating confusion in networks and the action channels that depend upon those networks.[6] The temptation for early cyber preemption might "succeed" to the point at which nuclear crisis management becomes weaker instead of stronger.

Ironically, the downsizing of US and post-Soviet Russian strategic nuclear arsenals since the end of the Cold War, while a positive development from the perspectives of nuclear arms control and nonproliferation, makes the concurrence of cyber and nuclear attack capabilities more alarming. The supersized deployments of missiles and bombers and expansive numbers of weapons deployed by the Cold War Americans and Soviets had at least one virtue. Those arsenals provided so much redundancy against first-strike vulnerability that relatively linear systems for nuclear attack warning, command and control, and responsive launch under—or after—attack sufficed. At the same time, Cold War tools for military cyber mischief were primitive compared to those available now. In addition, countries and their armed forces were less dependent on the fidelity of their information systems for national security. Thus the reduction of US, Russian, and possibly other forces to the size of "minimum deterrents" might compromise nuclear flexibility and resilience in the face of kinetic attacks preceded or accompanied by cyber war.[7]

Offensive and defensive information warfare as well as other cyber-related activities is obviously very much on the minds of US military leaders and others in the American and allied national security establishments.[8] Russia has also been explicit about its cyber-related concerns. President Vladimir Putin urged the Russian Security Council in early July 2013 to improve state security against cyber attacks.[9] Russian security expert Vladimir Batyuk, commenting favorably on a June 2013 US-Russian agreement for protection, control, and accounting of nuclear materials (a successor to the recently expired Nunn-Lugar agreement on nuclear risk reduction), warned that pledges by Presidents Putin and Barack Obama for cooperation on cybersecurity were even more important: "Nuclear weapons are a legacy of the 20th century. The challenge of the 21st century is cybersecurity."[10] On the other hand, arms control for cyber is apt to run into daunting security and technical issues, even assuming a successful navigation of political trust for matters as sensitive as these. Of special significance is whether cyber arms-control negotiators can certify that hackers within their own states are sufficiently under control for cyber verification and transparency.

The cyber domain cuts across the other geostrategic domains for warfare as well: land, sea, air, and space. However, the cyber domain, compared to the others, suffers from the lack of a historical perspective. One author argues that the cyber domain "has been created in a short time and has not had the same level of scrutiny as other battle domains."[11] What this might mean for the cyber-nuclear intersection is far from obvious. Table 1 summarizes some of the major attributes that distinguish nuclear deterrence from cyber war, according to experts, but the differences between nuclear and cyber listed here do not contradict the prior observation that cyber and nuclear domains inevitably interact in practice. According to research professors Panayotis A. Yannakogeorgos and Adam B. Lowther at the US Air Force Research Institute, "As airmen move toward the future, the force structure—and, consequently, force-development programs—must change to emphasize the integration of manned and remotely piloted aircraft, space, and cyber-power projection capabilities."[12]

Table 1. Comparative attributes of cyber war and nuclear deterrence

Cyber War	*Nuclear Deterrence*
Source of attack may be ambiguous—third-party intrusions masquerading as other actors are possible.	Source of attack is almost certain to be identified if the attacker is a state, and even terrorist attackers' nuclear materials may be traceable.
Damage mostly to information systems, networks, and their messaging contents although these might have spillover effects to the operations of military combat systems, economy, and social infrastructure.	Failure of deterrence can lead to historically unprecedented and socially catastrophic damage even in the case of a "limited" nuclear war by Cold War standards.
Denial of the attacker's objectives is feasible if defenses are sufficiently robust and/or penetrations can be repaired in good time.	Deterrence by means of threat to deny the attacker its objectives is less credible than the threat of punishment by assured retaliation (although improved missile defenses seek to change this).
The objective of cyber attacks is typically disruption or confusion rather than destruction per se.	Nuclear deterrence has rested for the most part on the credible threat of massive, prompt destruction of physical assets and populations.
Cyber war and information attacks can continue over an extended period of time without being detected and sometimes without doing obvious or significant damage—some are not even reported after having been detected.	The first use of a nuclear weapon since 1945 by a state or nonstate actor for a hostile purpose (other than a test) would be a game-changing event in world politics, regardless of the size of the explosion and the immediate consequences.
The price of entry to the games table for cyber war is comparatively low—actors from individual hackers to state entities can play.	Building and operating a second-strike nuclear deterrent requires a state-supported infrastructure, scientific and technical expertise on a large scale, and long-term financial commitments.

Source: The author. See also Timothy L. Thomas, *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker* (Ft. Leavenworth, KS: Foreign Military Studies Institute, 2012), 60–66; and Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 27–28 and passim.

Cyber Attacks and Information Wars: How Significant?

The DOD and other government agencies, together with military and information technology experts, anticipate that future interstate conflict will include cyber attacks and information wars.[13] But the term *cyber war* may be misleading since attacks on computers and networks are only one means of accomplishing the objective of neutralizing the enemy's critical infrastructures.[14] As Joel Brenner has noted,

> The U.S. Navy spent about $5 billion to develop a quiet electric drive for its submarines and ships so they'd be silent and hard to track. Chinese spies stole it. The navy spent billions more to develop new radar for their top-of-the-line Aegis Cruiser. Chinese spies stole that, too. The electronic intelligence services of the Chinese and the Russians are working us over—taking advantage of our porous networks and indifference to security to steal billions of dollars' worth of military and commercial secrets. Some of our allies, like the French and the Israelis, have tried it too.[15]

One purpose for activity that the DOD refers to as information and infrastructure operations would not be mass destruction (although destructive secondary effects are possible) but mass and/or precision *disruption*.[16] According to Robert A. Miller, Daniel T. Kuehl, and Irving Lachow, the purpose of an information and infrastructure operation would be to "disrupt, confuse, demoralize, distract, and ultimately diminish the capability of the other side."[17] This concept lends itself to consideration for a deterrent mission based on the credible threat of conventional or nuclear response. One must always remember, however, that the unique, prompt lethality of nuclear weapons creates a separate grammar for the conduct of nuclear war even if such a war would remain within the boundaries of strategic logic.[18] As Colin Gray has warned,

> First, except for highly unusual cases, cyber power is confined in its damaging effects to cyberspace. This is not to understate the problems that can be caused by cyber attack, but it is to claim firmly that the kind of damage and disruption that cyber might affect [*sic*] cannot compare with the immediate and more lasting harm that nuclear weapons certainly would cause.[19]

It merits emphasis that cyber war, or deterrence primarily exercised in cyberspace, is emphatically cognitive in its epistemic center of gravity. However, for cyber war (or deterrence) to be of significant interest to strategists, it must also find meaningful application to the strategic and tactical problems that analysts and war fighters are expected to solve. In this regard, theories of cyber war or deterrence raise some of the same concerns that nuclear deterrence theories have done. In both cases, the theorist risks giving way to the temptation of putting forward elegant conceptual architectures for which pertinent applications are remotely visible, if at all. One must be alert to the possible distraction of nuclear or cyber versions of the Schlieffen plan.

Missile Defenses: Prophecy or Problem?

Technical Uncertainties

The cyber aspects of nuclear deterrence intersect with those pertinent to missile defense. Missile defenses, if successful, offer the possibility that deterrence by threat of unacceptable retaliation could be supported by deterrence based on denial of the attacker's objectives.[20] Today, missile defenses remain technologically and politically contentious. Russian objections to the European Phased Adaptive Approach (EPAA) to missile defenses proposed by the United States and North Atlantic Treaty Organization (NATO) remained emphatic even as reportedly secret DOD studies cast doubt on the technical proficiency of the proposed components for the European ballistic missile defense (BMD) systems.[21] A study by the US National Academy of Sciences on missile defense technologies called into question some of the thinking of the Obama administration and the US Missile Defense Agency about the priority of certain missions and technologies for BMD.[22] On the other hand, other expert scientists criticized the aforementioned study as containing "numerous flawed assumptions, analytical oversights, and internal inconsistencies" leading to "fundamental errors in many of the report's most important findings and recommendations" and as undermining its scientific credibility.[23] Future technology challenges to the development and deployment of missile defenses will have more to do with the "arbitrary complexity" of software engineering for multiple contingencies and players, compared to the bipolar and physics-centric context of the High Cold War.[24] Suffice it to say that the academic and policy arguments continue as to the feasibility and desirability of building missile defenses, alongside the inertial pull of research and development funding in this direction since the Reagan administration's Strategic Defense Initiative.[25]

Political Pitfalls

If the linkage between US and NATO plans for European missile defenses and further progress in US-Russian strategic nuclear arms reductions was not yet a hostage relationship, it was clearly a problematical connection.[26] The New Strategic Arms Reduction Treaty (START) agreement does not preclude the United States from deploying future missile defenses despite Russian efforts during the negotiating process to restrict American degrees of freedom in this regard.[27] But then Russian president Dmitry Medvedev and his predecessor-successor Putin have made it clear that Russia's geostrategic perspective links US and NATO missile defenses to cooperation on other arms control issues. Meanwhile the United States and NATO in 2011 moved forward with the first phase of a four-phase deployment of the EPAA for missile defenses.[28] In March 2013, Secretary of Defense Chuck Hagel announced plans to modify the original plan for the EPAA by abandoning the originally planned deployments of SM-3 IIB interceptor missiles in Poland by 2022. Nevertheless, this step failed to reassure Russian doubters about the US and NATO claims that their regional and global missile defenses were not oriented against Russia. Russian officials frequently reiterate demands for a legally binding guarantee from the United States and NATO that Russian strategic nuclear forces would not be targeted or affected by the system.[29] Table 2 summarizes the status of the EPAA BMD as of autumn 2013.

Table 2. European Phased Adaptive Approach to missile defense

	Phase I	*Phase II*	*Phase III*	*Phase IV (canceled March 2013)*
Time Frame	*2011*	*2015*	*2018*	*2020*
Capability	Deploying today's capability	Enhancing medium-range missile defense	Enhancing intermediate-range missile defense	Early intercept of MRBMs, IRBMs, and ICBMs
Threat/ Mission	Address regional ballistic missile threats to Europe and deployed US personnel.	Expand defended area against short- and medium-range missile threats to Southern Europe.	Counter short-, medium-, and intermediate-range missile threats to include all of Europe.	Cope with MRBMs, IRBMs, and potential future ICBM threats to the United States.
Components	AN/TPY-2 (FBM) in Kurecik, Turkey; C2BMC in Ramstein, Germany; Aegis BMD ships with SM-3 IA off the coast of Spain	AN/TPY-2 (FBM) in Kurecik, Turkey; C2BMC in Ramstein, Germany; Aegis BMD ships with SM-3 IB off the coast of Spain; Aegis Ashore with SM-3 1B in Romania	AN/TPY-2 (FBM) in Kurecik, Turkey; C2BMC in Ramstein, Germany; Aegis BMD ships with SM-3 IIA off the coast of Spain; Aegis Ashore with SM-3 IB/IIA in Romania and Poland	AN/TPY-2 (FBM) in Kurecik, Turkey; C2BMC in Ramstein, Germany; Aegis BMD ships with SM-3 IIA off the coast of Spain; Aegis Ashore with SM-3 IIB in Romania and Poland
Technology	Exists	In testing	Under development	In conceptual stage when canceled
Locations	Turkey, Germany, ships off the coast of Spain	Turkey, Germany, ships off the coast of Spain, ashore in Romania	Turkey, Germany, ships off the coast of Spain, ashore in Romania and Poland	Turkey, Germany, ships off the coast of Spain, ashore in Romania and Poland

Source: Karen Kaya, "NATO Missile Defense and the View from the Front Line," *Joint Force Quarterly*, issue 71 (4th Quarter 2013): 86. For pertinent technical challenges relative to target acquisition, discrimination, interception, and data networking, see Steven J. Whitmore and John R. Deni, *NATO Missile Defense and the European Phased Adaptive Approach: The Implications of Burden Sharing and the Underappreciated Role of the U.S. Army* (Carlisle, PA: US Army War College, October 2013), 11–17.

Note: Separate national contributions to the mission of European BMD have been announced by the Netherlands and France.

Aegis Ashore - land-based component of the Aegis BMD system
AN/TPY-2 (FBM) - Army-Navy / Transportable Radar Surveillance, Model 2 (forward-based mode)
BMD - ballistic missile defense
C2BMC - command, control, battle management, and communications
ICBM - intercontinental ballistic missile
IRBM - intermediate-range ballistic missile
MRBM - medium-range ballistic missile

Although the prospects for US-Russian or NATO-Russian agreement on European missile defenses might seem challenging at this writing, the prospects for US cooperation with allies and partners outside Europe on regional missile defenses are more favorable. The potential bull market for missile defenses lies in Asia, including prompts from Sino-Japanese rivalry, North Korean threats and missile tests, and deterrence challenges between India and Pakistan. From the standpoint of military modernization, both conventional and nuclear, as well as the expectation of future war, Europe is a relatively pacific security community compared to turbulent Asia. Should deterrence fail, missile defenses might appeal to states in Asia as supports for deterrence by denial-of-enemy-attack objectives and as means of damage limitation. Missile defenses for some US allies and partners might also reinforce US security guarantees based on the American nuclear umbrella and consequently reduce the incentives for those states to develop their own nuclear arsenals.[30]

Arms Reductions: Analysis

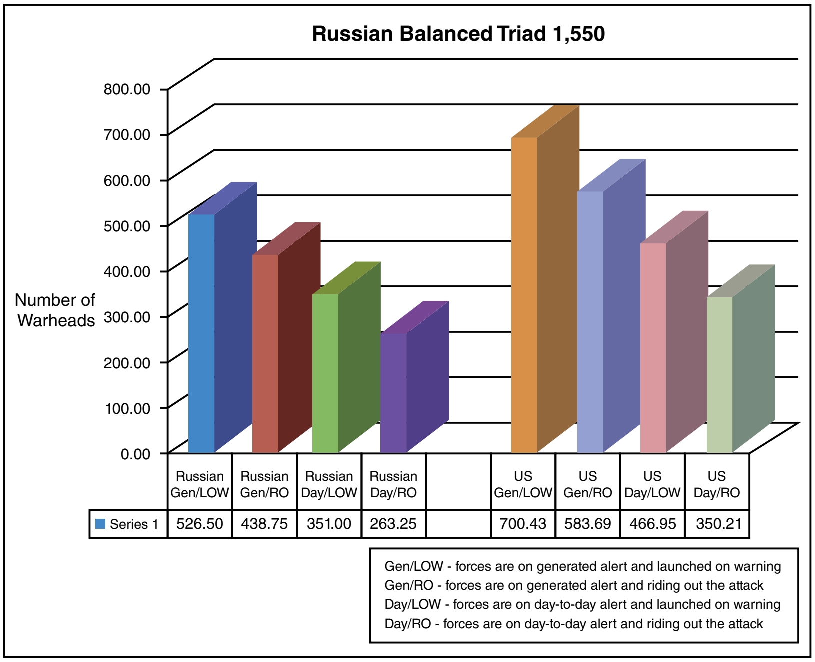
Force Exchange Models

The New START agreement of 2010 mandates modest reductions in the numbers of deployed strategic weapons and launchers, building on the Strategic Offensive Reductions Treaty reached earlier between the United States and Russia during the George W. Bush administration. In his Berlin speech of 19 June 2013, President Obama indicated US interest in post–New START reductions of about one-third in the numbers of Russian and American deployed intercontinental weapons.[31]

Could the United States and Russia safely take the step, from the New START maximum limit of 1,550 to roughly 1,000 operationally deployed nuclear warheads on intercontinental missiles and heavy bombers while preserving deterrence and arms control stability? The analysis that follows uses summary figures to interrogate that issue.[32]

New START and lower-limit force structures are projected based on various expert assessments and are tested by our model for their nuclear exchange outcomes.[33]

Figures 1 and 2 summarize the outcomes of US-Russian strategic nuclear exchanges, assuming a New START–compliant limit of 1,550 or 1,000 operationally deployed warheads on intercontinental launchers for each state. Figure 1 displays the numbers of second-strike surviving and retaliating warheads for each state under a deployment ceiling of 1,550 weapons, and figure 2 provides similar information for the case of 1,000 deployed weapons. In figures 3 and 4, respectively, we introduce antimissile and air defenses (combined) into the equation for each state, providing a variable range of possible performances against second-strike retaliating weapons: phase I defenses successfully intercept at least 20 percent of the second-strike retaliating warheads; phase II defenses, at least 40 percent; phase III defenses, at least 60 percent; and phase IV defenses, at least 80 percent.



	Russian Gen/LOW	Russian Gen/RO	Russian Day/LOW	Russian Day/RO		US Gen/LOW	US Gen/RO	US Day/LOW	US Day/RO
🟦 Series 1	526.50	438.75	351.00	263.25		700.43	583.69	466.95	350.21

Gen/LOW - forces are on generated alert and launched on warning
Gen/RO - forces are on generated alert and riding out the attack
Day/LOW - forces are on day-to-day alert and launched on warning
Day/RO - forces are on day-to-day alert and riding out the attack

Figure 1. US-Russia surviving and retaliating warheads (1,550 deployment limit)

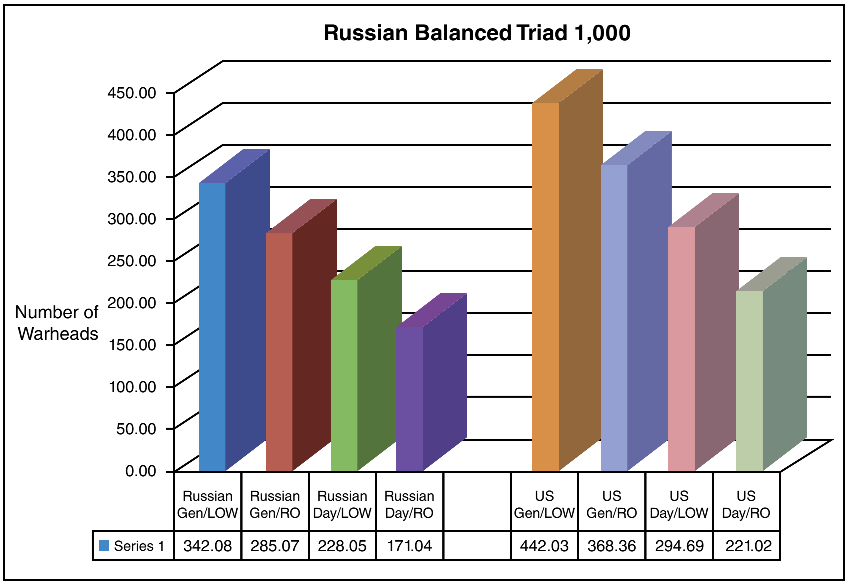


Figure 2. US-Russia surviving and retaliating warheads (1,000 deployment limit)

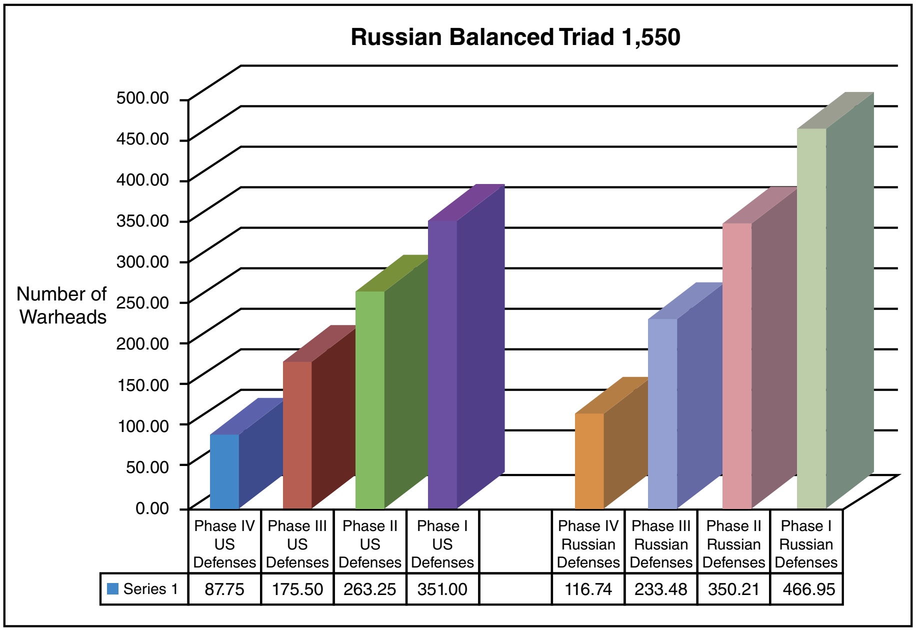


Figure 3. US-Russia surviving and retaliating warheads versus defenses (1,550 deployment limit)

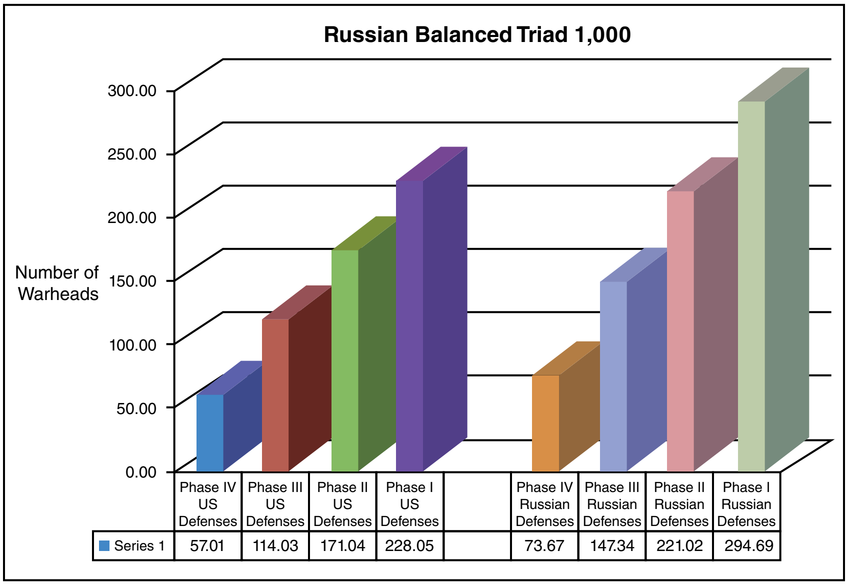


Figure 4. US-Russia surviving and retaliating warheads versus defenses (1,000 deployment limit)

Results and Implications

The preceding figures appear to show that each state has numbers of surviving and retaliating weapons sufficient to satisfy the criterion of "unacceptable damage" in a second strike so long as unacceptable damage is defined by traditional US political and military standards.[34] However, the assumptions about rationality or reasonableness on which traditional models of deterrence have rested may be misleading. As Keith B. Payne has noted in arguing for a more empirical approach to deterrence,

> Attempting to become familiar with the decision-making dynamics of foreign leaders, for the purpose of establishing an informed basis for deterring and coercing them, is not a trivial undertaking. And, it must be acknowledged that even extensive efforts at acquiring information concerning the factors underlying a challenger's decision-making will not preclude surprising, unpredictable behavior based on unfamiliar or wholly obscure motives, goals, and values.[35]

For example, some expert analysts have suggested that improving accuracies for delivering nuclear and conventional weapons may make counterforce strategies attractive to some states, including nuclear weapons states other than the United States and Russia.[36] In contrast, other researchers have warned that even nuclear wars smaller than those involving those two countries, such as a future nuclear conflict between Israel and Iran, could result in historically unprecedented and socially unmanageable consequences for both sides (in addition to uncertain side effects for the rest of the region).[37]

Thus the appeal of nonnuclear systems, including cyber weapons, for prospective attackers rests in part on their putative capacity for *calculated deception* combined with *precise lethality*. On this very point, Russian deputy prime minister Dmitry Rogozin has warned that information weapons are becoming first-strike weapons against enemy political, military, and industrial centers. Rogozin also claimed that Pentagon computer games showed that strikes by some 3,000–4,000 precision-guided munitions could destroy as much as 80–90 percent of Russia's nuclear potential.[38] Of course a US attack of this scale on Russia and Russia's probable responses would destroy political stability and economic viability in much of Europe and Central Eurasia in addition to whatever damage was caused to their respective state territories. Deterrence failure remains a dead end to be avoided; relative advantage is a cruel hoax.

Another challenge for the Obama administration is the potential for conflict between its objectives for achieving global denuclearization and for reducing the role of nuclear weapons in US military strategy on the one hand and for promoting advanced conventional weapons, including missile defenses and offensive weapons for precision global strike (PGS), on the other. For example, China's putative posture of minimum deterrence with respect to its numbers of deployed strategic weapons assumes a minimum second-strike capability relative to the United States that might be threatened by enhanced missile defenses and/or PGS weapons.[39] Furthermore, as previously noted, Russia has also warned that US missile defenses nominally aimed at Iran might eventually pose a threat to Russia's strategic nuclear deterrent.[40]

Conclusions

Nuclear weapons find themselves anomalies in a post–Cold War world in which they have become detached from their origins in a US-Soviet global rivalry. They still command respect for their unique ability to cause unprecedented mass destruction in a short time and to create long-term lethal effects. However, the environment for strategy-making and policy-relevant nuclear deterrence, arms control, and disarmament analysis has already changed profoundly—and more changes are ahead. Changes in technology are the most visible, but their impact extends beyond nuts and bolts. The diversification of offensive strike platforms, the development of improved antimissile and antiair defenses, and the increasing importance of cyber, including offensive and defensive information warfare, could combine to create a paradigm shift in the thinking about major war in advanced countries. The preceding discussion at best scratches the surface of this possibly tectonic change.

One paradox of the nuclear-cyber age is that the ability of the nuclear great powers to deter one another might encourage an undeserved complacency as to the substructure of regional nuclear deterrence, especially among existing and nuclear-aspirational powers in the Middle East and South and East Asia.[41] A multipolar nuclear power system outside Europe creates potential instabilities that will challenge existing notions of deterrence rationality as well as the endurance of the nonproliferation regime. US and allied planning for nuclear crises will have to take into account the possibility of scenarios with plot lines unscripted in past war games, including cases of ambiguity about whether "nuclear" use had actually occurred.[42] For these reasons, the two-dimensional analysis offered here, relative to US-Russian nuclear dynamics, overlaps inescapably and inevitably with the emerging multipolar nuclear power system of which it is a part. But now the United

States and Russia have the incentives and opportunities, unlike the Cold War Americans and Soviets, to pursue multilevel-system crisis management and shared nonproliferation objectives without a presumption of ideological hostility. The system "default" is to more nuclear initiative from the regions and (hopefully) to multilateral arms reductions beyond the precedents set by New START and any follow-ons.

The relationship between offensive nuclear force reductions and missile defenses (with or without cyber in the mix) is a complicated one. Missile defenses are more promising technologies than they were in the previous century. Expert studies, however, suggest that anti-BMDs are much more viable prospects against small attacks by regional foes than they are strategic counterweights to massive long-range missile attacks.[43] There is room for security cooperation in missile defense by NATO and Russia against possible threats posed by Middle Eastern or other nuclear capabilities. But the effects of nuclear weapons spread in the Middle East or additional proliferation in Asia cannot be precluded only by missile defenses or even by solely military responses. Smart diplomacy combined with limited regional missile defenses might buy time for more ambitious nonproliferation and counterproliferation initiatives to work.[44] ✪

Notes

[1] Freeman Dyson, *Weapons and Hope* (New York: Harper and Row, 1984), 223–38.

[2] According to information security and intelligence expert Joel Brenner, the US military-industrial complex is the world's "fattest espionage target"; moreover, the assault on our national defense establishment "is constant, it is relentless, and it is coming from all points on the compass in ways both old and new." Brenner, *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World* (New York: Penguin Books, 2013), 73.

[3] Thomas M. Chen, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace* (Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, September 2013), 9–10 and passim.

[4] Insightful analyses pertinent to this topic include Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, April 2013); Kamaal T. Jabbour and E. Paul Ratazzi, "Does the United States Need a New Model for Cyber Deterrence?," in *Deterrence: Rising Powers, Rogue Re-*

gimes, and Terrorism in the Twenty-First Century, ed. Adam B. Lowther (New York: Palgrave-Macmillan, 2012), 33–45; and Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009). Other references on this topic appear in later notes. The chronology of key government documents pertinent to cyberspace and US national security strategy is nicely summarized in Chen, *Assessment*, appendix, 45–46.

[5] On the information operations concepts of major powers, see Timothy L. Thomas, *Cyber Silhouettes: Shadows over Information Operations* (Ft. Leavenworth, KS: Foreign Military Studies Office, 2005), chaps. 5–6, 10, 14, and passim. See also Pavel Koshkin, "Are Cyberwars between Major Powers Possible? A Group of Russian Cybersecurity Experts Debate [*sic*] the Likelihood of a Cyberwar Involving the U.S., Russia or China," *Russia Direct*, 1 August 2013, http://russia-direct.org, in *Johnson's Russia List 2013*, no. 143 (6 August 2013), davidjohnson@starpower.net.

[6] Cyber weapons are not necessarily easy to use effectively as enabling instruments for operational-tactical or strategic effect. See Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge, UK: Cambridge University Press, 2007), especially chaps. 4–5.

[7] An expert critique of proposals for minimum deterrence for US nuclear forces appears in Dr. Keith B. Payne, study director, and Hon. James Schlesinger, chairman, Senior Review Group, *Minimum Deterrence: Examining the Evidence* (Fairfax, VA: National Institute for Public Policy, National Institute Press, 2013). For a favorable expert assessment of the prospects for minimum deterrence, see James Wood Forsyth Jr., Col B. Chance Saltzman, and Gary Schaub Jr., "Remembrance of Things Past: The Enduring Value of Nuclear Weapons," *Strategic Studies Quarterly* 4, no. 1 (Spring 2010): 74–90.

[8] USCYBERCOM plans for the equivalent of a "Star Wars" cyber defense against attacks on computer networks and other targets might be delayed or diverted by political controversy over National Security Agency surveillance. See David E. Sanger, "N.S.A. Leaks Make Plan for Cyberdefense Unlikely," *New York Times*, 12 August 2013, http://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html.

[9] "Putin Calls to Strengthen Protection against Cyber Attacks," *Itar-Tass*, 5 July 2013, in *Johnson's Russia List 2013*, no. 122 (5 July 2013), davidjohnson@starpower.net.

[10] Cited in Jonathan Earle, "U.S. and Russia Sign New Anti-Proliferation Deal," *Moscow Times*, 19 June 2013, in *Johnson's Russia List 2013*, no. 111 (19 June 2013), davidjohnson@starpower.net.

[11] Clifford S. Magee, "Awaiting Cyber 9/11," *Joint Force Quarterly*, issue 70 (3rd Quarter 2013): 76.

[12] Dr. Panayotis A. Yannakogeorgos and Dr. Adam B. Lowther, "Saving NATO with Airpower," *Royal Canadian Air Force Journal* 2, no. 1 (Winter 2013): 70.

[13] See, for example, Chen, *Assessment*, 10–11 and passim; Brenner, *Glass Houses*, especially chaps. 6–7; Timothy L. Thomas, *Three Faces of the Dragon: Cyber Peace Activist, Spook, Attacker* (Ft. Leavenworth, KS: Foreign Military Studies Office, 2012); and Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness* (Ft. Leavenworth, KS: Foreign Military Studies Office, 2011). See also Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), http://www.defense.gov/news/d20110714cyber.pdf; White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: White House, May 2011), http://www.whitehouse.gov/sites/default/files

/rss_viewer/international_strategy_for_cyberspace.pdf; Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle Barracks, PA: Strategic Studies Institute and US Army War College Press, April 2013), 8, http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1147; Robert A. Miller, Daniel T. Kuehl, and Irving Lachow, "Cyber War: Issues in Attack and Defense," *Joint Force Quarterly*, issue 61 (2nd Quarter 2011): 18–23; Libicki, *Cyberdeterrence and Cyberwar*; P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (New York: Penguin Books, 2009); John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Chicago: Ivan R. Dee, 2008), especially chaps. 6–7; and Libicki, *Conquest in Cyberspace*, especially 15–31.

[14] Miller, Kuehl, and Lachow, "Cyber War."

[15] Brenner, *Glass Houses*, 3.

[16] An example of such an attack was provided by the Stuxnet "worm" used to attack Iran's centrifuges as part of its nuclear program. Reportedly, some 1,000 of 5,000 centrifuges were temporarily disabled by the United States and Israel as part of a US program called Olympic Games that began under George W. Bush and continued into the Obama administration. See David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, 1 June 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0.

[17] Miller, Kuehl, and Lachow, "Cyber War," 19. Some of these objectives might also be accomplished by "friendly conquest" as opposed to "hostile conquest" in cyberspace. See Libicki, *Conquest in Cyberspace*, 125–26, for contrasting definitions and the remainder of chap. 6 for pertinent discussion.

[18] Patrick M. Morgan discusses the relationship between reexamination of deterrence theory and practice and cybersecurity in his article "The State of Deterrence in International Politics Today," *Contemporary Security Policy* 33, no. 1 (April 2012): 85–107, especially 101–3.

[19] Gray, *Making Strategic Sense of Cyber Power*, 36.

[20] According to Adam B. Lowther, deterrence can be conceptualized as a continuous spectrum with three components: deterrence by dissuasion, deterrence by denial, and deterrence by threat. Moving across the spectrum, from dissuasion through denial to threat, increases the level of action by the state attempting to deter. See Lowther, "How Can the United States Deter Nonstate Actors?," in Lowther, *Deterrence: Rising Powers*, 163–82, especially 166–67.

[21] Desmond Butler, "Flaws Found in U.S. Missile Shield for Europe," *Army Times*, 9 February 2013, http://www.armytimes.com/article/20130209/NEWS/302090305/Flaws-found-in-U-S-missile-shield-for-Europe. See also "US Missile Defense Shield Flawed—Classified Studies," *Russia Today*, 11 February 2013, http://rt.com/usa/us-missile-defense-flaws-811/.

[22] National Research Council, *Making Sense of Ballistic Missile Defense: An Assessment of Concepts and Systems for U.S. Boost-Phase Missile Defense in Comparison to Other Alternatives* (Washington, DC: National Research Council, National Academy of Sciences, National Academies Press, 2012), prepublication copy, accessed 17 September 2012, http://www.nap.edu.

[23] George N. Lewis and Theodore A. Postol, "The Astonishing National Academy of Sciences Missile Defense Report," *Bulletin of the Atomic Scientists*, 20 September 2012, http://thebulletin.org/astonishing-national-academy-sciences-missile-defense-report-0.

[24] Rebecca Slayton, *Arguments That Count: Physics, Computing, and Missile Defense, 1949–2012* (Cambridge, MA: MIT Press, 2013).

25. Superior treatment of technical, political, and economic challenges to US and NATO plans for European missile defenses is provided in Steven J. Whitmore and John R. Deni, *NATO Missile Defense and the European Phased Adaptive Approach: The Implications of Burden Sharing and the Underappreciated Role of the U.S. Army* (Carlisle Barracks, PA: Strategic Studies Institute and US Army War College Press, October 2013).

26. For US and NATO missile defense plans, see LTG Patrick J. O'Reilly, USA, director, Missile Defense Agency, "Ballistic Missile Defense Overview," 12-MDA-6631 (briefing presented to the 10th Annual Missile Defense Conference, Department of Defense, Washington, DC, 26 March 2012), http://mostlymissiledefense.files.wordpress.com/2013/06/bmd-update-oreilly-march-2012.pdf.

27. *Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms* (Washington, DC: Department of State, 8 April 2010), http://www.state.gov/documents/organization/140035.pdf.

28. The Obama Phased Adaptive Approach to missile defense will retain and improve some technologies deployed by the George W. Bush administration but shift emphasis to other interceptors supported by improved battle management command, control, and communications (BMC3) systems and launch detection and tracking. See Karen Kaya, "NATO Missile Defense and the View from the Front Line," *Joint Force Quarterly*, issue 71 (4th Quarter 2013): 84–89; John F. Morton and George Galdorisi, "Any Sensor, Any Shooter: Toward an Aegis BMD Global Enterprise," *Joint Force Quarterly*, issue 67 (4th Quarter 2012): 85–90; and Frank A. Rose, deputy assistant secretary, Bureau of Arms Control, Verification and Compliance, "Growing Global Cooperation on Ballistic Missile Defense" (remarks as prepared, Berlin, Germany, 10 September 2012), http://www.state.gov/t/avc/rls/197547.htm.

29. For example, see "Moscow Needs More 'Predictability' in NATO Missile Defense Plans," *RIA Novosti*, 23 October 2013, in *Johnson's Russia List 2013*, no. 191 (24 October 2013), davidjohnson@starpower.net.

30. For pertinent discussion, see the essays in Dr. Adam Lowther, ed., *The Asia-Pacific Century: Challenges and Opportunities* (Maxwell AFB, AL: Air University Press, Air Force Research Institute, April 2013).

31. Peter Baker and David E. Sanger, "Obama Has Plans to Cut U.S. Nuclear Arsenal, If Russia Reciprocates," *New York Times*, 18 June 2013, http://www.nytimes.com/2013/06/19/world/obama-has-plans-to-cut-us-nuclear-arsenal-if-russia-reciprocates.html?_r=0. See also Roberts Rampton and Stephen Brown, "Obama Challenges Russia to Agree to Deeper Nuclear Weapon Cuts," Reuters, 20 June 2013, in *Johnson's Russia List 2013*, no. 212 (20 June 2013), davidjohnson@starpower.net.

32. The author gratefully acknowledges that figures 1–4 are based on a model originally developed by Dr. James J. Tritten, who is not responsible for its use here or for any arguments or opinions in this article.

33. Force structures in the analysis are notional and not necessarily predictive of actual deployments. For expert appraisal, see Hans M. Kristensen, *Trimming Nuclear Excess: Options for Further Reductions of U.S. and Russian Nuclear Forces*, Special Report no. 5 (Washington, DC: Federation of American Scientists, December 2012), http://www.fas.org/programs/ssp/nukes/publications1/TrimmingNuclearExcess.pdf; Gen James Cartwright, retired, chair, *Global Zero U.S. Nuclear Policy Commission Report: Modernizing U.S. Nuclear Strategy, Force Structure and Posture* (Washington, DC: Global Zero, May 2012), http://www.globalzero.org/files/gz_us_nuclear_policy_commission_report.pdf; Pavel Podvig, "New START Treaty

in Numbers," *Russian Strategic Nuclear Forces* (blog), 9 April 2010, http://russianforces.org/blog/2010/03/new_start_treaty_in_numbers.shtml. See also Joseph Cirincione, "Strategic Turn: New U.S. and Russian Views on Nuclear Weapons," New America Foundation, 29 June 2011, http://newamerica.net/publications/policy/strategic_turn; and "U.S. Strategic Nuclear Forces under New START," Arms Control Association, July 2013, http://www.armscontrol.org/factsheets/USStratNukeForceNewSTART.

34. According to some experts, the United States could conceivably satisfy its requirements for strategic nuclear deterrence with fewer than 400 deployed warheads on intercontinental launchers. See James Wood Forsyth Jr., B. Chance Saltzman, and Gary Schaub Jr., "Minimum Deterrence and Its Critics," *Strategic Studies Quarterly* 4, no. 4 (Winter 2010): 3–12. Counterarguments appear in Payne and Schlesinger, *Minimum Deterrence: Examining the Evidence*, passim, especially 65–70.

35. Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington: University Press of Kentucky, 2001), 101.

36. For example, see Keir A. Lieber and Daryl G. Press, "The New Era of Nuclear Weapons, Deterrence, and Conflict," *Strategic Studies Quarterly* 7, no. 1 (Spring 2013): 3–14.

37. Cham E. Dallas et al., "Nuclear War between Israel and Iran: Lethality beyond the Pale," *Conflict and Health*, 10 May 2013, via BioMed Central, accessed 15 May 2013, http://www.conflictandhealth.com/content/7/1/10. See also Anthony H. Cordesman, *Iran, Israel, and Nuclear War: An Illustrative Scenario Analysis* (Washington, DC: Center for Strategic and International Studies, 19 November 2007), http://csis.org/files/media/csis/pubs/071119_iran.is&nuclearwar.pdf; and US Congress, Office of Technology Assessment, *The Effects of Nuclear War* (Washington, DC: Government Printing Office, May 1979), especially 27–44 for case studies of attacks on a single city. The Office of Technology Assessment cautions that the effects of even a small or limited nuclear attack would be "enormous" (p. 4).

38. Cited in Ilya Maksimov and Sergey Kuksin, "Russia Will Not Be a Bystander in the Arms Race," *Rossiyskaya Gazeta*, 28 June 2013, in *Johnson's Russia List 2013*, no. 122 (5 July 2013), davidjohnson@starpower.net.

39. Lora Saalman, "How Chinese Analysts View Arms Control, Disarmament, and Nuclear Deterrence after the Cold War," in *Engaging China and Russia on Nuclear Disarmament*, Occasional Paper no. 15, ed. Cristina Hansell and William C. Potter (Monterey, CA: James Martin Center for Nonproliferation Studies, April 2009), 47–71.

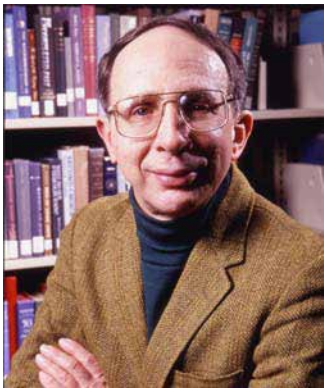
40. For an expansion of the point about the possible conflict between Obama nuclear disarmament and advanced conventional weapons modernization goals, see Andrew Futter and Benjamin Zala, "Advanced US Conventional Weapons and Nuclear Disarmament: Why the Obama Plan Won't Work," *Nonproliferation Review* 20, no. 1 (2013): 107–22, http://dx.doi.org/10.1080/10736700.2012.761790.

41. Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (New York: Henry Holt, 2012), especially 215–20 and 267–70. For additional perspective on the second nuclear age, see Lowther, *Deterrence: Rising Powers*; Paul K. Davis, *Structuring Analysis to Support Future Decisions about Nuclear Forces and Postures*, Working Paper WR-878-OSD (Santa Monica, CA: RAND National Defense Research Institute, September 2011); Michael Krepon, *Better Safe Than Sorry: The Ironies of Living with the Bomb* (Stanford, CA: Stanford University Press, 2009), especially 94–132; and Colin S. Gray, *The Second Nuclear Age* (Boulder, CO: Lynne Rienner Publishers, 1999).

[42] For some interesting possibilities in this regard, see George H. Quester, *Nuclear First Strike: Consequences of a Broken Taboo* (Baltimore: Johns Hopkins University Press, 2006), 24–52, especially 25–30. This author road tests some models for multipolar nuclear power systems in "Anticipatory Attack," his working paper in progress, available upon request.

[43] National Research Council, *Making Sense of Ballistic Missile Defense*.

[44] Sources of instability in the second nuclear age will include major powers, secondary powers, and groups sometimes making creative political uses of nuclear weapons short of war, overlaid by great-power competition within a multipolar nuclear system. See Bracken, *Second Nuclear Age*, especially 93–126; James E. Goodby, "The End of a Nuclear Era," *New York Times*, 14 August 2013, http://www.nytimes.com/2013/08/15/opinion/global/the-end-of-a-nuclear-era.html?_r=0; and C. Dale Walton and Colin S. Gray, "The Geopolitics of Strategic Stability: Looking Beyond Cold Warriors and Nuclear Weapons," in *Strategic Stability: Contending Interpretations*, ed. Elbridge A. Colby and Michael S. Gerson (Carlisle Barracks, PA: Strategic Studies Institute and US Army War College Press, 2013), 85–115.



Dr. Stephen J. Cimbala

Dr. Cimbala (BA, Penn State; MA, PhD, University of Wisconsin–Madison) is Distinguished Professor of Political Science at Penn State–Brandywine and the author of numerous works in the fields of US national security, nuclear arms control, and other topics. He is an award-winning Penn State teacher, and his recent publications include *Arms for Uncertainty: Nuclear Weapons in US and Russian Security Policy* (Ashgate, 2013) and *US National Security: Policymakers, Processes and Politics* (with Sam C. Sarkesian and John Allen Williams) (Lynne Rienner, 2013).

Let us know what you think! Leave a comment!