O Divine Art of Subtlety and Secrecy in the Age of Nuclear Byzantine Generals

The NAPSNet Policy Forum provides expert analysis of contemporary peace and security issues in Northeast Asia. As always, we invite your responses to this report and hope you will take the opportunity to participate in discussion of the analysis.

Recommended Citation

Peter Hayes, "O Divine Art of Subtlety and Secrecy in the Age of Nuclear Byzantine Generals", NAPSNet Policy Forum, September 19, 2013, https://nautilus.org/napsnet/napsnet-polic-forum/divine-art-of-subtlety-and-secrecy-in-the-age-of-nuclear-byzantine-generals/

by Peter Hayes

September 19, 2013

I. Introduction

Peter Hayes writes: "Ultimately, commanders have to trust themselves, their staff, and their organization. But if ...problem[s] reside in the nature of nuclear warfare itself, and the organizations are incapable of perfect implementation of nuclear strategy...then nuclear weapons are fatally flawed as a means of warfare..." Hayes quips, "Perhaps [we] should revise [the NRA] slogan: “Guns don’t kill people, people do” to: “Nuclear weapons don’t start nuclear wars; nuclear weapons organizational systems and people do.”

Peter Hayes is Professor of International Relations, School of Global, Urban and Social Studies, Royal Melbourne Institute of Technology University, Australia and Director, Nautilus Institute.

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

II. Policy Forum by Peter Hayes

O Divine Art of Subtlety and Secrecy in the Age of Nuclear Byzantine Generals

In the *Art of War*, Sun Tzu praises the “divine art” of using invisibility and inaudibility to attack an enemy’s weak points. He approvingly quotes Ts`ao Kung: "Emerge from the void, strike at vulnerable points, shun places that are defended, attack in unexpected quarters."

Large organizations are cumbersome, slow, and have many moving parts. When they add new defenses, they create new angles and pathways of attack. The more complex the defenses, the more an agile, skillful, and alert adversary can identify porosity in the defense itself, and use it to enter the adversary’s territory unobserved.

As Eric Schlosser explains in his Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety, human fallibility combined with and technological complexity generates an "always/never" dilemma. "Ideally,” he writes, “a nuclear weapon would always detonate when it was supposed to -- and never detonate when it wasn't supposed to.” The result is organizational controls that fail, as he documents, in extraordinarily dangerous ways.

This combination of big organizations relying on standard operating procedures striving for absolute control over nuclear weapons may lead to cybernetic outcomes that reduce ultimate control. As Paul Bracken explains, the US Strategic Air command found that many proposed fail-safe systems could lead to unanticipated outcomes, and was forced to adopt relatively loose controls in order to be able to fire the force at all—adding a twist to the hazards documented by Schlosser in that the controls also proffer an enemy a way to disrupt its nuclear-armed adversary.

Even without malevolent, stealthy attack, nuclear organizations can trip up strategy. In their U.S. Air Force Tactical Missiles 1949-1969, The Pioneers, George Mindling and Robert Bolton describe deployments of nuclear tipped missiles in Asia-Pacific and Europe. Jon Mitchell documents one high alert of these missiles in Okinawa during the 1962 Cuban Missile Crisis which, if push had come to shove between the Soviets and the United States, would have resulted in launching these missiles at

China! This was an artifact of the rigidity of the targeting system at lower echelons, whatever the intentions would have been at the top echelons of the US command system at the time.

Today, nuclear weapons organizations are old and tired in the United States. In Russia, the situation with nuclear forces is even worse. In China, strategic nuclear forces are modernizing and growing fast, so perhaps they are on an organizational up-swing. But in these and the other nuclear weapons states, the same control-defense-release dilemma is at work.

Consequently, new forms of attack involving stealth and pre-emplacement of "sleepers" inside enemy states and sending "information bombs" across physical and cyber-borders are in play with respect to nuclear weapons organizations. The United States spends millions of dollars to scan its own intelligence workforce looking for individuals with connections to al-Qaeda and other hostile groups. All major states are already engaged in offensive cyber-warfare operations, including the United States, to exploit silent, stealthy holes in their adversaries' organizations. Operatives from al-Qaeda reportedly run technological research programs to figure out digital means to defeat drones attacking from the sky—and it may be only a matter of time before drone warfare comes to the United States as reprisal for US attacks around the world.

When traditional defenses built to secure and control nuclear weapons are overlaid by new types of offensive warfare, no-one can anticipate all the failures that may ensue. These may be the result of tight coupling of these systems, generating reciprocal amplification of error due to the interaction of enemy nuclear weapons organizations; or they may be the result of a persistent, disciplined, and determined non-state actor who manages to enter a nuclear weapons organization inside-out, either in person, or virtually.

When new sources of organizational instability arise due to unreliable components, arbitrary errors in function may result that are random and can amplify errors in related functions—a fault known as the Byzantine Generals' Problem –their dilemma being the problem of how to act in concert when some generals may be traitors—but no-one knows who.

Today, no nuclear command-and-control organization, no matter how "isolated" by design or location, operates without being nested in a vast network of support systems, all of which represent entry points and possible modes of failure, including common modes. No-one can be sure of the security of their nuclear forces or of the reliability of their control.

Even the DPRK has this problem. It is often said that due to its isolation and totalitarian nature, the North Korean military is relatively invulnerable to cyber-warfare that might cripple military infrastructure such as command-and-control systems for nuclear weapons. However, there's no reason to believe that the Korean People's Army is not using computer systems for command, control, communications and other functions, connected via fiber optic cables laid underground especially to avoid US and South Korean signals intelligence.

Moreover, there's even less reason to think that its adversaries have not attempted to exploit the well-known proclivity of the regime to read the laptops of visitors to its country. Loading one of these machines with a replicating virus is a sure-fire transmission strategy. Should it gain access to the DPRK's military's IT system, such malware may have devastating impact given its propensity to extraordinarily centralized control—possibly far more so that its reported offensive cyber-warfare operations against South Korea and its allies whose loosely coupled military units may be far less vulnerable to error propagation and more capable of autonomous operations.

Ultimately, commanders have to trust themselves, their staff, and their organization. But if the problem resides in the nature of nuclear warfare itself, and the organizations are incapable of

perfect implementation of nuclear strategy—indeed, are driven to pervert the strategy in order to secure the weapons and vice versa—then nuclear weapons are fatally flawed as a means of warfare.

Perhaps the US National Rifle Association's should revise its slogan: "Guns don't kill people, people do" to read: "Nuclear weapons don't start nuclear wars; nuclear weapons organizational systems and people do."

III. NAUTILUS INVITES YOUR RESPONSES

The Nautilus Peace and Security Network invites your responses to this report. Please leave a comment below or send your response to: nautilus@nautilus.org. Comments will only be posted if they include the author's name and affiliation.

View this online at: https://nautilus.org/napsnet/napsnet-policy-forum/divine-art-of-subtle-y-and-secrecy-in-the-age-of-nuclear-byzantine-generals/

Nautilus Institute
608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org