The Cyber Threat to Nuclear Stability

February 12, 2016

By Paul Bracken

Paul Bracken is Professor of Management and Political Science at Yale University. He is author of *The Command and Control of Nuclear Forces* (Yale University Press, 1983); *Fire in the East: The Rise of Asian Military Power and the Second Nuclear Age* (HarperCollins, 1999); and *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (Times Books, 2012). He is currently working on a book on stability in the second nuclear age. He is a member of FPRI's Board of Advisors.

Abstract: *The thesis of this article is that cyber war technologies are spilling over into precision strike and nuclear mission areas. The result will transform deterrence and arms race stability and lead to other significant changes. The driver behind this is a combination of long standing problems with mobile missiles along with new technologies not usually factored into strategic assessments: big data analytics, computer vision, and related information systems. When combined with drones and precision strike, the hunt for mobile missiles is becoming faster, cheaper, and better. The implications of this finding vary by country, but will shape major power nuclear modernization, crisis stability among secondary powers, and conventional attack of nuclear deterrents.*

Air Force Staff and civilian personnel concentrate on exercise scenarios during "Cyber Guard 2015" in Suffolk, Va (DoD photo by Marvin Lynchard.)

doi: 10.1016/j.orbis.2016.02.002

The rising alarm to date over cyber security has focused on pilfered files, disruption of electricity and communications, and hacks of commercial and military computers. But a more serious form of cyber threat is now apparent. Cyber attacks can destabilize nuclear deterrence because they are a key element in locating mobile missiles, which became the foundation of deterrence among the new nuclear states in the Middle East, South Asia, and East Asia, thereby upsetting the embryonic nuclear stability that appears to have developed in these regions. The driver for this is not the hacking of command and control (e.g., loading malware into the firing circuit of a nuclear missile so it is unable to launch). Rather, it arises from the integration of cyber weapons and other technologies—especially drones, precision strike, and data analytics. Such an integrated system provides a remarkable ability to hunt mobile missiles that are the deterrent backbone of the new nuclear powers. Mobile systems can be found, their movements tracked, and then destroyed, using conventional or nuclear strikes. The technologies for doing so have received enormous impetus in recent years from both business and military interests.

A remarkable, decades-long interaction between strategic postures is playing out before our eyes. In the 1990s, North Korea, Pakistan, India, and Israel began to base their nuclear deterrents on mobile systems. Even some non-nuclear (so far) states (e.g., Saudi Arabia, Syria, Iran), also shifted to mobile missiles. The impetus for this shift was the United States' decisive success with precision strikes in the first Gulf War, Kosovo, Iraq, and Afghanistan. Since almost any fixed target is vulnerable, the militaries of many states believed that mobile systems were able to offer a way out to avoid destruction by a precision conventional attack. But this situation is now changing because mobile systems are not nearly as survivable as was believed a decade ago. Long recognized weaknesses in mobile systems have combined with new, cutting edge search technologies to strip features that seemed to assure survivability. This development has considerable strategic implications. For one thing, it enhances the possibility of a surprise attack by a smaller, new nuclear power against another.

In addition, nuclear modernization by major powers, like the United States, Russia and China, will take place in a *cyber* environment, where the *search* for mobile systems will be cheaper, faster, and better. This is a radically different information environment than the one that characterized the Cold War or the era of the "revolution in military affairs" (RMA) of the late twentieth century. Then, only *accuracy* was improving while s*earch* continued to be slow, costly, and spotty. How the United States, China, and Russia build cyber into their modernization programs will be a contentious issue. The way they deal with secondary nuclear states (e.g., tracking their deterrents, information transfer to regional allies and the like) will also be important. Extended deterrence, for example, will require new information structures that balance regional deterrence with stability.

Strategic Postures

A strategic framework rather than a predictive academic theory is the first requirement for any coherent discussion about nuclear weapons. Without it a debate about strategy and modernization, biases and politics lacking the rational context that