

Cyberwar as a Confidence Game

We encourage you to e-mail your comments to us at: strategicstudiesquarterly@maxwell.af.mil.

Reader's Comments

From Dave:

One thing missing from this paper is any evidence that this kind of logic (aka, Fear Uncertainty and Doubt in military information systems as applied to network centric warfare) has any real-world effect. Militaries (including our own) simply don't take these things into account when deploying new systems.

But the main anomaly in the paper is simple: He treats Stuxnet as an aberration, rather than the tip of the iceberg that finally made the newspapers. And this leads him (and most other strategic analysts) to conclude that hacking does not have real world effects. I have to assume this is the WWII legacy of Enigma - where in order to take advantage of intelligence you had to go out and order your sub killers to go sink a boat. But just because hacking is tied to intelligence > bodies in most countries, and staffed with people who look and act a lot like intelligence officers, does not make it the same thing. Hacking is as kinetic as a cruise missile when you do it right.

From Greg:

I agree with you Dave. Cyberwar is technical. Granted, like any war, it must be backed by intel and psyops. But, like any war, the kills people see in the press are kinetic. Cruise missiles are technical, and kinetic. But, everything is backed by intel. Even missiles. In cyber, the importance of HUMINT far outweighs that of kinetic damage.

The technology is new and different, but the classic principle applies. This war is not new.