# US needs new national strategy for era of cyber aggression, new paper concludes

April 19 2010

The nominee to head the Pentagon's new CyberCommand testified in front of Congress late last week that employing Cold War strategies to cyberwarfare challenges may not work for the United States.. A newly published research paper by a University of Cincinnati professor and colleagues goes a step further and concludes more directly that deterrence can not serve as the primary national cybersecurity strategy.

In testimony on April 15th before the U.S. Congress, Lt. General Keith A. Alexander offered his view that a Cold War approach of nuclear deterrence as a strategy for securing the United States might not translate effectively into the new realm of cyberwarfare, an area where the U.S. is just beginning to think about broader strategic approaches.

That same subject area is addressed in a new article in the Journal of Homeland Security and Emergency Management by UC Professor of Political Science Richard Harknett and co-authors John Callaghan and Rudi Kauffman. They say that to deal with cyberaggression, a more traditional model of warfighting will have to become the focus if cyberspace is to become more secure and safe.

In their article, "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," Harknett and his co-authors argue that "the inherent characteristics of cyberspace require adoption of a full war-fighting posture that moves out of the fifty-plus year comfort zone of deterrence as the dominant strategic anchor... We must organize thinking about managing cyber-leveraged war so that damage is contained and reduced.

Counter-intuitively, these futuristic threats require us to adopt the historical posture of traditional warfare."

By traditional warfare, the authors mean the traditional offense-defense framework that has defined war strategy throughout much of history. While a deterrence posture works in a nuclear context when the alternative for both sides is mutually-assured destruction, several factors unique to cyberwarfare make applying the deterrence model an awkward fit.

For one thing, cyberwarfare is an offense-dominated enterprise. Attacks can be carried out cheaply and in ways that make determining responsibility a slow process and difficult to establish. Deterrence is also undercut by the possibility of attackers using previously unknown approaches that greatly diminish their susceptibility to responses.

Harknett and his co-authors suggest the establishment of a three-tiered "continuum of cyberaggression" to help guide U.S. strategy in responding to attacks. They write: "Implicit in this categorization is that not every cyber threat reaches the level of national security concern, but given the unique, ubiquitous and dual-use nature of digital and computer technology, a national cybersecurity strategy must comprehensively consider the interconnectivity across the continuum of cyberaggression."

The three proposed tiers, in order of severity, are cybercrime, cyberespionage and reconnaissance, and the most serious level, cyber-leveraged war. The highest level would cover not just purely digital attacks, but also those that lead to disruption or destruction of physical infrastructure as well, such as a broad attack against the electric grid.

It is at this highest level that the United States needs to adopt policy that is oriented toward containing damage as well as for fighting in an offensive posture against those who would seek to engage in cyber-

leveraged war. Being well-prepared, both offensively and defensively, will produce caution in the minds of others about attacking, and, thus, the strategy can produce a residual deterrent effect. But, the authors believe, this is likely to be temporary and under constant pressure.

"Importantly, as the ubiquity of cyber grows societally across the globe, effective norms against cyberaggression will become increasingly important in reigning in unacceptable forms of behavior in this new realm of human interaction," Harknett and colleagues write. This line of argument seems to parallel thoughts by Lt. General Alexander, who called on Congress to consider new legal and policy contexts for cyberspace.

In the end, however, Harknett and his co-authors conclude that "in facing down threats to national security, the United States must organize itself around the reality of war preparation and fighting, rather than the hope of avoidance, as the principle upon which cybersecurity will be advanced."

Provided by University of Cincinnati