From: **Chuck Woolery** chuck@igc.org
Subject: RE: SUBSCRIBERS: Items
Date: September 17, 2022 at 6:05 PM
To: Dick Bernard dick.bernard@icloud.com

Nukes not worth the worry.

https://www.washingtonpost.com/opinions/2022/09/15/deterrence-cyberspace-conflict-new-strategy/

Opinion | Will deterrence have a role in the cyberspace 'forever war'? - The Washington Post

Opinion

Will deterrence have a role in the cyberspace 'forever war'?

By David Ignatius
Columnist Follow
September 15, 2022 at 6:36 p.m. EDT

At a time of growing concern about possible nuclear threats from Russia, some prominent defense strategists are arguing for a new theory of deterrence. They argue that military conflict is now so pervasive in cyberspace that the United States should seek to shift away from deterrence in this domain — and more aggressively exploit the opportunities it presents.

Beware, reader, in exploring this topic: Deterrence strategy is one of the wooliest and most abstract areas of defense analysis. In the early Cold War decades, it was the province of professors such as Herman Kahn at the Rand Corp., and Thomas Schelling and Henry Kissinger at Harvard — sometimes collectively known as the "wizards of Armageddon." They "thought about the unthinkable" when it came to nuclear war, partly to dissuade the Soviet Union from ever launching an attack. Times have changed, argues the new book "Cyber Persistence Theory: Redefining National Security in Cyberspace." Its three authors have all worked closely on cyber strategy for the Pentagon: Michael P. Fischerkeller as a cyber expert with the Institute for Defense Analyses; Emily O. Goldman as a strategist at U.S. Cyber Command; and Richard J. Harknett as a cyber expert at the University of Cincinnati and the first scholar-in-residence at Cyber Command.
The book isn't an official policy document. But a foreword from Gen. Paul Nakasone, the head of Cyber Command and the National Security Agency, notes that the three authors have been "laying the foundations for the Command's

approach of Persistent Engagement" and that their book offers a "framework for understanding ... operational effectiveness moving forward."
To sum up the authors' arguments: Cyberweapons fundamentally change the nature of warfare. Borders don't matter much to digital code. And cyberwar is a continuum (and always happening at a low level), rather than an on-off switch. It's a new domain, with new rules.

"Cyberspace must be understood primarily as an environment of exploitation rather than coercion," the authors write. "Achieving strategic gains in the cyber strategic environment does not require concession of the opponent." In other words, much of what we think we know about war doesn't apply in this domain.
I had a chance to explore this esoteric subject in August, when the authors asked me to moderate a public discussion of their book at the National Defense University. The gathering produced a lively exchange among military cyber strategists.

To get an overview of the evolution of deterrence thinking, let's start with Harknett's vision of three phases in the history of warfare, culminating in cyber. The first period, beginning in ancient history, involved "conventional" weapons — rocks at first, then eventually guns, cannons, battleships, bombers — to coerce the adversary into submission. Nation states zealously defended their borders, and the goal of warfare was coercion and victory. Deterrence involved having more and better cannons, bigger battleships, more planes. But obviously, looking at the two world wars in the 20th century, that version of deterrence didn't work very well. The arsenals almost invited war.

That first period lasted until 1945, when the United States introduced nuclear weapons that, soon enough, were duplicated by the Soviet Union. With the potential to kill hundreds of millions of people in a quick exchange, these weapons could effectively destroy civilization. The culmination of war became not victory but doomsday.
Nuclear war, as was often said, cannot be won and should never be fought. So, the goal of nuclear strategy was not to win wars but to prevent them. This nuclear version of deterrence has worked quite well for 73 years and counting.
The third period involves cyberweapons, and the assumptions are fundamentally different. Weapons can't be counted, identified, tracked or easily controlled. They are used in a borderless electronic world where traditional ideas of sovereignty don't work very well. The authors argue that this domain is "micro-vulnerable (and inherently exploitable)," in that targets can be hit easily, but "macro-resilient (and thus stable)," because nations will persist, even if targeted.
Two lessons of the Ukraine war is that cyber defenses appear to work better than might have been expected, and that cyber offense works worse. That's one explanation for Ukraine's amazing resilience against the Russian onslaught.
The authors offer some suggestions for this new domain: Strategists should have rules for continuous engagement, rather than plan for contingencies; they should prepare for continuous operations not "episodic" ones, and they should seek

cumulative gains, rather than final victory. As the authors wrote in a recent article in the National Interest: "Because of the fluidity of digital technology, security rests on seizing and sustaining the initiative."
Cyberspace might prove to be the ultimate version of forever war. But if these strategists are right, it could be less dangerous, and ultimately more stable, than the convulsive explosions we've known as war for millennia.

My comment: Traditional weapons are used up when used. Cyber, biological, and nano technologies can be weaponized and made to be replicable when used. This single factor changes war profoundly because engineering them are relatively cheap, easy, easy to hide and deliver, reproduce themselves, and they don't leave a fingerprint or a return address. This makes them virtually untraceable and useful for anonymous or red flag attacks. Even framing another nation or violent extremist group as the attacker. Together the weaponization of these technologies make the cold war concepts of "peace through strength", and deterrence - obsolete. Dead! And 'forever wars' a permanent fixture in our lives until humanity gains wisdom to put the protection of human rights and the environment above the protection of national sovereignty and corporations. AI might gain wisdom and do this before we do. Until then, Bio and Cyber security are oxymorons. Security has always been iffy, but these tiny bits of information will continue to be engineered to evade defenses and target specific weaknesses in the living systems and structures, and the cyber systems and structures that modern life depends on. Things change. Can we?

Chuck Woolery, Former Chair
United Nations Association, Council of Organizations
315 Dean Dr., Rockville, MD 20851
Cell:240-997-2209 chuck@igc.org

Blogs: 435 Campaign: www.435globaljustice.blogspot.com (May 2017 through today)
Dothefreakinmath http://dothefreakinmath.blogspot.com (June 2006 to Nov 2016)
The Trilemma http://trilemma.blogspot.com/ (Oct 2011 to Nov 2013)

"Today the most important thing, in my view, is to study the reasons why humankind does nothing to avert the threats about which it knows so much, and why it allows itself to be carried onward by some kind of perpetual motion. It cannot suffice to invent new machines, new regulations, new institutions. It is necessary to change and improve our understanding of the true purpose of what we are and what we do in the world. Only such an understanding will allow us to develop new models of behavior, new scales of values and goals, and thereby invest the global regulations, treaties, and institutions with a new spirit and meaning." **President Vaclav Havel, Czech Republic.**

"A human being is part of the whole, called by us 'Universe'; a part limited in time and space. He experiences himself, his thoughts and feelings, as something separated from the rest - a kind of optical delusion of his consciousness. This delusion is a kind of prison for us, restricting us to our personal desires and affection for a few persons nearest us. Our task

our personal desires and affection for a few persons nearest us. Our task must be to free ourselves from this prison by widening our circle of compassion to embrace all living creatures and the whole nature in its beauty. Nobody is able to achieve this completely, but striving for such achievement is, in itself, a part of the liberation, and a foundation for inner security." *-Albert Einstein. As quoted in Quantum Reality, Beyond the New Physics, p. 250.*

"The sad truth...is that most evil is done by people who never made up their minds to be or do either evil or good." Hannah Arendt quoted in The Bulwork.

What are you doing to ensure the funding and achievement of the 17 Sustainable Development Goals by or before the year 2030? Connect the dots! See the web of life! Achieve 'justice for all'. Or, prepare for the catastrophic consequences. cw

From: Dick Bernard <dick.bernard@icloud.com>
Sent: Friday, September 16, 2022 8:59 PM
To: Dick Bernard <dick.bernard@icloud.com>
Subject: SUBSCRIBERS: Items

Some items of possible interest to you in the next two weeks: https://thoughtstowardsabetterworld.org/all-hands-on-deck/