The Passy Press®
Letters to the Editor

From: Michael Wyly <mwyly@undisclosed.com>
To: Nick Gardiner <enpg@thepassypress.com>
Sent: 1 December 2018 at 16:30:04 CET
Subject: Cyber Essay, November 2018

Dear Sir,

In his prescient article, “The Existential Threat of Cyber”, the author submits that the man-made creation of “cyberspace” has become a threat to the very survival of our country. Nature and cyberspace are “fundamentally different” in that our adversaries, unable to change the boundaries of nature, will alter the boundaries of cyberspace, placing our economic, political, and military sectors at risk.

Why did we ever start sending classified information via cyber in the first place? What was the matter with transmitting top secret materials on paper in a double-envelope delivered by a courier with a .45 pistol on his hip, the documents to be destroyed outdoors in the “burn barrel” after reading?

To withdraw from use of cyberspace would seriously limit our competitiveness. Also, cyberspace offers opportunities to disrupt and deceive our adversaries. that is too lucrative to ignore. Yes, we are spied on. But we can spy too. Also our adversaries’ understanding and use of this new medium places us in a position where we must participate to survive economically.

Compared to all other nations in the world it is the United States’ combination of productive innovation with unbridled freedom that makes us what we are: *the* nation that exceeds all others in opportunity and quality of life.

Now that the cyber age is upon us we find ourselves able to compete *only if* we join and remain in the world of cyber.

Any initiative that seeks to be competitive, in order not to stagnate and smother under the success of competing forces must incorporate a clearly defined mission with a focus, enough ambiguity to invite innovation as it emerges, decisive leadership to maintain momentum, and enough flexibility among leadership to allow *speed* in its implementation. All of the above require communications via cyberspace in order to be competitive.

I will draw from my own profession as a thirty-plus year U.S. Marine in order to present here an example of how *military* necessity might call for an understanding by leadership of how to field a new idea without one’s adversary being able to derive a “picture” of what we are doing, cyber espionage notwithstanding

There arises in every era a need to project military force into hostile territory. It is out of that need that our U.S. Marine Corps has risen to the challenge of so-called “forcible entry”. Well known now are the efforts in the 1920’s and 1930’s on the part of the U.S. Marine Corps with the Navy to develop a means of getting from ship to shore in what appeared more and more to be an inevitable conflict in the Pacific with the Japanese. We were able in that era to conceptualize and

actually practice with enough security that we could develop a tactical scenario that would work: the amphibious landing in the transition of forces from ship to shore.

A World War II amphibious landing required conceptualization of four basic aspects defined above: (1) *a focus* in the form of a chosen beachhead; (2) enough *ambiguity* to invite surprise as we make battlefield decisions in real time - such as where and when to break out of the beachhead once secured; (3) decisive leadership to maintain momentum in the form of a commander's order and attack plan *after* the landing; and (4) enough flexibility to keep the enemy off balance through *speed* in implementing the attack inland once ashore.

To project combat power ashore was and still is why we have a Marine Corps. How will we do it next time? We don't know yet and neither does our "enemy", whoever that may be.

What is certain is that in our modern world the first two decisions can be worked into deception plans that can take their form in cyberspace while the third and fourth, for security, must remain exclusively in human-to-human close-hold top secrecy, nowhere to be found in cyberspace save for a few "detractors" submitted to confuse and mis-lead the enemy.

Let the foregoing military scenario serve as an example. Competition is competition whether on the battlefield or between two competing businesses in a contest over one to win the other's money. The analogies abound.

These same four decisions are common to any competitive endeavor: (1) focus on a course of action; (2) an action chosen in real time based on the developing situation; (3) subsequent actions after the first action is initiated; and (4) an ongoing sensitivity to opposing or competing actions.

In this way we take advantage of the new world of cyberspace without sacrificing the ultimate key to security: the silence of non-communication except between close and trusted individuals, unseen and unheard.

The real concern now is to recognize that cyberspace – manmade though it is – has passed out of man's control in terms of our laws and regulations. Holding to our principle of Government by The People, we need a means to actively educate The People on what cyberspace is and its many ramifications that now so strongly influence everything from industry through government and schools, public and private. Our own *United States* Government has spread its rules and regulations over some ten different sub-committees in the House and Senate, these under the separate headings of Defense, State, Intelligence, and Infrastructure, each with its own portfolio on "Cyber". Decentralization is healthy so long as the separate agencies communicate with each other. Once such communication is in being our Government can initiate an education program, and then enforce penalties for cyber-theft and like crimes.

We are still human. And over all things mechanical, we have the edge.

Sincerely,

Michael Wyly

Michael Wyly, Colonel Michael D. Wyly USMC (Ret) and was Executive Director, CEO and Founder of The Bossov Ballet Theater in Maine. He is a graduate of the United States Naval Academy.