The Passy Press®
Letters to the Editor

From: Lee Gaillard < lgaillard@undisclosed.com>
To: Nick Gardiner <enpg@thepassypress.com>
Sent: 23 Nov 2018 at 04:17
Subject: Cyber Essay, November 2018

Dear Sir,

On Friday, November 16, *The Hill* reported that "President Trump...signed into law a bill that cements the Department of Homeland Security's (DHS) role as the main agency overseeing civilian cybersecurity, with a focus on securing federal networks and protecting critical infrastructure from cyber threats." Talk about too little, too late. And just how much attention will DHS be able to pay to cybersecurity given its numerous other foci?

Clearly, Name Withheld's essay on the existential threat of cyber could not appear at a more crucial moment.

The writer justly identifies the key role of the U.S. in creating the technologies that govern cyber operations...and the difficulties of setting boundaries in a limitless domain where cyber theft of intellectual property has run rampant. The threats are real--especially economically and militarily, as she or he points out. How do we protect ourselves? What consequences can be imposed...and by whom? What entity becomes 'The Enforcer'? And totalitarian governments, with their command-and-control structures, have the advantage of focus without the legal constraints democracies impose upon themselves. All good points.

What I miss, however, is 1) some key background context, and 2) specific examples beyond just annual economic losses ranging from $225 billion to $600 billion.

Background context? The writer's focus justifiably seems to be on China. Yet no mention of President Trump and his blundering response to Chinese 'trade practices' which include all of the above? Slap major tariffs on *every*one, including our allies, in blind frustration? How about bringing the issue to the United Nations? Or getting our allies to address the problem *with* us against China even while, at least at the start, negotiating with China? A little late now, to be sure.

Let's also take a look at some of the damage we've been doing *to ourselves* even before the cyberworld came into focus: at the end of the cathode ray tube era for television sets, Zenith and Magnavox and all other major TV manufacturers were no longer able to make their own TV tubes: they had sold the licenses and outsourced production because, in the short run, it was cheaper. *But we lost manufacturing know-how and infrastructure in the process*. Same thing with the special photographic methods used in manufacturing computer chip circuits. We designed the F-1 rocket engine of 1.5 million pounds thrust to take us to the moon...and are now equipping our *Atlas* rocket launch vehicles with *Russian* engines. Go figure; 'profit motive' needs addressing.

Now consider dangerous rising tensions in the South China Sea and East China Sea as China expands its defense perimeter eastward and builds military bases atop artificially dredged islands piled atop reefs in areas *claimed by several different nations.* Meanwhile, the US provocatively

challenges, legally, this expansion by sailing two *Arleigh Burke*-class destroyers through the Taiwan Strait and makes bomber overflights close to Chinese claimed territorial limits. The UN stands by and does nothing about clarifying the International Law of the Sea regarding current territorial limits--3 mi.? 12 mi.? 200 mi.? Which is legally binding these days, and which is seen just as an 'economic interest zone'? Conflict could be triggered in the not too distant future in these areas...and *that*'s why China is on a breakneck pace trying to acquire the technologies to modernize and advance its military capabilities, especially in airpower. (They are already well supplied with superb Russian supersonic antiship missiles better than anything we have and may also have Russia's excellent wake-homing torpedo, not to mention its *Shkval*, the torpedo that can do more than 100 kts. with the aid of a supercavitating nose cone.)

But if that's going to be the focus, then at least a mention of China's alternate 'legal' means of getting our intellectual property/tech secrets ought to appear: through China's government-controlled corporations' (AVIC et al.) *requirement* that American corporations wishing to sell to the huge Chinese consumer base (whether Fiat/Chrysler vehicles or Boeing aircraft...and others) must first provide 'offset manufacturing opportunities' in forced 'Joint Venture' arrangements in which our corporations hand over key technologies and even help Chinese set up equivalent production facilities in those areas. **OR...you don't get the contract.** This has been going on for decades, and our *own corporate greed is a key contributing factor.*

And what they cannot then get this way, they try to obtain via cybertheft--hacking and cyber espionage. A Chinese national (government agent) was recently named for hacking into GE/Safran engine documents to obtain technology on their CFM *Leap* composite turbofan composition and molding methods, for example. Other specific examples could also have been included to demonstrate the advances the Chinese hope to get by plundering our design secrets: stolen data that led to their FC-31 stealth fighter that mimics the F-35; similar data used to shape the fuselage of their new F-20 long-range 'stealth' interceptor; design data that shaped their new Y-20 four-engine transport so that it resembles our C-17. *But they desperately need good jet engine data*: their best engines are still bought from Russia, and for their new commercial and military aircraft, they are desperate to acquire the background data and technology that will enable them to build their own world-class turbofans. They are not there yet and are trying to reverse engineer and steal that technology from wherever they can get it--from Russia (via reverse engineering) and the U.S. (via cybertheft--see above). Here is where our national security is *really* threatened.

I hope Name Withheld's essay generates many responses and potential specific steps that can be taken next. Department of Homeland Security is the depressing alternative.

Sincerely,

Lee Gaillard

Lee Gaillard served in the Marine Corps Reserves in the 1960s; worked in industry, publishing, and secondary education; and has written widely on aviation and defense issues. He is a contributor to the Center for Defense Information's Straus Military Reform Project and has written analyses of the F-35 Lightning II and MV-22 Osprey for COUNTERPUNCH and as a monograph for CDI. He has a BA from Yale and an MA from Middlebury College.