VULNERABILITY/CONNECTIVITY – Pt. 1

By Michael Ventura

August 8, 2014

Dark Angel premiered October 3, 2000. Created by James Cameron and Charles H. Eglee, the Fox series pilot opened with eerily crew-cut children in their jammies fleeing in the snow and getting shot. Cut to Jessica Alba on a motorcycle in a dilapidated Seattle with drones patrolling overhead.

Alba narrated: "They used to say one nuclear bomb can ruin your whole day. It was sort of a joke until the June morning when those terrorist bozos whacked us with an electromagnetic pulse from 80 miles up. You always hear people yapping about how it was all different before the Pulse – land of milk and honey, blah, blah, blah, blah – with plenty of food and jobs, and things actually worked. … Americans really thought they had it dialed in, money hanging out the butt. But it was all just a bunch of ones and zeros on a computer someplace. So when that bomb went klabooey, and the electromagnetic pulse turned all the ones and zeros into plain old zeros, everyone was like, 'No way!' America's just another broke ex-superpower looking for a hand-out and wondering why."

The writers compressed Alba's narration after the pilot: "Terrorists set off a nuclear device 80 miles up. The electromagnetic pulse fried every computer chip within a thousand miles. We went from superpower to Third World country overnight."

Google "electromagnetic pulse" and you'll find that *Dark Angel* wasn't kidding, and that the usual suspects developing electromagnetic pulse weapons that don't require nukes.

In 2000, *Dark Angel's* Pulse could merely cripple society, but now everything runs on chips. Cars, trucks, planes, trains, ships. Hospitals. Power grids. Water systems. Gas pumps. Appliances. Communications. Manufacturing. Retail. And just about everything military. Chips rule.

That's why U.S. counterintelligence "studies, with code names like *Dark Angel*," try to catch up to the stunning reality of society's vulnerability (*The New York Times,* April 28, 2009). The *Times* reporter thought "cyber war would not be as lethal as atomic war … nor as visibly dramatic." Oh yeah? If everything that needs a chip within 1,000 miles stopped dead at once?

A *U.S.News & World Report* headline, Jan. 28: "Fatal Inaction – The U.S. remains vulnerable to EMP [Electro Magnetic Pulse] attacks." John Holdern, "the Obama administration's current top science and technology adviser," predicted that, if cyber-attacked on a large scale, the U.S. would need "a recovery period of 4 to 10 years." (The idea of a recovery period is typical of this administration's chronic optimism.)

My point is not: "Oh my God, what shall we do?!"

This is what interests me: With eyes wide shut (my new favorite phrase), we have collectively created the most vulnerable society in history; we depend upon a hypersensitive technology for almost everything.

We were vulnerable to nuclear weapons, but that was sort of impersonal: You get whacked or you don't (you probably do). In contrast, EMPs would wreck society precisely on the personal level, but on a mass scale, leaving individuals just about helpless: a society based on connectivity but unable to connect – to practically anything.

It wouldn't be pretty. (Will you carry a hammer in your car if your chips fail, you can't get out, and can't phone?)

It's not just EMPs. What about "space weather"? "A once-in-a-century solar storm could cause the financial damage of 20 Hurricane Katrinas" (*The New York Times,* June 17, 2011). That number increases exponentially with every passing ultradigitalized year – and those storms do happen.

Then there's digital longevity. We save everything digitally, "but digital storage is perishable … Disks corrode, bits 'rot' and hardware becomes obsolete … and even if you could find the right drive [for obsolete devices], there's a good chance its magnetic properties will have decayed beyond readability" (*The New York Times,* August 7, 2011).

Maybe quantum and/or DNA computers will change that. But right now is right now, and this is where we are: in a state of fantastic vulnerability that is completely obvious and just as completely ignored – ignored, that is, except for the issue of privacy.

Thanks to Edward Snowden, we've confirmed our suspicions that everything digital is vulnerable to surveillance. "As the security expert Bruce Schneier wrote recently, it isn't that the Internet has been penetrated by the surveillance state; it's that the Internet, in effect, *is* a surveillance state" (*The New York Times,* June 9, 2013, italics in the original).

We're used to headlines like "Is your TV watching you? Latest models raise concerns" (NBCnews.com, March 19, 2012). Or these, from *The New York Times:* "Facebook Tinkers With Users' Emotions in News Feed Experiment" (June 29) and "Unblinking Eyes Track Employees" (July 9).

We take in stride things like: "Chinese hackers … broke into the computer networks of the United States government agency that houses the personal information of all federal employees … targeting the files on tens of thousands … who have applied for top-secret security clearances" (*The New York Times*, July 9).

And we love the so-called Cloud, where we're invited to store our data and our digital possessions, though we've no idea where a particular cloud may be, how it's monitored, who has access, and, "Where's the plug?"

But we do know it's not a cloud, right? It's an enormous warehouse packed with machines that require lots of air conditioning.

Isn't it interesting that our wondrous computers depend for their existence upon the lowly air conditioner? Air conditioners depend upon a digitally manipulated power grid. Power grids depend on generators propelled by gas, water, coal, nukes, wind, and even sun, plus jillions of digital circuits that in turn depend upon … you get the idea. Connectivity: vulnerability.

On the one hand, as a society, we buy the government's line about the need for constant war and believe its uncorroborated statements about terrorists, so obsessed with safety that the majority is happy to give up constitutional rights in safety's name.

On the other hand, we've chosen to be more vulnerable, with a more unsafe infrastructure, than any society in history – and the collective stance seems to be that it's not a choice, and all this just somehow happened because we delight in the convenience of our devices.

Sleepwalkers with eyes wide shut.

Americans like to ask, "What should we do about that?" It's a phony question. It exists merely so we may quickly come to the conclusion that we can do nothing. Then we change the channel.

Maybe it's a species thing.

Don't look now, but, as yet, we have no understanding of why we do what we do as a species, collectively, beyond the fragile boundaries of individuality.

Why, rather suddenly, is there this species-imperative to connect, connect, connect – not ideologically, but electronically? As a species, we lust so desperately to connect that we risk our very civilization on the gamble of circuitry. We don't care that it's desperate or that it's a gamble. We don't let that cross our so-called minds. We're excited beyond measure by a massive power of connection that can be held in one's hand. This very instrument I type on can connect to practically anything. We wipe the concurrent vulnerability from our consciousness, privately and collectively – the dangers are in plain sight, but invisible.

It's a helluva experiment. I wonder why we're doing it.

Anyway, here's to you and me, teetering on an edge that's paper-thin and as wide as the head of a pin.