Cybergeddon

Russia apparently has executed the most sophisticated and potentially most dangerous cyber-attack in history on the U.S. Government and private sector, penetrating the defenses of even the Cyber and Infrastructure Security Agency (CISA)—that is supposed to be the chief guardian against such threats to U.S. critical infrastructures.

For at least 9 months, cyber-spies roamed undetected through: the National Nuclear Security Administration (responsible for U.S. nuclear weapons); the Department of Energy and Federal Energy Regulatory Commission (responsible for protecting national electric grids); defense contractors designing the nation's most advanced weapons; and 18,000 other government and corporate victims.

Still unknown is the scale and depth of the damage.

We will be fortunate if the still continuing cyber-attack is "merely" an intelligence gathering operation, and not also a sabotage mission implanting logic-bombs, viruses, and cyber-bugs for future use.

Premature claims the cyber-attack is for spying, not sabotage, smells like making excuses to understate potential damage—and to escape acknowledging an act of war.

Washington does not know what to do.

As after past major cyber-attacks, Washington is full of sound and fury, promising reforms and retribution, that will probably come to nothing.

Washington's impotence and irresolution will invite future, increasingly aggressive, cyber-attacks.

Yet for decades Washington has been competently counseled on cyber-threats and solutions. 23 years ago, for example, the President's Commission on Critical Infrastructure Protection in their report "Critical Foundations: Protecting America's Infrastructures" (October 1997) warned:

"In the cyber dimension there are no boundaries. Our infrastructures are exposed to new vulnerabilities—cyber vulnerabilities—and new threats—cyber threats. And perhaps most difficult of all, the defenses that served us so well in the past offer little protection from the cyber threat. Our infrastructures can now be struck directly by a variety of malicious tools."

The Defense Science Board report "Resilient Military Systems and the Advanced Cyber Threat" (January 2013) warned: "While the manifestation of a nuclear and cyber attack are very different, in the end, the existential impact to the United States is the same."

Most dangerous, Washington is ignorant of the full magnitude of the cyber-threat, that has kinetic and nuclear dimensions. The Congressional EMP Commission warns:

"Combined-arms cyber warfare, as described in the military doctrines of Russia, China, North Korea, and Iran, may use combinations of cyber-, sabotage-, and ultimately nuclear EMP-attack to impair the United States quickly and decisively by blacking-out large portions of the electric

grid and other critical infrastructures…The synergism of such combined arms is described in the military doctrines of all these potential adversaries as the greatest revolution in military affairs in history—one which projects rendering obsolete many, if not all, traditional instruments of military power." ("Assessing the Threat from EMP Attack" July 2017)

Is it significant that the protracted 9-months attack on the U.S. in the cyber-domain preceded and coincides with Russia's major strategic forces exercise on December 9, wherein dictator Vladimir Putin personally oversaw live-launching ICBMs, SLBMs, and cruise missiles, simulating a nuclear war against the United States?

Is it significant that on December 15, Russia test-launched an anti-satellite missile, threatening assets critical to the U.S. military and economy in the domain of space?

Is it significant that Russia's VOSTOK 2018 massive military exercise, mobilizing 300,000 troops, 1,000 aircraft, and simulating a nuclear World War III, was preceded by cyber-attacks on hundreds of U.S. electric utilities?

Cyber-attacks by Russia, China, and North Korea are not only about stealing U.S. intellectual property and collecting intelligence on U.S. vulnerabilities, but also about testing U.S. responses. Most ominously—they are practicing a revolutionary new way of warfare coordinating all arms for cyber, space, and terrestrial blitzkrieg.

Washington seems incapable of connecting the dots, unlike Lt. Colonel (ret.) Bob Lindseth, former Deputy Director for Intelligence on the Joint Chiefs of Staff and Professor of Information Operations at National Intelligence University:

"In today's world a nuclear conflict will be preceded by Cyber operations in every form." (December 18, 2020)

Unlike Admiral (ret.) William Studeman, former Acting Director CIA:

"I see little discussion anywhere of threats which integrate cyber and nuclear (all kinds including EMP) in both the offensive and defense…All these experts seem to stay in their 'vertical/stove-piped' fields of expertise and thinking. I think that Cyber/Information Operations and nuclear integrated threats/vulnerabilities considered together need more and new thinking." (December 17, 2020)

What is to be done?

Washington's favorite solution—a global treaty on cyberwarfare—will NOT work, despite advocacy by such enthusiasts as Microsoft's President Brad Smith: "We need a set of binding rules. And we need a commitment by the democracies to hold authoritarian regimes accountable, so they keep their hands off of civilians in this time of peace when it comes to cyberspace." (December 15, 2020)

Authoritarian regimes will sign anything and cheat on everything.

We need real technical experts on cyber and EMP in charge of protecting the nation.

Chris Krebs, Director of CISA until recently fired, a lawyer and former lobbyist for Microsoft, with no deep technical expertise on cyber or EMP, is the poster child for failure.

Washington needs to read, heed, and rapidly implement the recommendations of its expert commissions and boards.

Dr. Peter Vincent Pry is Executive Director of the Task Force on National and Homeland Security, served as Chief of Staff of the Congressional EMP Commission, and on the staffs of the House Armed Services Committee and the CIA. He has authored numerous books and articles on EMP and Cyber Warfare.

https://www.newsmax.com/peterpry/cyberattacks-nuclear-exercises-cisa/2020/12/21/id/1002586/