

Obama Declares Global Cyberwar

By [Stephen Lendman](#)

Global Research, February 06, 2013

Theme: [Police State & Civil Rights](#), [US NATO War Agenda](#)

Throughout his tenure, Obama governed lawlessly for the monied interests that own him. He's waged no-holds-barred war on humanity.

Strategy includes homeland tyranny, fear-mongering, saber rattling, hot wars, proxy ones, drone ones, domestic political ones, geopolitical ones, financial ones, anti-populist ones, sanctions, subversion, sabotage, targeted assassinations, mass murder, cyberwar, and more.

In May 2009, [Obama](#) prioritized cybersecurity. He called cyber-threats "one of the most serious economic and national security challenges we face as a nation."

"America's economic prosperity in the 21st century will depend on cybersecurity."

He ordered a top-to-bottom review. A Cyberspace Policy Review report followed. He waged cyberwar on Iran. He did so cooperatively with Israel.

In spring 2010, Iranian intelligence discovered Stuxnet malware contamination. The computer virus infected its Bushehr nuclear facility. At the time, operations were halted indefinitely.

Israel was blamed. Washington was involved. Had the facility gone online infected, Iran's entire electrical power grid could have been shut down.

A more destructive virus called Flame malware is known. Internet security experts say it's 20 times more harmful than Stuxnet. Iran's military-industrial complex is targeted. So is its nuclear program. Maximum disruption is planned.

Obama supports draconian cybersecurity bills. Passage threatens constitutional freedoms.

Targeted assassinations eliminate America's enemies. Lawless domestic spying is policy. So is warrantless wiretapping. Americans are as vulnerable as others.

Obama's waging war on humanity. He's doing it multiple ways. Last October, he signed an executive order. It expanded military authority. It authorized cyberattacks. It redefined defense. Doing so lawlessly legitimizes aggression.

In November, Presidential Policy Directive 20 followed. It's secret. It set guidelines for confronting cyberspace threats.

Last fall, Defense Secretary Leon Panetta warned of a "cyber Pearl Harbor." It could "cause physical destruction and loss of life," he said. It could "paralyze and shock the nation and create a new profound sense of vulnerability."

US officials never lack for hyperbole. Fear-mongering is longstanding policy. So are Big Lies, false flags, and other pretexts for wars, other military actions, and disruptive ones.

Cyberwar capability adds to America's arsenal. Preemption adds another dirty tactic.

In early February, US media reports headlined stepped-up cyberwar. Preemption is prioritized. Nation states, organizations, and individuals are fair game.

US Cyber Command (USCYBERCOM) has full operational control. It's a cyber hit squad. It's part of the US Strategic Command.

It's based at Fort Meade, MD. General Keith Alexander serves as National Security Agency (NSA) director and US Cyber Command head.

The [New York Times](#) cited a secret legal review. It affords Obama sweeping preemptive cyberattack powers.

It permits him "to order a preemptive strike if the United States detects (allegedly) credible evidence of a major digital attack looming from abroad."

His word alone is policy. Corroborating evidence isn't needed. Efforts to protect classified and proprietary information are increasing.

The [Washington Post](#) said wireless and technology giants are battling over a plan to create super Wi-Fi networks.

The [Wall Street Journal](#) said Google, Microsoft and Amazon are competing to control cloud computing business.

The [Christian Science Monitor](#) said preemptive cyberwar entered America's arsenal. It "nudged up along side other" approved tactics and techniques.

New policies govern how intelligence agencies work. They've been unrestrained before. They'll have greater powers now.

The New York Times said they'll be able to "carry out searches of faraway computer networks for signs of potential attacks on the United States and, if the president approves, attack adversaries by injecting them with destructive code - even if there is no declared war."

Rules of engagement are classified. Effectively there are none. Cyber-warriors are freewheeling. They're unrestrained.

They'll operate anywhere globally. China is a target of choice. It's America's main economic and geopolitical competitor.

An unnamed US official said new cyberwar strategy is "far more aggressive than anything" used or recommended before. The gloves are off. Anything goes.

Major disruptions can occur without firing a shot. Military and/or civilian power grids can be crippled. So can financial systems and communications networks.

Another unnamed US official said cyberweapons are so powerful that “they should be unleashed only by” presidential order. Exceptions would be tactical strikes.

Examples include disabling command and control as well as ground radar ahead of conventional strikes. At the same time, most cyberoperations are presidential prerogatives.

Expect Obama to take full advantage. Extrajudicial operations are prioritized. Rule of law principles are spurned. Operational procedures have been in development for over two years.

They’re headlined now. They coming out when cyberattacks more often target US companies and critical infrastructure. An unnamed US power station was crippled for weeks.

The New York Times, Washington Post, and Wall Street Journal reported cyberattacks. Obama prioritizes preemption. Doing so has no legal standing. Self-defense alone is justified. Acting on suspicions without evidence is aggression.

New rules serve Washington. Lawyers get marching orders. They’re well paid to subvert accepted legal standards. Doing so doesn’t change them.

What constitutes “reasonable and proportionate force” resides in the eye of the aggressor. New guidelines exclude the Pentagon from defending US companies or individuals without presidential authority.

Doing so is Homeland Security’s prerogative. The FBI has investigatory authority. Cybersecurity legislation remains stalled in Congress. Expect stepped up efforts for passage.

Doing so will more greatly comprise freedom. Full-blown tyranny approaches. It’s a hair’s breadth away. Whistleblowers are targeted. Dissent is endangered.

There’s no place to hide. Big Brother’s expanding exponentially. Cyber-preemption adds greater police state power.

On February 3, a [Washington Post](#) editorial headlined “Cyberwar, out of the shadows,” saying:

US Cyber Command is expanding exponentially. Doing so “is indicative of how conflict is moving toward center stage for the military, a domain similar to land, sea, air and outer space.”

It’s heading America toward unchallenged dominance.

In May 2000, the Pentagon’s Joint Vision 2020 called for “full spectrum dominance” over all land, surface and sub-surface sea, air, space, electromagnetic spectrum and information systems with enough overwhelming power to fight and win global wars against any adversary.

Doing so includes nuclear weapons use preemptively. Non-nuclear countries and adversaries are fair game.

Cyber Command includes:

(1) “Combat mission forces” cooperatively with military units.

(2) "Protection forces" to defend Pentagon networks.

(3) "National mission forces" to head off threats to critical infrastructure. They'll operate outside America. They'll function anywhere if authorized. They'll strike US adversaries preemptively.

Targeting cuts both ways. Incoming attacks can precede or follow US ones. Secrecy is prioritized but compromised. Spies have clever ways of doing it.

Rules of engagement aren't clear. Public information is limited. Sunlight is the best disinfectant. Policy need generous doses.

"If conflict in cyberspace is underway," said the Post, "then it is important to sustain support for the resources and decisions to fight it, and that will require more candor."

Expect little forthcoming from the most secretive administration in US history. Obama's first term prioritized homeland repression and lawless aggression. Imagine what he has in mind for term two.

Stephen Lendman lives in Chicago and can be reached at lendmanstephen@sbcglobal.net.

His new book is titled "Banker Occupation: Waging Financial War on Humanity."

<http://www.claritypress.com/LendmanII.html>

Visit his blog site at sjlendman.blogspot.com and listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network Thursdays at 10AM US Central time and Saturdays and Sundays at noon. All programs are archived for easy listening.

<http://www.progressiveradionetwork.com/the-progressive-news-hour>

<http://www.dailycensored.com/obama-declares-global-cyberwar/>

The original source of this article is Global Research
Copyright © [Stephen Lendman](#), Global Research, 2013

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: **[Stephen Lendman](#)**

About the author:

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net. His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III."

<http://www.claritypress.com/LendmanIII.html> Visit his blog site at sjlendman.blogspot.com. Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network. It airs three times weekly: live on Sundays at 1PM Central time plus two prerecorded archived programs.

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca