Pentagon: Cyberattack an Act of War

Following up on the publication of the "International Strategy for Cyberspace" by the Obama administration last month, the Pentagon clarified and expanded upon its intention to consider a computer attack as equivalent to a more traditional act of war. The White House's strategy made clear that:

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country … We reserve the right to use all necessary means — diplomatic, informational, *military*, and economic … in order to defend our Nation. … [Emphasis added.]

The Pentagon is proceeding to define what constitutes an attack or an act of aggression sufficient to provoke a military response. According to the *New York Times*, "[A]ny computer attack that threatens widespread civilian casualties — for example, by cutting off power supplies or bringing down hospitals and emergency-responder networks — could be considered an act of aggression." What's missing from the Pentagon's attempts to clarify is what sort of threshold or level of attack would merit or justify a military response. And it was clear, by default, that the Pentagon *would determine that on a case-by-case basis*, whether the threat is from a "terrorist" group or a single computer operator, no matter where they, or it, might be located.

The Pentagon also failed to indicate what sort of military response would be undertaken, given that the source of most attacks is notoriously difficult to find. Last fall, when Google's servers were attacked, the Pentagon never clearly determined the source, and only later did Google conclude that the attack came from China. This leaves enormous discretion in the hands of the military. One former Pentagon official observed, "One of the questions we have to ask is, 'How do we know we're at war?' How do we know when it's [just] a hacker and when it's the [Chinese] People's Liberation Army?"

The cyber strategy being promoted by the White House includes "neutralizing cyberattacks in the making," along with "other forms of deterrence, including threatening a country's well-being. …"

Recognizing that cyberattacks could emanate from within the United States, the Department of Defense announced that it is "working hand in hand" with the Department of Homeland Security. Under the agreement, personnel from both departments will be sharing information. In simple terms, with the evisceration of the Fourth Amendment primarily through the Patriot Act, individual citizens' security, safety, and privacy will now be invaded at will by the military services as well as by Homeland Security agents. All of this is being done to protect the government's information network, which includes some 15,000 military networks. Chillingly, Kristin Lord, coeditor of a report just published by the Center for a New American Security, noted that cyberattacks on those military networks "could disable critical equipment and even turn it against its users."

Not wasting any time, the Department of Homeland Security is now requiring energy companies, water suppliers, and financial institutions to rank the most serious threats to their computer infrastructure,

and then to find ways to counter them. Each business is now required to have an independent commercial auditor assess its plans and then report the results to the DHS.

All that is needed, now, is for a "cyber event" to unleash these agencies to work their will. George Washington (a *nom de plume*), writing for ZeroHedge.com, suggests that such an event could be a "false flag" effort to accelerate and expand the powers granted to the two departments. Quoting U.S. President James Madison, "If Tyranny and Oppression come to this land, it will be in the guise of fighting a foreign enemy," Washington then proceeded to note several highly suspect events in the past that were used to expand government power and accelerate military adventurism:

> • The U. S. Navy's own historians now say that the sinking of the *USS Maine* — the justification for America's entry into the Spanish-American War — was probably caused by an internal explosion … rather than [an] attack by the Spanish.
>
> • The Gulf of Tonkin Incident which led to the Vietnam War was a fiction.
>
> • Two lies were used to justify the 1991 Gulf War.
>
> • In a newly-released documentary, U.S. soldiers admit that if they accidentally kill innocent Iraqis or Afghanis, they [have been ordered to] "drop " automatic weapons near their bodies so they can pretend they were militants.
>
> • Former Chairman of the Joint Chiefs of Staff General Hugh Shelton told Jon Stewart that a Clinton cabinet member proposed letting Saddam kill an American pilot as a pretext for war in Iraq.
>
> • Former Justice Department lawyer John Yoo suggested creating a false terrorist organization as a tool in fighting terrorism, "with its own websites, recruitment centers, training camps and fundraising efforts. It could launch fake terrorist operations and claim credit for real terrorist strikes. …"
>
> • Craig Murray, former British Ambassador to Uzbekistan, wrote in October of 2006, "The evidence that the US directly contributed to the creation of the current civil war in Iraq by its own secretive security strategy is compelling."

The recent cyberattack on the International Monetary Fund (IMF) has led some to consider this as possibly another false-flag operation, designed to create the impetus for the international regulation of the Internet. FoxNews.com noted that "cyber security experts say the only way to effectively combat the menace is for the public and private sectors to join forces and combine greater regulation with international action." Alexander Klimburg, a cyber-security specialist at the Austrian Institute for International Affairs, saw the IMF attack as a way to force international cooperation: "This is potentially a great opportunity to launch a 'communal' investigation into an attack on a 'communal' institution."

Whether the cyberattack on the IMF was another false-flag operation to generate additional momentum for "international cooperation" in regulating the Internet remains to be seen. As Anthony Wile noted:

> If a false flag cyber attack was to be created and, say, attributed to Iran, then the US President might be under an affirmative obligation to declare war against Iran. No doubt, US powers-that-be could also justify a significant takeover of the American Internet and further reduce American civil rights.
>
> These sorts of things have happened before. It is neither incendiary nor unpatriotic to recite them. … Western elites are evidently and obviously at war [not with terrorists but] with their own

citizens.

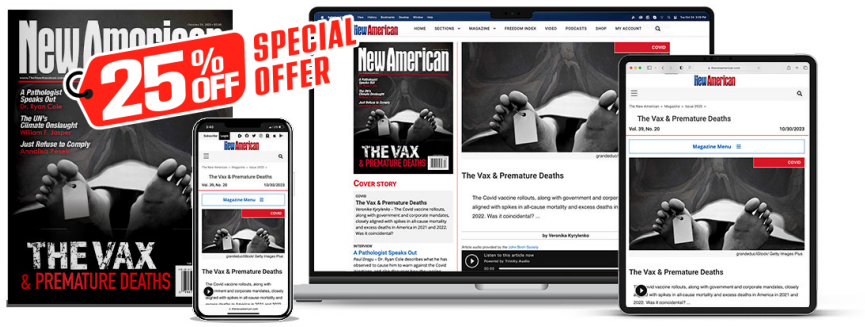
Even if the attack on the IMF's computers were a solitary and unrelated event, is it not reasonable to anticipate other false-flag events that could be used to push for more "international cooperation" resulting in further erosion of American citizens' freedoms, including use of the Internet?

Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture,
and technology, we bring you an unparalleled array of topics that matter most.



What's Included?

24 Issues Per Year
Optional Print Edition
Digital Edition Access
Exclusive Subscriber Content
Audio provided for all articles
Unlimited access to past issues
Coming Soon! Ad FREE
60-Day money back guarantee!
Cancel anytime.

Subscribe