source: Wall Street Journal

Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force

The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force.

The Pentagon's first formal cyber strategy, unclassified portions of which are expected to become public next month, represents an early attempt to grapple with a changing world in which a hacker could pose as significant a threat to U.S. nuclear reactors, subways or pipelines as a hostile country's military.

In part, the Pentagon intends its plan as a warning to potential adversaries of the consequences of attacking the U.S. in this way. "If you shut down our power grid, maybe we will put a missile down one of your smokestacks," said a military official.

Recent attacks on the Pentagon's own systems—as well as the sabotaging of Iran's nuclear program via the Stuxnet computer worm—have given new urgency to U.S. efforts to develop a more formalized approach to cyber attacks. A key moment occurred in 2008, when at least one U.S. military computer system was penetrated. This weekend Lockheed Martin, a major military contractor, acknowledged that it had been the victim of an infiltration, while playing down its impact.

The report will also spark a debate over a range of sensitive issues the Pentagon left unaddressed, including whether the U.S. can ever be certain about an attack's origin, and how to define when computer sabotage is serious enough to constitute an act of war. These questions have already been a topic of dispute within the military.

One idea gaining momentum at the Pentagon is the notion of "equivalence." If a cyber attack produces the death, damage, destruction or high-level disruption that a traditional military attack would cause, then it would be a candidate for a "use of force" consideration, which could merit retaliation.

The Pentagon's document runs about 30 pages in its classified version and 12 pages in the unclassified one. It concludes that the Laws of Armed Conflict—derived from various treaties and customs that, over the years, have come to guide the conduct of war and proportionality of response—apply in cyberspace as in traditional warfare, according to three defense officials who have read the document. The document goes on to describe the Defense Department's dependence on information technology and why it must forge partnerships with other nations and private industry to protect infrastructure. The strategy will also state the importance of synchronizing U.S. cyber-war doctrine with that of its allies, and will set out principles for new security policies. The North Atlantic Treaty Organization took an initial step last year when it decided that, in the event of a cyber attack on an ally, it would convene a group to "consult together" on the attacks, but they wouldn't be required to help each other respond. The group hasn't yet met to confer on a cyber incident. P
entagon officials believe the most-sophisticated computer attacks require the resources of a government. For instance, the weapons used in a major technological assault, such as taking down a power grid, would likely have been developed with state support, Pentagon officials say.

The move to formalize the Pentagon's thinking was borne of the military's realization the U.S. has been slow to build up defenses against these kinds of attacks, even as civilian and military infrastructure has grown more dependent on the Internet. The military established a new command last year, headed by the director of the National Security Agency, to consolidate military network security and attack efforts.

The Pentagon itself was rattled by the 2008 attack, a breach significant enough that the Chairman of the Joint Chiefs briefed then-President George W. Bush. At the time, Pentagon officials said they believed the attack originated in Russia, although didn't say whether they believed the attacks were connected to the government. Russia has denied involvement.

The Rules of Armed Conflict that guide traditional wars are derived from a series of international treaties, such as the Geneva Conventions, as well as practices that the U.S. and other nations consider customary international law. But cyber warfare isn't covered by existing treaties. So military officials say they want to seek a consensus among allies about how to proceed.

"Act of war" is a political phrase, not a legal term, said Charles Dunlap, a retired Air Force Major General and professor at Duke University law school. Gen. Dunlap argues cyber attacks that have a violent effect are the legal equivalent of armed attacks, or what the military calls a "use of force."

"A cyber attack is governed by basically the same rules as any other kind of attack if the effects of it are essentially the same," Gen. Dunlap said Monday. The U.S. would need to show that the cyber weapon used had an effect that was the equivalent of a conventional attack.

James Lewis, a computer-security specialist at the Center for Strategic and International Studies who has advised the Obama administration, said Pentagon officials are currently figuring out what kind of cyber attack would constitute a use of force. Many military planners believe the trigger for retaliation should be the amount of damage—actual or attempted—caused by the attack.

For instance, if computer sabotage shut down as much commerce as would a naval blockade, it could be considered an act of war that justifies retaliation, Mr. Lewis said. Gauges would include "death, damage, destruction or a high level of disruption" he said.

Culpability, military planners argue in internal Pentagon debates, depends on the degree to which the attack, or the weapons themselves, can be linked to a foreign government. That's a tricky prospect at the best of times.

The brief 2008 war between Russia and Georgia included a cyber attack that disrupted the websites of Georgian government agencies and financial institutions. The damage wasn't permanent but did disrupt communication early in the war.

A subsequent NATO study said it was too hard to apply the laws of armed conflict to that cyber attack because both the perpetrator and impact were unclear. At the time, Georgia blamed its neighbor, Russia, which denied any involvement.

Much also remains unknown about one of the best-known cyber weapons, the Stuxnet computer virus that sabotaged some of Iran's nuclear centrifuges. While some experts suspect it was an Israeli attack, because of coding characteristics, possibly with American assistance, that hasn't been proven. Iran was the location of only 60% of the infections, according to a study by the computer security firm Symantec. Other locations included Indonesia, India, Pakistan and the U.S.

Officials from Israel and the U.S. have declined to comment on the allegations.

Defense officials refuse to discuss potential cyber adversaries, although military and intelligence officials say they have identified previous attacks originating in Russia and China. A 2009 government-sponsored report from the U.S.-China Economic and Security Review Commission said that China's People's Liberation Army has its own computer warriors, the equivalent of the American National Security Agency.

That's why military planners believe the best way to deter major attacks is to hold countries that build cyber weapons responsible for their use. A parallel, outside experts say, is the George W. Bush administration's policy of holding foreign governments accountable for harboring terrorist organizations, a policy that led to the U.S. military campaign to oust the Taliban from power in

Afghanistan.