Written by **Joe Wolverton, II, J.D.** on June 22, 2012

The Pentagon Is Developing Cyber Weapons That Launch Without Human Intervention

The United States government is developing a computer system that would allow it to conduct cyber warfare without the intervention of a human programmer.

Recently, stories have leaked detailing the U.S. government's creation and implementation of two cyber attacks on the information systems of other nations.

"Flame" was the name of a computer virus reportedly developed and launched by the United States in order to glean critical data from computers in several Middle Eastern countries.

According to a story published in the *Washington Post*, the United States and Israel launched a joint venture to develop the Flame virus. Once launched into cyber space, the code reportedly collected online intelligence data that was then used to create a similar bit of malware that would cripple Iran's nuclear capabilities. Officials cited in the *Post* article revealed that the effort was a collaboration of the National Security Agency (NSA), the CIA, and the Israeli military.

One product of that Israeli-American secret enterprise was the Stuxnet virus. Stuxnet was the virus allegedly deployed by the United States to decelerate Iran's progress toward the development of a nuclear weapon.

Apparently, Flame and Stuxnet were just the beginning of a more sophisticated and sustained American cyber assault against the Iranian nuclear infrastructure. As one source quoted by the *Washington Post* reports: "This is about preparing the battlefield for another type of covert action," said one former high-ranking U.S. intelligence official, who added that Flame and Stuxnet were elements of a broader assault that continues today. "Cyber-collection against the Iranian program is way further down the road than this."

There is substantial evidence that this unnamed intelligence official knew what he was talking about.

Soon after the existence of Flame and Stuxnet was uncovered (some say leaked by the Obama administration itself), the *Post* ran a story claiming that the ultra-secret Defense Advanced Research Projects Agency (DARPA) was preparing to test "unmanned cyber attacks" that launch themselves without the need of a human at the controls.

Last month, Ellen Nakashima wrote an article about a just such a program being carried out by DARPA. According to Nakashima, the project is codenamed Plan X, and its goal is to "develop systems that could give commanders the ability to carry out speed-of-light attacks and counterattacks using preplanned scenarios that do not involve human operators manually typing in code — a process considered much too slow."

Yes, the need for a human being to launch these cyber attacks is seen by the government as an

unnecessary speed bump, much the same way they see the Fourth Amendment's requirement that a warrant be obtained before anyone is searched or anything is seized as a result of that search.

One former member of the Air Force Judge Advocate General Corps sees the Pentagon's creation of these weapons as the first step toward the deployment of an autonomous weapon that not only launches without human direction, but can choose its own targets, as well.

"News reports that DARPA is seeking proposals for methodologies that would automate cyber responses in predetermined scenarios is an almost inevitable development given the speed in which cyberattacks can cause harm," said Charles Dunlap, now a Duke University Law School professor. "The very idea of autonomous weapons systems of any kind, cyber or kinetic, is controversial on legal, ethical and even pragmatic warfighting grounds. Yet the development and deployment of such weaponry is sure to continue even as we sort out the law and policies to address it."

For its part, the Department of Defense responds that any operations conducted by the government in cyber space will be used solely for the protection of our national security. Of course, the United States does not control the Internet, despite its best efforts. Within the worldwide web of interconnected computers, there are many who would and could develop and deploy many of the same cyber weapons against the United States. The Pentagon knows this, as well, and is apparently taking steps to prevent it.

One such defensive measure is the National Cyber Range being created by DARPA. The Strategic Technology Office at DARPA reports the following progress and purposes of these efforts on its website:

> Replicating the complexity of thousands of globally interconnected network systems is a challenge faced by researchers developing tools to protect our nation against the growing threat of cyber attacks. Sophisticated attacks as well as adaptive malware have the ability to devastate defense and commercial networks. DARPA was tasked by the Comprehensive National Cybersecurity Initiative (CNCI) to "establish a front line of defense against today's immediate threats by creating or enhancing … the ability to act quickly to reduce our current vulnerabilities and prevent intrusions" (National Security Presidential Directive 54 (NSPD)-54).

It would seem that the more we live by the cyber sword the more likely it becomes that we will eventually die by it — or at least be seriously wounded. There are those working in the shadowy world of Internet security and cyber warfare who recognize the substantial danger posed by these digital weapons to the stability of our own online infrastructure.

Dave Aitel, president of Immunity, Inc., a cyber security company, is a former NSA computer scientist and he believes that Flame and Stuxnet utilized certain "techniques that could have been used against us just as effectively."

In a statement by Aitel quoted at Nextgov, the order to deploy Flame and Stuxnet was given by President Obama himself. "Obama has to say, yes or no," he said.

Naturally, the Pentagon is ready to launch these cyber weapons at a moment's notice. "If so directed, [the Department of Defense] is prepared to defend U.S. national security interests through all available means," Defense spokeswoman Lt. Col. April Cunningham said. "[The Department of Defense] is committed to protecting the individual privacy of communications on the Internet and the civil liberties of the American people," she told Nextgov.

There is nothing unconstitutional or immoral about the active protection of American cyber security

from attack. It can be rightly said that such actions represent a 21st-century application of national security that is in complete harmony with the enumerated powers of the federal government as set forth in the Constitution. The problem that arises, however, is when these shields are hammered into swords and used to attack and disable the Internet infrastructure of other nations. That sort of preemptive attack has no constitutional or moral basis.

Besides, there is the frightening scenario described above by Aitel. What will the United States do if a nation decides unilaterally that its own national security is threatened by America's possession of so many nuclear weapons and decides to dismantle the computer systems that control those missiles? On what moral ground will the United States stand in defense of such attacks?

What's more, just as there is collateral damage in traditional warfare, it seems only logical that there would be some such analogous harm that occurs as the result of cyber attacks.

Nextgov reports just such an incident associated with the development of the Flame virus:

> Still, Microsoft suffered some collateral damage from Flame. The designers of the virus exploited a previously unknown flaw in the company's digital certificates to disguise malicious code as a Microsoft product. The software firm subsequently issued an update to block other hackers from abusing the fraudulent certificates.
>
> Kaspersky Labs, the security firm that discovered Flame, describes the bug as "the largest cyberweapon to date," referring to its 20 megabytes. The tool can scoop up massive amounts of valuable information such as screenshots of online chats, audio recordings from internal microphones, and storage files.

Is it too incredible to believe that our own government would secretly launch these viruses on its own citizens? As the size, scope, and resources of the surveillance state continue increasing, it seems possible if not probable that the federal government would be willing to use the technology it is developing to expand the view open to its ever-prying eye. And the most worrisome aspect of all this is that most of the snooping is done without warrants in direct violation of the Fourth Amendment to the Constitution.

Some disagree.

General Harry D. Raduege, a former director of the Defense Information Systems Agency, insists, "All new cyberweapons must adhere to all the U.S. federal laws."

As true as General Raduege's statement might be in theory, no one can argue that the law (including the Constitution) is repeatedly and routinely ignored by the federal government in its quest to track, target, and eliminate those it considers enemies of the state or potential threats to our national security.