Carpet bombing in cyberspace
Why America needs a military botnet
BY COL. CHARLES W. WILLIAMSON III

The world has abandoned a fortress mentality in the real world, and we need to move beyond it in cyberspace. America needs a network that can project power by building an af.mil robot network (botnet) that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic. America needs the ability to carpet bomb in cyberspace to create the deterrent we lack.

America faces increasingly sophisticated threats against its military and civilian cyberspace. At the same time, America has no credible deterrent, and our adversaries prove it every day by attacking everywhere. Worse, our defensive concept is fundamentally flawed, and we have not learned the simplest lessons of history.

As much as some think the information age is revolutionary, local networks and the Internet are conceptually similar to the ancient model of roads and towns: Things are produced in one place and moved to another place where they have more value. The road-and-town model works well between cooperating states, but states also compete, and when they do, they sometimes have to defend themselves from attack. In today's Internet, network "towns" are "fortified" with firewalls, gateways, passwords, port blocking, intrusion detection devices and law enforcement. This approach uses the same strategy as the medieval castle with its walls, moat, drawbridge, guards, alarms and a sheriff. While castles worked more or less for hundreds of years, they are now abandoned as completely ineffective except against the most anemic attack.

The time for fortresses on the Internet also has passed, even though America has not recognized it. Now, the only consequence for an adversary who intrudes into or attacks our networks is to get kicked out — if we can find him and if he has not installed a hidden back door. That is not enough. America must have a powerful, flexible deterrent that can reach far outside our fortresses and strike the enemy while he is still on the move.

Homer's epic poems describe how fortified Troy held out against the united Greek armies for 10 years until Troy finally fell when it foolishly brought the threat inside its own walls by falling for the enemy's masquerade in the form of a giant wooden horse. Today, it is no coincidence that the Trojan horse exploit uses the same technique on the Internet by hiding a threat inside what appears to be a gift.

In spite of Troy's defeat, fortresses worked for thousands of years because they were so reliable and cheap compared to standing armies. Fortresses reached their zenith in the medieval castle, even though they were vulnerable to siege, tunneling and the threat that someone would open the gate from inside. However, the popularity of castles declined as the power of artillery increased. While fortresses enjoyed some notable successes, even the post-Civil War settlement of the American West evolved to relying on quickly constructed fortresses with wooden walls to house a highly mobile attack force that could secure a vast area.

The death knell for the fortress came during World War II at the Belgian Fort Eben-Emael. Its answer to the artillery threat was thicker and higher walls and the threat of its own artillery against any enemy in the vicinity of the fort, especially at the nearby bridge. But the attack did not come across the bridge. It came from the air. The Germans cunningly dropped storm troopers in gliders right in the middle of the fort, engaged the garrison and tied it up long enough for the massive German Army swarming across the bridge to compel surrender, which came in just one day.

Today, every Army outpost in America traces its roots to the walls, guards and gates of Troy. But none of today's forts relies for boundary defense on anything more substantial than a chain-link fence, even though the base may contain billions of dollars in military equipment and the things most important to the soldiers — their families. The U.S. intends for defense of its "forts" to occur thousands of miles away. We intend to take the fight to the enemy before the enemy has a chance to come here. So, if the fortress ultimately failed, does history provide a different model?

AIR BASE DEFENSE

Almost from the beginning, air base defenders recognized the need to defend in close, coupled with the necessity of finding the enemy and destroying his planes on the ground before they launch.

In "Air Warfare and Air Base Air Defense," John F. Kreis described the early defense of the air weapon. From the beginning of World War I, defense happened when the enemy was above your airfield, with expediencies such as Lewis machine guns mounted on stumps in the ground. However, by 1915, British Maj. Gen. Hugh Trenchard's large, repeated raids on German airfields put the Germans on the defensive. Today's air base defense concept still uses a layered defense in depth, but it starts as far as possible from the air bases, then relies on close-in defense only as a last resort. That capability in cyberspace can exist in an af.mil botnet.

A botnet is a collection of widely distributed computers controlled from one or more points. Criminals build botnets by using automated processes to break through the defenses of computers anywhere in the world and implant their programs or code. Often, the computer user is tricked through a crafty e-mail into cooperating with the installation of the code. The infected machines are called zombies and can be remotely controlled by masters. Hackers can build multiple levels of masters and zombies with millions of computers.

Hackers often use botnets to generate spam, but their real strength lies in their ability to generate massive amounts of Internet traffic and direct it against a small number of targets. This is called a distributed denial of service (DDOS) attack. The effect is that the target computers are cut off from the Internet. Because communication is often a computer's main purpose, a compromised computer might as well be a rock. While preparation and money can help target computers defend themselves, once under attack, they have little ability to recover.

Multiday attacks against CNN and Yahoo in 2000 and against Estonia in 2007 cost tens of millions of dollars. The SANS Institute projects that increasingly sophisticated botnets will be the No. 2 cyber security menace for 2008. A DDOS attack against a net-centric military could stop or delay any operation it intended. How could the U.S. military build such a system?

BUILDING THE AF.MIL BOTNET

The U.S. would not, and need not, infect unwitting computers as zombies. We can build enough power over time from our own resources.

Rob Kaufman, of the Air Force Information Operations Center, suggests mounting botnet code on the Air Force's high-speed intrusion-detection systems. Defensively, that allows a quick response by directly linking our counterattack to the system that detects an incoming attack. The systems also have enough processing speed and communication capacity to handle large amounts of traffic.

Next, in what is truly the most inventive part of this concept, Lt. Chris Tollinger of the Air Force Intelligence, Surveillance and Reconnaissance Agency envisions continually capturing the thousands of computers the Air Force would normally discard every year for technology refresh, removing the power-hungry and heat-inducing hard drives, replacing them with low-power flash drives, then installing them in any available space every Air Force base can find. Even though those computers may no longer be sufficiently powerful to work for our people, individual machines need not be cutting-edge because the network as a whole can create massive power.

After that, the Air Force could add botnet code to all its desktop computers attached to the Nonsecret Internet Protocol Network (NIPRNet). Once the system reaches a level of maturity, it can add other .mil computers, then .gov machines.

To generate the right amount of power for offense, all the available computers must be under the control of a single commander, even if he provides the capability for multiple theaters. While it cannot be segmented like an orange for individual theater commanders, it can certainly be placed under their tactical control.

For computer network attack intended to create effects for a theater commander, the most sensible person to exercise tactical control is the Joint Force Air Component Commander (JFACC). The JFACC is responsible for the theater's deep-strike capability and habitually operates in parallel warfare with hundreds of simultaneous strikes on hundreds of locations. That is exactly the kind of capability provided by the af.mil botnet. Also, the JFACC has the most at stake in using the botnet for deterrence, limited strike or massive strike because it is the JFACC who will have to send in his joint airmen if the botnet fails. This means he will have the most incentive to compel the Air Force to build and exercise this tool for him.

Computer network defense presents a different problem. Here, the botnet needs to be under the tactical control of a combatant commander with global responsibility. The enemy is almost certain to attack from every quarter and will completely ignore or actively exploit our seams between regions. Cutting up the botnet into regional pieces would so dilute its power that it would be worthless and make rapid employment functionally impossible.

The system also needs to avoid tampering and fratricide. Cannoneers of fuse-fired artillery carried spikes which they could quickly drive in the fuse hole to prevent the weapon from being turned on friendly forces if their position was overrun. The af.mil botnet could replicate that protection with various mechanisms, including disabling the botnet code if an automated check

indicated the code has been altered. The af.mil botnet could protect against fratricide by having filters to prevent attacks against .mil, .gov or registered allied addresses, unless specifically overridden.

PARADE OF HORRIBLES

Lawyers have been known to trot out a “parade of horribles” to demonstrate weaknesses in an idea. These issues are difficult but not insurmountable. But before addressing them, it is important to note what the botnet is not.

The af.mil botnet is not a replacement for law enforcement action or diplomacy. If the harm coming to U.S. systems is low enough that a military response is not required, the U.S. must default to traditional responses that respect the sovereignty of other nations, just as we expect them to respect our sovereignty and the primacy of our responsibility to stop harm coming to them from the U.S. With that understanding, what challenges remain?

Some people would fear the possibiltiy of botnet attcks on innocent parties. If the botnet is used in a strictly offensive manner, civilian computers may be attacked, but only if the enemy compels us. The U.S. will perform the same target preparation as for traditional targets and respect the law of armed conflict as Defense Department policy requires by analyzing necessity, proportionality and distinction among military, dual-use or civilian targets. But neither the law of armed conflict nor common sense would allow belligerents to hide behind the skirts of its civilians. If the enemy is using civilian computers in his country so as to cause us harm, then we may attack them.

On the other hand, if the U.S. is defending itself against an attack that originates from a computer which was co-opted by an attacker, then there are real questions about whether the owner of that computer is truly innocent. At the least, the owner may be culpably negligent, and that does not, in fairness or law, prevent America from defending itself if the harm is sufficiently grave. Two scenarios reveal that the issues are more political than legal.

From a legal standpoint, the U.S. has long been a proponent of the international law doctrine of “defense in neutral territory” since Secretary of State Daniel Webster in 1842 accepted the British explanation that they had exercised their right of self-defense in capturing the steamer Caroline from an American pier, setting it ablaze, then sending it plunging over Niagara Falls after it had been used in the service of Canadian rebels: “Respect for the inviolable character of the territory of independent nations is the most essential foundation of civilization ... [and] exceptions should be confined to cases in which the ‘necessity of that self-defence is instant, overwhelming, and leaving no choice of means, and no moment for deliberation.’” Notably, the British were not responding to harm caused by the U.S. government but to harm caused by criminals acting from U.S. territory. That may well be the case if the U.S. uses the af.mil botnet defensively. However, the bigger legal challenge for the U.S. is reciprocity. What we do to other countries, they get to do to us without our complaining.

The political ramifications may be more difficult to manage. A U.S. defensive DDOS attack on a neutral country, or on multiple neutral countries, will certainly require the U.S. to explain itself. Commanders need to be ready to disclose some facts indicating why the U.S. took action and

what they did to tailor their response. Finally, the U.S. needs to be ready to consider legitimate claims for compensation, if warranted.

The truly difficult problems come in defending against attack from devices adversaries have captured from U.S. or allies' civilians. Generally, the U.S. military is not going to attack a U.S. private computer. Harm coming from one of those machines will first be treated as a crime, and military forces should stay out of the situation in accordance with the Posse Comitatus Act. However, Title 10 of the United States Code, Section 333, allows the president to order use of the military in the U.S. under tightly controlled conditions when civil authorities are overborne.

More challenging is the problem of an attack coming from an ally's civilian computers. Obviously, the U.S. would seek allies' cooperation if at all possible, but we could be in a position of launching an attack on a nation whom we have sworn to protect in a mutual defense pact. Together, the U.S. and its allies can reduce this risk by cooperating to maximize computer security. If we attack them as a matter of proportionate response, it would only be because computers in their territory are attacking us.

The biggest challenge will be political. How does the U.S. explain to its best friends that we had to shut down their computers? The best remedy for this is prevention. The U.S. and its allies need to engage in a robust joint endeavor to improve net defense and intelligence to minimize this risk.

A smart enemy will load his attack code in as many countries as possible so that when we launch a defensive strike, the maximum number of countries will be angry at the U.S. at the same time. However, this carries some risk for the real controller of the botnet that struck the U.S. If they spread their code broadly, they increase the incentive for multiple countries to cooperate in finding the truth of the attacks, so risk balances against reward. In the meantime, we have defended our own capability if circumstances required.

Also, a smart enemy will use "IP spoofing" by crafting his own DDOS attack packets to appear to come from somewhere other than the Internet Protocol (IP) address of the real node launching the attack. He could even craft his packets to make it appear the attack was coming from inside U.S. military networks so that if we merely captured the apparent source IP address and used that to aim the attack we would fire our botnet at our own computers. However, U.S. operators need not use the source IP address as the only pointer. All available information can be used to aim the attack, including the sophistication of the attack, targeting of sensitive systems and level of damage. If intelligence and circumstances point to a particular country, the U.S. is not barred from exercising its rights of self-defense or proportionate response just because the attacker was crafty. Military history is full of deception, and IP spoofing is simply the latest incarnation. In addition, the attacker could be guilty of the war crime of perfidy, or at least violate the U.N. prohibition against unfriendly acts, and call down on himself the ire of the international community, if he attempts to hide inside the cyber domain of a neutral nation. In any event, this threat illustrates the urgent need to improve the chance of proper targeting of our response to attack by cooperating to build an Internet version of the Distant Early Warning radars (the DEW Line) the U.S. and its allies jointly employed near the Arctic Circle during the Cold War.

There will be voices of skepticism.

“There are engineering challenges.” Yes, there are. They include potential choke points at border routers and backbone gateways. However, there are solutions, such as broadly distributing the computers or routing the technology refresh machines directly to the Internet. America’s Air Force has tackled tougher challenges. In any case, the current defensive concept is fundamentally flawed and cannot continue as our sole protection.

“Intelligence requirements would be too great.” While the joint doctrine on information operations notes that intelligence requirements for information operations can be more extensive than for kinetic operations, it did not contemplate an af.mil botnet. One of the advantages of a botnet is that offensive targeteers essentially only need the IP address of the target device, plus an appropriate level of intelligence, to allow an informed collateral damage assessment.

“Our enemies will know it was America that attacked them.” Precisely. We want potential adversaries to know this capability works and will be used when needed. In fact, we should do live-fire demonstrations on the Internet against range targets so foreign signals intelligence organizations can observe. Of course, we should fire inert rounds so as to not give away secrets.

“We might kill someone in a hospital or shut down emergency services.” The risk of this occurring is overblown. Hospitals and emergency services already need backup plans in case of many exigencies from natural causes, including the types of power and communications outages that a DDOS could cause. Also, target preparation in cyberspace can create no-strike lists just like the physical world.

“Brute force attacks lack elegance.” Who cares? The U.S. successfully conducted area bombing against Taliban trenches in Afghanistan. Not every attack needs to be with a laser-guided bomb. Brute force has an elegance all its own.

“This is not a silver bullet.” Of course not. A DDOS is not a good defense against espionage. The U.S. still needs a layered defense in-depth with firewalls, software patches, good information assurance and brilliant defenders because the botnet would do little against a phishing attack in which a hacker tricks people into running malicious software. However, what the botnet offers that does not exist today is the ability to let the enemy know he might be caught and suffer an attack that would take the benefit out of his risk.

“We might start a new arms race.” We are in one, and we are losing. Gen. James Cartwright, then-commander of the U.S. Strategic Command, testified for the 2007 Report to Congress of the U.S.-China Economic and Security Review Commission that analysts think China has the world’s largest denial-of-service capability. Can the U.S. reasonably believe that other nations have not learned from the DDOS attacks on Yahoo and CNN in 2000 or on Estonia in 2007? As Gregory Rattray projected in his book, “Strategic Warfare in Cyberspace,” if we are, or are about to be, engaged in a conventional conflict, the adversary may launch a DDOS that, under the right circumstances, could deter or delay us. Their capability could reduce our options. In addition, at least one foreign nation has advocated unrestricted warfare in cyberspace.

While the U.S. can have a plan to control each of the “horribles” in the parade, it is less certain that adversaries will.

The days of the fortress are gone, even in cyberspace. While America must harden itself in cyberspace, we cannot afford to let adversaries maneuver in that domain uncontested. The af.mil botnet brings the capability to help defeat an enemy attack or hit him before he hits our shores.