Low-level cyberattacks are common but truly damaging ones are rare
By James Andrew Lewis, Washington Post, October 10, 2013

Anyone with a computer and an internet connection can launch a cyber “attack,” but the skills and tools needed to do real damage are still in short supply. The internet was not built to be secure and will not become secure anytime soon. Networks are vulnerable. This explains why cyber espionage and fraud are so easy. Economies depend on the internet and a growing number of services and devices – factories, electrical power plants, airplanes, cars - are connected to it, making an irresistible target. Crash the computers that run these systems and things stop. Power grids, financial networks, communications, public utilities and transportation systems are all targets for cyber attack. But truly damaging attacks are hard to pull off.

Cyber attacks can disrupt data and services to sow confusion, damage networks and computers (including computers embedded in weapons systems) and in some instances, destroy machinery. The risks are real, but easily exaggerated, as when a group of defense advisors intoned in a recent report, that cyber attacks have “potential consequences similar in some ways to the nuclear threat of the Cold War.” Just as early air power enthusiasts ascribed miraculous qualities to air attack, expecting it to produce intolerable destruction and rapid victory, the discussion of cyber attack too easily veers into the realm of science fiction, what one senior naval officer calls “fairy dust.” Sprinkle a little cyber fairy dust on your military problem and it will disappear.

There is no fairy dust when it comes to offensive cyber capabilities. In the movies, a hacker types wildly on a laptop for a few seconds and turns off a city’s lights. In fact, a serious attack can take months to prepare, probing the target network and developing code tailored to damage, disrupt or destroy. Attacks have several stages: reconnaissance to identify the target’s vulnerabilities, breaking in, delivering the software “payload,” and then “triggering” it – all without being detected. The most damaging cyber attacks – like Stuxnet, the attack that destroyed centrifuges used by the Iranian nuclear program - are still a high art. Only the U.S., UK, China, Russia, and Israel possess the necessary skills, but many others want them.

Offensive cyber capabilities provide real military advantage. This is why most leading military powers are developing them. Publicly available information shows forty-six countries with military cyber programs, and twelve countries admitting to offensive cyber capabilities in 2012 (up from only four in 2011). Other countries have military programs but don’t admit to them.

Unlike the U.S., most countries say very little about their military doctrine. Most of them blend warfighting and covert action in their cyber war planning. Each nation’s plans for offensive cyber operations reflect their different military strategies. The Russians combine political action with cyber strikes on command networks and critical infrastructure to cripple opponents at the start of conflict. The Chinese focus on quickly disabling U.S. military systems and have systematically hacked into every weapon related to U.S. plans for an “Air-Sea Battle” in Asia. Iran will attack energy infrastructure and sees cyber as a way to score against a distant and once-invulnerable foe. North Korea’s attacks are driven by internal politics and dislike of the South.

There have been only a handful of true cyber attacks. Russia and China are hyperactive in cyber espionage, but are cautious about offensive use and avoid actions that could trigger a violent
response. Iran and North Korea are more aggressive and are improving their cyber capabilities. Iran attacked Saudi Aramco, destroying data on 30,000 hard drives. North Korea did something similar to South Korean banks. The worry is that either country will miscalculate in using cyber attacks and stumble into a larger conflict.

Jihadis, anarchists and other non-state actors don’t yet have real cyber attack capabilities. This is not much of a comfort because acquiring attack capabilities is getting easier. The trend in information technology is commoditization – products get smaller, cheaper, and more powerful. Cyber attack is being commoditized and cyber crime provides innovative tools (like the one Iran used against Aramco). Jihadis prefer the drama and violence of bombs to cyber attack, but this may change. The Syrian Electronic Army has only basic skills but could use its ties to Russian and Iranian hackers to improve. The global trend is increased capabilities and more attackers.

For the U.S., offensive cyber capabilities provide a new way to attack. The recently leaked Presidential Policy Directive 20 set the rules for “offensive cyber operations.” Only the President can approve a cyber operation likely to result in “significant consequences” that could produce loss of life or a damaging reaction, although the Secretary of Defense or the head of U.S. Cyber Command can take independent action in an emergency. The U.S. could relax the requirement for Presidential approval - similar to the Presidential authorization needed to use nuclear weapons - as technology improves, but offensive cyber capabilities are still too new, with too many unknown risks, to let anyone but the President make a decision with potentially profound consequences for the nation.

Cyber attack creates conflicts among military goals and missions. The fundamental conflict is whether to collect intelligence or to attack. Cyber weapons can be “single-use.” After the first attack, an opponent will develop countermeasures or fix vulnerabilities, making the weapon useless in the future (no one will fall for Stuxnet again). Cyber attacks can have unpredictable effects. Attacking a “tactical” target could also unintentionally damage “strategic” targets hundreds of miles away and expand any conflict. An attacker may not know what is connected to a target network - one early cyber attack disabled its target along with a broadcast network in a nearby allied country. Attacking a bridge and knocking out a hospital is something to avoid because it runs contrary to our rules for warfare and could create enormous political damage.

Someone needs to decide when the benefit of an attack outweighs the loss of intelligence or the political risk, or when a target justifies expending a weapon that might never work again. The inability to predict collateral damage and uncertainty over political effect has made the U.S. cautious. PPD-20 restricts independent action by tactical and operational commanders for this reason. A local commander may not know all the tradeoffs or the risks that using cyber attack could entail. Until we get better predictive tools, judgments about risk and consequences require decisions that only the top defense officials in Washington can make.

Offensive cyber operations are an inevitable part of conflict. They are no more likely to go away than are guns or missiles. A new technology appears and is adopted for military use. Soon all advanced militaries have it. If the technology is cheap enough, smaller countries and amateurs will acquire it as well. This has been the pattern for weapons since the start of the industrial revolution and it still holds for cyber attack. Perhaps nations will agree on limits to govern
offensive cyber capabilities – although until this year, there wasn’t even international agreement that the laws of armed conflict could apply to cyber attack - but no one will give them up. Offensive cyber operations give the U.S a military advantage, but opponents can also carry them out. America leads the world in cyber offense, but our defenses are weak and we are beginning to lag behind others nations. U.S. policy is troublingly incongruent. Strengthening offensive cyber capabilities is a military program with wide support, but strengthening defensive capabilities runs counter to strongly held ideologies and commercial interests. Our defenses have not kept up in the face of growing foreign capabilities. Cyber deterrence is a non sequitur – words that people have strung together in lieu of thought – because in cyberspace, a strong offense is not the best defense. We may have the best offensive cyber capabilities on earth, but when it comes to defense, America still depends on the kindness of strangers, since despite years of noisy discussion, if somebody decides to attack us we are in no way ready to protect ourselves in cyberspace.