

# INFORMATION OPERATIONS NEWSLETTER



Compiled by: [Mr. Jeff Harley](#)  
**US Army Space and Missile Defense Command  
Army Forces Strategic Command  
G39, Information Operations Division**

The articles and information appearing herein are intended for educational and non-commercial purposes to promote discussion of research in the public interest. The views, opinions, and/or findings and recommendations contained in this summary are those of the original authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of the Army, or U.S. Army Strategic Command.

[ARSTRAT IO NEWSLETTER ON PHI BETA IOTA](#)

[ARSTRAT IO NEWSLETTER AT JOINT TRAINING INTEGRATION GROUP FOR INFORMATION OPERATIONS \(JTIG-IO\) -  
INFORMATION OPERATIONS \(IO\) TRAINING PORTAL](#)

# TABLE OF CONTENTS

VOL. 12, NO. 08 (JUNE 2012)

1. [Stuxnet: US Can Launch Cyberattacks But Not Defend Against Them, Experts Say](#)
2. [Offensive Information Warfare and Red Teams](#)
3. [Cyber Warfare...Brought To You by J.C. Wylie](#)
- 4.

## Stuxnet: US Can Launch Cyberattacks But Not Defend Against Them, Experts Say

By Gerry Smith, Huffington Post, 06/01/2012

Since President Barack Obama took office, the United States, along with Israel, has launched a series of cyber attacks that have damaged Iran's nuclear program, according to a June 1 story in The New York Times. These attacks are apparently the first time that the United States used a cyberweapon to damage another country's infrastructure, the Times writes.

But should another country launch a similar attack, experts say the United States remains woefully unprepared to defend itself.

James Lewis, a senior fellow at the Center for Strategic and International Studies, said the United Kingdom, Russia, China and Israel all have cyberweapons, while France, Germany, Iran and North Korea are trying to develop them.

"We're in a place where these weapons exist and people will use them," Lewis said.

However, the United States "does not really have any defense against this," he said. "We depend on the kindness of strangers that someone hasn't launched something against us," said Lewis.

Last year, the Pentagon said that computer sabotage coming from another country can constitute "an act of war."

According to the Times, Obama accelerated covert cyber attacks against Iran that began during the Bush administration. One attack temporarily took out nearly 1,000 of the 5,000 centrifuges Iran used to purify uranium, slowing the country's ability to develop nuclear weapons, the Times reports, citing interviews with current and former U.S., European and Israeli officials involved in the cyber program.

Since these attacks by computer worm became public in 2010, security researchers have speculated that the United States and Israel were behind them, although neither country had publicly acknowledged its role. Cybersecurity experts have dubbed the worm Stuxnet and called it the most sophisticated cyberweapon ever created.

The confirmation that the United States was behind Stuxnet is another sign of the Obama administration's efforts to build up the country's offensive cyber capabilities. Earlier this week, the Washington Post reported on a Pentagon effort to develop new technologies to launch cyber attacks, including a plan to map the entirety of cyberspace and build a system that can launch cyberweapons without human operators typing in the code.

But experts say America's ability to defend itself in turn is lagging. The computers that ran Iran's nuclear centrifuges and were hacked by Stuxnet were made by the German company Siemens, whose industrial control systems are used around the world. In December, Siemens announced it was working to fix security flaws in those systems after the U.S. Department of Homeland Security warned that such flaws could make public utilities, hospitals and other critical infrastructure vulnerable to cyber attack, according to Reuters.

"We now live in a world where industrial control systems can be attacked in the event of a crisis. That goes for ours as well as everybody else's," warned Stewart Baker, a former assistant secretary at the Department of Homeland Security.

And yet, Baker said, "We do not have a serious plan for defending our industrial control systems even though our entire civil society depends on it."

Congress is considering legislation to bolster the cybersecurity of the nation's most vital computer networks. Sens. Joe Lieberman (I-Conn.) and Susan Collins (R-Maine) have introduced a bill that would require power plants and other critical infrastructure to meet baseline security standards. The bill, which has the support of the Obama administration, is expected to receive a vote in coming weeks.

But Republicans and business lobbyists have opposed imposing cybersecurity regulations, saying they hurt private companies, which control the majority of critical infrastructure. Last month, the House passed a cybersecurity bill that did not set security standards, but instead focused on greater sharing of information between the public and private sectors.

Some experts saw irony in the news that the United States was behind Stuxnet. Jason Healey, director of cyber statecraft initiatives at the Atlantic Council, said some current and former government officials have cited Stuxnet as an example of why the federal government needs to impose security regulations on critical infrastructure.

"They've said, 'Look at this dangerous thing out there,'" noted Healey. "But we wrote it. We unleashed this thing. It's like an arsonist calling for a better fire code."

Healey said the United States must better secure its own cyber defenses before it launches more cyber attacks on other countries.

"I'm hearing a lot today about glass houses and stones," he said.

[Table of Contents](#)

## Offensive Information Warfare and Red Teams

By Uri Fridman, [SOFRep.com](#), June 2, 2012

*It's 0100. The moon sits high in the sky over the target's facility. Four men dressed in BDUs and gear are sneaking in by the tree line, about 50 meters outside the building outer perimeter fence. Pausing occasionally to peer through night vision monoculars to scan the perimeter. They make it to the final penetration position.*

*One of the men keys a mike and relays their position to the TOC (Tactical Operations Center) where another team is ready for the next phase of the operation. This team is comprised of highly skilled digital operators with backgrounds in computer hacking, intelligence, electronics and networking.*

*They've already spent the better part of 2 months preparing the mission's digital package: digital intelligence gathered via OSINT and direct digital actions (DDA) – in other words, through good, solid network and computer hacking.*

*They've also performed an onsite analysis: they used laptops and highly sensitive antennas to scan for radio frequencies emanating from the target and a good solid recon by observing guard patrol schedules and looking for holes in the perimeter for possible breach points.*

*They are now ready to execute the next DDA in support of the team on the ground. This digital op will enable the team to bypass the fence's security and remain undetected.*

*Suddenly, a patrol vehicle appears near the corner of the building, its headlights coming in directly to the men. The operators freeze. Not a single movement. The vehicle passes, and the men remain undetected.*

*Minutes later, the men reach the fence's back gate. They wait. The team at the TOC is busy with their computers. They have full access to the command and control (C2) computers deep inside the bowels of the target. The backdoor they installed not long ago provides a full range of options.*

*One of the digital soldiers sends a pre-recorded command, and the C2 computer disables the camera and disengages the lock on the fence's back door. The ground team moves in quietly. The gate is closed and the security features are enabled again.*

*At around 0200, the operators enter the target's office, where he – a well known terrorist – plans the next attacks on the free world. Not this time, the operators think. They place the specially crafted explosive device under the chair and leave, undetected.*

The story above might seem out of a Hollywood movie, however, it is as close to a real operation as I am allowed to write. The digital operators are part of a special breed of people working for a very skilled red team.

What are Red Teams? They're the special operation forces of the security industry. They are composed of highly skilled individuals hired by clients (government and private) to break into their own networks and physical security. These guys find the security flaws so they can be patched before someone with malicious plans can sneak in.

The DoD defines them as an organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment, and from the perspective of adversaries and others.

You can read more about Red Teams in:

[Inside NSA Red Team Secret Ops With Government's Top Hackers](#)

[Anatomy of a Red Team Attack](#)

Red Teams can be used to support SOF units as intelligence gathering elements. They can also be used to augment those units by providing digital and comm support and running digital operations (DO) to make the operators on the ground more efficient.

In past operations where my team was involved, we supported those units in two different phases.

1. We provided the initial digital recon of the target, including inside information about sentry schedule, different access routes (those that were locked during the night hours and those open but monitored), number

of personnel inside the facility during the different times of the day, hardware and software information, provided a complete site casing including detailed sketches based on the design blueprints extracted from a computer, and a week's worth of daily activity logs hour per hour.

2. We also acted as a direct action support team, providing real time information about what the target was doing inside the premises, location of sensitive computers, disabling alarms and other security features in real time, etc.

All that information was carefully analyzed and compared with the intel gathered by the unit's own intel guys and was found either at the same level or, in most cases, more accurate.

The guys on the ground went in having a clear image of what to expect on the site and what to look for once they were inside the building.

Another type of operations the Red Teams can run is the DDA. Direct digital action ops are what people today refer as "cyber-battles." The digital operators study the targets, prepare their weapons (a weaponized PDF, a website containing malicious code, a backdoor ready to be dumped into the target's system by hiding it inside another program, etc) and perform the attack. Attacks can disrupt the ability of the target to reach the Internet or communicate with their people; it can destroy their backends and frontends (software); it can disperse wrong information and generate chaos, and it can bring the whole enemy operation to a halt.

Digital warfare, also known as cyber warfare (although I don't like to use that term), is increasing in tempo. Governments are realizing that the future battles are going to be fought both on the real and the virtual worlds.

Red teams can help, if only by pointing the weak spots on our own defenses.

[Table of Contents](#)

## Cyber Warfare...Brought To You by J.C. Wylie

Posted at [Information Dissemination](#), May 31, 2012

Future thinking about cyber operations is often analogized to early airpower doctrine. Like the early airpower theorists, Gregory Rattray also points out that cyberwar theorists also make the mistake of assuming that cyber operations capabilities will be standalone strategic weapons. The cyber weapon, in other words, is not always going to get through. More likely is cyber warfare operations and tactics augmenting regular operations and tactics. In other words, the difference is between an unrealistic vision of cyberwar and a very much plausible conception of cyberwarfare.

Naval warfare and special operations theory may present a better prism for viewing how cyber operations will play out. In his seapower classic *Military Strategy: A Theory of Power Control*, Rear Admiral J.C. Wylie argued that the aim of strategy was to gain some measure of control over the adversary. There were essentially two styles of strategy: sequential and cumulative. Sequential strategy utilizes force in discrete, linear packages. An land army on campaign sweeping through a territory destroys an enemy state layer by layer, division by division. Cumulative forms of strategy, on the other hand, build gradual and nonlinear pressure on an opponent.

The classic example is the relationship between the land war in the European Theater of Operations and the Combined Bomber Offensive. By tying down precious German resources, the Bomber Offensive amplified the strategic effect of the land campaigns. Airpower advocates were, of course, wrong that a strategic airpower offensive would on its own negate the need for a land campaign. But the Bomber Offensive cannot simply be dismissed as a failure merely because it did not live up to its planners' strategic expectations. In naval warfare, the Pacific Theater of operations paired a sequential strategy of advance through fortified island networks with the cumulative destruction of the Japanese merchant fleet by submarines. To go even farther back in military history, Winfield Scott's Anaconda Plan, which exploited Union strength on the rivers and the oceans, amplified the strategic effect of land operations in the Western and Eastern theaters of operation.

So how does Wylie fit into cyber operations? Well, first let's take a look at what Kings' College professor Thomas Rid has written about the characteristics of cyber weapons:

Cyber-weapons span a wide spectrum. That spectrum, we argue, reaches from generic but low-potential tools to specific but high-potential weaponry. To illustrate this polarity, we use a didactically helpful comparison. Low-potential 'cyber-weapons' resemble paintball guns: they may be mistaken for real weapons, are easily and commercially available, used by many to 'play,' and getting hit is highly visible -- but at closer inspection these 'weapons' will lose some of their threatening character. High-potential cyber-weapons could be compared with sophisticated fire-and-forget weapon systems such as modern anti-radiation missiles: they require specific target intelligence that is programmed into the weapon system itself, major investments for

R&D, significant lead-time, and they open up entirely new tactics but also novel limitations. This distinction brings into relief a two-pronged hypothesis that stands in stark contrast to some of the debate's received wisdoms. Maximising the destructive potential of a cyber-weapon is likely to come with a double effect: it will significantly increase the resources, intelligence and time required to build and to deploy such weapons -- and more destructive potential will significantly decrease the number of targets, the risk of collateral damage and the coercive utility of cyber-weapons.

We also know that certain weapons are modular and customizable for multiple roles, the development and acquisition cycle (at least compared to certain air superiority platforms) is very agile, weapons utilize the target system itself as a means of inflicting coercive damage, and they are heavily customized to the target and difficult to utilize in a salvo capacity. Because of this, it is unlikely they can be utilized as a standalone strategic weapon.

DoD seems to realize this too. Take a look at this graf from an article on DARPA's Plan X:

*Cyberwarfare conjures images of smoking servers, downed electrical systems and exploding industrial plants, but military officials say cyberweapons are unlikely to be used on their own. Instead, they would support conventional attacks, by blinding an enemy to an impending airstrike, for example, or disabling a foe's communications system during battle.*

Yup, sounds cumulative. DoD's vision of cyber capabilities is explicitly based on the presumption that they amplify the capabilities of conventional attacks.

One vision of how cumulative strategy might be realized in a cyber context can be found in a distillation of cumulative strategy in the special operations community. James D. Kiras has argued in his work on special operations that the relationship between special operations forces and general purpose forces also demonstrates the intersection of cumulative and sequential strategy. Special operations forces use psychological and material attrition to raise cumulative costs of operating, enhancing the striking power of conventional forces. A group of commandos raising havoc in the enemy rear area disrupts the target's logistics and forces tactical dispersion, weakening the ability to win the fight in the forward edge of the battle area. Unlike the stereotype of attrition encountered in maneuver warfare literature, attrition can have nonlinear cumulative effects. The kind of damage inflicted by cumulative capabilities, be it naval forces, airpower, or special operations units, snowballs into a fearsome weapon.

Lukas Milevski has made the analogy that cyber operations have many of the same characteristics as special operations forces. High-risk special operations depend on significant amounts of target intelligence, surprise (the zero-day exploit), and are utilized against targets in which tailored and customizable means trump general purpose conventional power. Moreover, Milevski observes that utilizing an exploit against an important system also simultaneously ensures that the same vulnerability cannot be exploited readily again through exposure. While Milevski is right to observe how the specialized nature of cyber operations generates a particular kind of cumulative pressure that augments sequential strategy, there is more to the Wyliean metaphor than simply special operations theory.

The routine conflation of intelligence exploitation systems with weapons is but one symptom of what NDU professor Sam Liles argues is a common confusion of information security (the protection of systems) and the optimization of networks with offensive warfare. Network-centric enhancement to make war or the ability to manage and provision a network, Liles observes, is not the same thing as waging war. Liles also argues in another post that the real ream of cyberspace is the zone of command, control, coordination, data and cognition---a "seam" between the respective domains that US military doctrine (at times artificially) defines. Such a conception broadens not only our conception of cyberspace but also our idea of what our means of cyber operations may be. We aim to use the seam to achieve a measure of control over the adversary. Moreover, just as the purpose of operations on the sea is to effect events on land, cyber operations ultimately are a means of exploiting the seam cumulatively to amplify the conventional (sequential) campaign.

Finally, this paragraph also demonstrates once again that some of the better ideas about this subject were written fifteen years ago:

*Another goal is the creation of a new, robust operating system capable of launching attacks and surviving counterattacks. Officials say this would be the cyberspace equivalent of an armored tank; they compare existing computer operating systems to sport-utility vehicles — well suited to peaceful highways but too vulnerable to work on battlefields. The architects of Plan X also hope 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. Officials compare this to flying an airplane on autopilot along predetermined routes.*

John Arquilla and David Ronfeldt originally conceived the role of cyber war not as a standalone strategic weapon but the integration of cyber tactics and operations into warfare as a whole. Hardened systems capable of surviving hits and giving back, at speeds faster than tactical operators can contemplate, as a means of amplifying conventional effects are well within the idea of warfare they predicted in their early works.

J.C. Wylie's works are, of course, an highly imperfect means of thinking about information power. But they offer a starting point as doctrine development, operational tests, and perhaps wartime employment further determine the American approach.

[Table of Contents](#)

[Table of Contents](#)