Computers as Weapons of War

"History teaches us that in asymmetric warfare the most heavily armed do not always win."[1]

—Ignacio Ramonet

By John Bumgarner

Most warfare throughout the two centuries of the industrial era centered on one principal strategic objective: the physical occupation of territory. The possibility of occupying territory, or the threat of becoming occupied, forced many nations to amass large standing armies, to maintain navies, and to build aircraft in hopes of achieving battlefield superiority against their adversaries.

Several pivotal events over the last three decades have been gradually changing that paradigm, shifting nation-states from the industrial era of warfare into the cyber defense era of warfare. One of these events was when cyberspace was classified by the United States government as being strategically important to national security.[2] With that classification, cyberspace became the fifth domain of war, comparable to the domains of land, sea, air, and space. The geopolitical events that were the tipping points that catapulted us from the industrial defense era to one of cyber defense, were the campaign-level cyber attacks launched against Estonia in 2007 and Georgia in 2008.[3] Global militaries are scrambling to understand their own capabilities, their adversaries' capabilities, and the new multidimensional, multidirectional and multilayered battlespace of cyberspace.

The U.S. armed forces have been grappling with these issues for years, but only recently established the U.S. Cyber Command (USCYBERCOM) to start addressing our national defense and economic survivability in cyberspace. The operational mission of the command is to coordinate U.S. operations in cyber network defense and cyber network attacks. The command is linked to the National Security Agency, which has a well established history of contributing to the nation's intelligence collection efforts (e.g. Signals intelligence (SIGINT) and technological advancements (e.g. cryptography) in the digital age.

The ever-increasing asymmetrical (e.g. Al-Qaeda) and peer-to-peer (e.g. Russia) threats posed within this new war-fighting domain are eclipsing current U.S. military doctrine, which outlines Information Operations (IO) capabilities. Current Joint Doctrine outlines five primary categories of IO capabilities, which are Computer Network Operations (CNO), Electronic Warfare (EW), Military Deception (MILDEC), Psychological Operations (PSYOP), and Operations Security (OPSEC).[4]

Electronic warfare, military deception, psychological operations, and operations security have a long established history within the industrial defense era. Computer Network Operations[5] is the only IO capability conceived entirely in the cyber defense era. CNO has three operational missions. The first is to defend information systems from enemy attacks. The second is to gather intelligence from adversarial networks. The final CNO mission is to conduct offensive cyber attacks against enemy computer systems and other electronic assets.

Combining core IO capabilities with traditional military operations (e.g. strikes, noncombatant evacuation operations) has been a major challenge for classically trained commanders. Military leaders need to realize that the cyber component of information operations can support a broad spectrum of combat and noncombat operations, as well as the continual preparations needed for both. Within certain offensive engagements, the IO component can be a more effective option than the use of conventional forces.

U.S. Air Force Senior Airman Lauren Johnson, a 379th Expeditionary Communications Squadron network control center technician, maintains the base computer server for more than 10,000 users January 4, 2010, at an undisclosed location in Southwest Asia. *(U.S. Air Force photo by Senior Airman Kasey Zickmund/ Released)*

U.S. military and political leaders are still debating the rules of engagement and the legitimacy of using the latter capability as an offensive technique in future warfare. In early 2009, Pentagon officials said they were uncomfortable discussing the issue of offensive cyber operations.[6] Senior government officials from the United States and Russia met in November 2009 to discuss the possible creations of treaties that would limit offensive cyber operations and curtail the development of cyber munitions.[7]

As an offensive capability, CNO engagements have as much potential to inflict physical damage on adversaries' information systems as a multi-million dollar missile does. In chemical production facilities, for example, computers controlling reactions that take place at high pressures and temperatures could be used to cause explosions and fires. Operations targeting national critical infrastructure, such as electrical generation systems that service large metropolitan areas, have the potential to cause extreme[8] economic loss and even considerable loss of life. Understanding the full range of offensive engagement possibilities that CNO components can bring to the fight is one of the greatest challenges in the cyber battlespace.

For a number of years, military operations have used electro-magnetic attacks to disrupt enemy communications on the battlefield, but there are now many additional IO capabilities. The cyber campaign against Georgia in August 2008 is probably the best example of how to properly employ one of the newest IO capabilities, computer network attack on a modern battlefield. During that campaign, Russians and Russian sympathizers disrupted key Georgian media sites through the Internet using denial-of-service — a neo-electronic warfare jamming technique of the cyber defense era.

The speed of action and multidirectional nature of these cyber strikes adhered to a classical military swarming technique, overwhelming the cyber defenses of the Georgian targets. The attacking forces were highly decentralized, but were able to synchronize and concentrate their operations in a way that made any Georgian defensive response nearly impossible. The primary objective of this cyber campaign was to support the Russian invasion of Georgia, and the cyber attacks fit neatly into a military-style invasion plan. Many of these cyber strikes were clearly designed to make it harder for the Georgians to determine what was happening. The inability of the Georgians to keep these websites up and running was instantly damaging to national morale. These attacks also served to delay any international response to the kinetic conflict unfolding in the South Ossetia region.

Probably the most important strategic lesson learned from the cyber campaign against Georgia is that cyber attacks are a viable military option on the battlefield. Another lesson is that cyber attacks can be launched from a safe remote location. Yet another lesson is that these operations can be employed in certain cases (e.g. targeting civilian communication facilities) where limiting the physical damage to the target is a strategic concern for the theater commander.

Even though the cyber campaign against Georgia was tactically successful, there are several disadvantages to using offensive cyber attacks against an adversary's information systems in place of more traditional attacks such as air strikes or direct

Alexsi, an Israeli air force crew chief, conducts preflight checks at Nellis Air Force Base, Nev., before a training mission at Red Flag July 20, 2009. Red Flag is a highly realistic combat training exercise that pits U.S. and allied nation air forces against simulated enemy forces in a challenging air, ground, cyberspace and electronic threat environment. *(U.S. Air Force photo by Tech. Sgt. Michael R. Holzworth/ Released)*

action missions by special operations units. One of these disadvantages is that cyber attacks don't produce quantifiable results as consistently as their kinetic counterparts do. This is due to the fact that specific cyber attacks can often be rendered useless by routine modification (e.g. application-level patches) in the target system. In military engagements involving equals, the tactical advantage for most offensive cyber attacks goes to the defender, because it is easier and faster to implement defenses than it is to develop offensive cyber attack techniques.

Even with these technical and tactical limitations, computer network operations have great potential in future military conflicts. For example, during the industrial warfare era acts of industrial sabotage against critical targets were often conducted by physical means, thus requiring localized access. In the cyber defense era, the potential for the military to conduct acts of industrial "cybertoge"[9] are increasing exponentially. Key nation states already possess the capabilities to disrupt information systems used within civilian industries that have strategic military value to a nation's war effort. These critical infrastructures include airports, electric power plants, dams, gas and oil pipelines, oil refineries, maritime ports, railroads and manufacturing facilities. Historical warfare precedence shows that all these industries have been targets of sabotage attacks using conventional kinetic methods, such as direct action missions by special operations forces.

Although conventional forces are effective for sabotage, IO forces can conduct many of these operations without causing physical damage to the target or placing soldiers in harms way. There are several technical cybertoge techniques available to offensive IO forces including the use of weaponized computer viruses or worms. Probably the most effective technique available to offensive IO forces is the intentional insertion of a "logic bomb,"[10] into an information system that the target is dependent upon. These malicious programs can be introduced through a variety of means, months or even years before they need to be triggered for a specific operation.

One example that has not been publicized occurred during an unannounced training exercise conducted at a major corporation. During that exercise, I personally crafted some specialized code that was designed to simulate a hardware failure on a common UNIX platform. The warning messages generated by the code contained valid support phone numbers, e-mails addresses, and website addresses for the platform vendor. The technical contact within the corporation contacted the vendor concerning the hardware problems. Over a two-week period the vendor sent multiple technicians to replace various hardware components within their platform. When a replacement component failed to resolve the problem, the technician would escalate the issue to the next tier of support at the vendor. Eventually the exercise was terminated, because the internal support team or the vendor couldn't identify the problem. During the exercise hundreds of man-hours and thousands of dollars were expended to tackle an information system hardware failure that was fictitious.

Unclassified historical examples of logic bomb deployments by military forces do not exist, but we have examples from the civilian sector. One of these examples involves a disgruntled employee who planted a logic bomb within the computers of UBS PaineWebber.[11] When the code was detonated it erased critical files on approximately 2,000 UBS's computers. According to published reports surrounding this incident some of the computers affected were offline for several weeks, which hindered USB's daily business operations. In 2008, a similar incident was accidentally foiled by an employee at the United States mortgage corporation Fannie Mae.[12] The Fannie Mae logic bomb was designed to erase the hard drives for 4,000 servers on a preset date.

There is also a purported historical example of the Central Intelligence Agency using a logic bomb to cause physical damage to a Siberian pipeline. This revelation was highlighted in the book *"At the Abyss: An Insider's History of the Cold War,"* written by Thomas Reed, a former Secretary of the Air Force and former Director of the National Reconnaissance Office. According to Reed's account of the incident, the CIA inserted malicious instructions in pipeline control system software stolen by the Russians. When the software was deployed in the Siberian network, it triggered the logic bomb to activate instructions that were designed to destabilize components that controlled pressure within the pipeline. These pressure destabilizations triggered a failure of safety mechanisms at the pipeline, which eventually exploded. The resulting consequences associated with this alleged attack are an excellent example of how a strategic supply line can be disrupted without using conventional methods (e.g. explosives).

The modern battlefield is littered with military equipment, such as main battle tanks, satellite communication architecture, and UAV battlefield surveillance systems, that contain sophisticated electronic components that can be targeted by cybertoge forces. In the heat of battle, enemy equipment containing embedded malicious code could activate, which in turn could disable computerized targeting systems, global positioning systems, thermal imaging devices, communication components or internal power plants in mechanized weapon systems

(e.g. Russian T-95 main battle tank). When utilized properly, cybertoge attacks achieve the element of surprise, because of their stealthy delivery method. This capability for surprise prevents the adversary from receiving indications that an attack is approaching or already initiated. Under ideal conditions, the enemy may be forced to withdraw or surrender their forces.

Targeted cyber attacks can be just as destructive as operations using cybertoge techniques. Probably the best documented evidence of such an attack is a previously classified video produced by the Department of Energy's Idaho National Laboratory for a project code named "Aurora."[13] This video shows a remote cyber attack being launched against control systems that managed an electric generator hosted within DOE test range in Idaho. The attack was highly effective in causing the generator to fail, because of the mechanical effects caused by the cyber attackers. The attack made the generator wobble and go out of control, caused the rotor to hit the stator, shredded the windings, and made the generator catch fire. This sort of attack becomes more effective, the larger the generator. It could be automated, is scalable, and could be used to destroy large numbers of generators simultaneously.

This successful attack was an eye opener for those industries and government agencies responsible for the security and economic stability of the electric grid in the United States. One of most troubling lesson learned from the Aurora project is how a cyber attack could cause lasting physical damage to a mechanical component. Electrical power components (e.g. dams, power plants, transmission lines) have been viable military targets since their inceptions into the world. During the World Wars, Allied Forces destroyed electric systems with massive bombing campaigns. In 1999, U.S. Forces operating in Serbia under the umbrella of NATO disrupted the electrical power infrastructure using a non-lethal munition,[14] which contained carbon graphite filaments.

While these aerial campaigns have been an efficient method of incapacitating an adversary's electrical systems cyber attacks can be employed in similar ways. Offensive IO forces can launch precision attacks in a given operational area, which could disrupt electrical power prior to committing any conventional forces (e.g. infantry, air assets). In certain political scenarios, the use of IO forces instead of conventional forces maybe the more strategically acceptable option. IO forces can be used in these circumstances to provide a proportional response that disrupts an enemy's critical infrastructures (e.g. electrical power). Limiting physical damage in these cases would greatly reduce repair time and possibly limit any post-conflict restitution payments to replace the components.

This type of attack aligns with one of Clausewitz's nine Principles of War. That principle is economy of force, which calls for the judicious exploitation of combat power in relation to achieving mission objectives. Military-level cyber attacks against electrical power generation facilities increases the likelihood for externalities consequences in the operational area. Such tactical cyber strikes can also cause major disruptions in conventional land-line and Voice over Internet Protocol (VoIP) communications infrastructure, cellular networks, television and radio broadcasts. These secondary disruptions could sever command and control (C2) channels or possibly cripple air defense networks, which would benefit conventional forces operations.

U.S. Marine Sgt. Kermit Harrison, far right, teaches advanced computer networking to Iraqi army Maj. Abbas Ahmed, Communication Officer, 7th Iraqi Army Division, at Camp Mejid, Asad, Iraq. *(U.S. Marine Corps photo by Staff Sgt. Chad L. Simon/Released)*

Another probable IO attack for military forces was highlighted in the 60 Minutes segment entitled "Sabotaging the System."[15] Experts working for the Sandia National Laboratory demonstrated in that segment how to disrupt production at an oil refinery. The cyber attacks were designed to cause critical components to overheat, leading to a catastrophic failure at the refinery. The experts caused this failure by modifying the BTU settings for a heating element within the refinery and by disabling the recirculation pumps used to control increases in temperature. Cyber attacks similar to the one conducted by Sandia could be carried-out by IO forces against refineries that produce fuels, lubricants or petrochemical products used by enemy forces.

Similar IO attacks could be conducted against nation states that have violated international treaties in order to carry out as uranium enrichment for nuclear weapons. Most of the unauthorized enrichment facilities in these cases are constructed deep underground. Conventional munitions, including bunker busters, could have difficulty penetrating and damaging these hardened structures. Cyber munitions, however, could be used to destroy key equipment used in the enrichment process. One of the primary IO targets would be the gas centrifuges used to create weapons grade uranium. The rotors within these centrifuges operate at extremely high speeds (e.g. 50,000 RPM). A cyber attack that increased the RPMs beyond normal safely levels could result in a catastrophic failure of a single centrifuge. Implementing this IO attack across thousands of centrifuges has the potential to disrupt enrichment operations for considerable periods of time.

Offensive military operations targeting enemy supply lines have been conducted for centuries. Modern militaries have adopted just-in-time inventory practices that have greatly limited their on-hand strategic stockpiles of beans, bullets, and

bandages. Offensive IO forces could be used to disrupt these critical supply lines. One of the high-value IO targets would be the computerized inventory control systems used within this fragile supply chain. Once the IO force has penetrated this computerized system, they can identify critical supplies, insert disinformation about the inventory levels of these supplies and then reroute these critical supplies to remote locations. Another probable IO attack would be to reprogram the Radio Frequency Identification (RFID) used to either track individual components or pallets of supplies. Certain RFID tag designs utilized ultra high frequency (UHF), which makes them highly prone to IO attacks using traditional electronic warfare methods. IO forces could also be used to target individual components (e.g. shore-to-ship cranes) used within the shipping process. Many of the modern shore-to-ship cranes are highly computerized, which makes them vulnerable to a targeted cyber attacks. Some of the systems use embedded operating systems (e.g. Microsoft Windows XP), which have known security vulnerabilities. IO forces could exploit one of these vulnerabilities to disable or damage the crane.

The U.S. Armed Forces have sometimes been called on to conduct preemptive conventional strikes against strategic enemy targets. On today's battlefield, military commanders can conduct preemptive cyber strikes against critical infrastructure targets (e.g. oil refineries, electrical power plants, telecommunication nodes) to potentially cause so much destruction that the enemy would have limited ability to carry out combat operations. Such preemptive actions could potentially reduce the collateral damage and casualties normally associated with military conflicts. An adversary that exercises a strategic first cyber strike that successfully disrupts an opponent's critical infrastructures prior to battle could potentially reduce the opponent's capacity to wage war.

The examples discussed in this paper are only a sampling of the possible offensive information operations that could be conducted by military forces within the Cyber Defense Era. These examples underline the importance of utilizing offensive IO forces in future military conflicts. The digital age has made cyber attacks a logical extension of projecting diplomatic and military power against our nation's adversaries.

In this new defense era, wars will not only be waged by high-tech conventional forces using bullets and bombs, but in concert with information operations forces using bits and bytes. Current U.S. military doctrine doesn't fully address these combined neo-warfighting capabilities. The doctrine also isn't designed to quickly adjust to rapid technological shifts that occurred in cyberspace, which could adversely affect military superiority. With the dawning of the Cyber Defense Era comes a pressing need to reassess traditional warfare doctrine to ensure that our armed forces meet the challenges that this new era brings to the 21st Century battlefield.

John Bumgarner *is the Research Director for Security Technology the U.S. Cyber Consequences Unit (US-CCU) and a Senior Research Fellow in International Security Studies at the Fletcher School of Law and Diplomacy of Tufts University. He was formerly a member of the Intelligence and Special Operations branches of the United States Army.*

Endnotes

1 Ignacio Ramonet, "Unjustified means." *Le Monde diplomatique*, November 1, 2001. Accessed at: http://mondediplo.com/2001/11/01unjustified

2 The National Military Strategy of the United States. Accessed at: http://www.defenselink.mil/news/Mar2005/d20050318nms.pdf

3 John Bumgarner and Scott Borg, Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008, A US-CCU Special Report, August, 2009.

4 Information Operations, Joint Publication 3-13, February 13, 2006. Information Operations also include various supporting and related capabilities. Supporting capabilities include: Counterintelligence (CI), Combat Camera (COMCAM), Information Assurance (IA), physical attack and physical security. Related capabilities include: Civil-Military Operations (CMO), Defense Support to Public Diplomacy (DSPD) and Public Affairs (PA).

5 Information Operations, Joint Publication 3-13, February 13, 2006. Computer Network Operations (CNO) includes: Computer Network Attack (CNA), Computer Network Defense (CND) and Computer Network Exploitation (CNE).

6 David E. Sanger and Thom Shanker, "Pentagon Plans New Arm to Wage Cyberspace Wars." *New Yorok Times*, May 28, 2009. Accessed at: http://www.nytimes.com/2009/05/29/us/politics/29cyber.html

7 John Markoff and Andrew E. Kramer, "In Shift, U.S. Talks to Russia on Internet Security." *New York Times*, December 12, 2009. Accessed at: http://www.nytimes.com/2009/12/13/science/13cyber.html? scp=2&sq=russia&st=cse

8 Milton Maltz, "Turning power lines into battle lines." *National Post,* October 21, 2009 Accessed at: http://www.financialpost.com/personal-finance/tax-centre/Story.html?id=2125907

9 The term cybertoge was coined by John Bumgarner, during a presentation entitled "Cybertoge Threats," which was presented at the National Defense Industrial Association Cyber Symposium in San Diego, California on October 27, 2009.

10 A "logic bomb" or "slag code" is a set of instructions that has been intentionally designed to execute (or 'explode') when a particular condition has been satisfied. Commonly these "bombs" delete or corrupt data, reset passwords, or have other harmful effects.

11 Sharon Gaudin, "Ex-UBS Systems Admin Sentenced To 97 Months In Jail." *Information Week,* December 13, 2006. Accessed at: http://www.informationweek.com/news/security/showArticle.jhtml?articleID=196603888

12 Thomas Claburn, "Fannie Mae Contractor Indicted For Logic Bomb." *Information Week*, January 29, 2009 Accessed at: http://www.informationweek.com/news/security/management/showArticle.jhtml? articleID=212903521

13 Jeanne Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid." *CNN,* September 26, 2007. Accessed at: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

14 The BLU-114/B is a non-lethal munition used to disrupt electrical systems. The device is also known as the "soft bomb," "graphite bomb" and "blackout bomb."

15 60 Minutes "Sabotaging The System." *CBS*, November 8, 2009. Accessed at: http://www.cbsnews.com/video/watch/?id=5578986