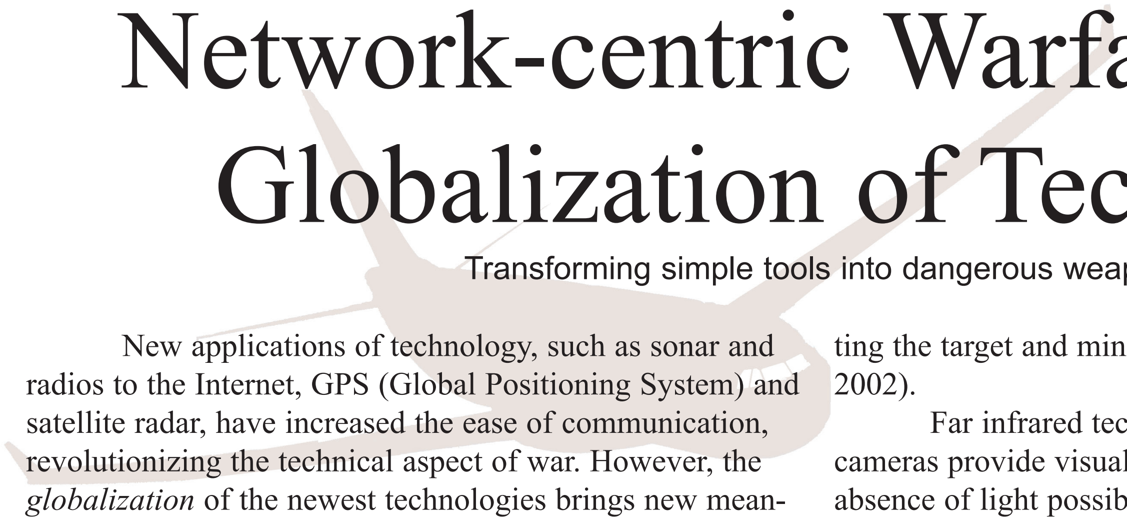

Network-centric Warfare and the Globalization of Technology

Transforming simple tools into dangerous weapons

by Ann Oh

New applications of technology, such as sonar and radios to the Internet, GPS (Global Positioning System) and satellite radar, have increased the ease of communication, revolutionizing the technical aspect of war. However, the *globalization* of the newest technologies brings new meaning to the multifunctional power of these devices, making them no longer exclusive to the government and the military. The utility of such technology is now in the hands of the global masses which can prove progressive, but also dangerous when applied to warfare.

The Changing Nature of Technological Warfare

Efficiency and greater access to technology flattened the chain of military command, giving soldiers on the ground greater access to information in order to calculate their next moves. Some believed that the recent advancements in technological warfare would make war as "predictable as chess" and bring an easy victory (Muller 2002). Unfortunately, the Iraq War exposed the true danger in technological warfare as terrorists wield everyday technology to their advantage. Furthermore, the inability to bring stability to the region shattered the faith in technology to accelerate the process of war and to bring a quick end. The distribution of technology caused by globalization reduces the exclusive advantage of the military by allowing greater access of information to terrorists, enabling them to create vast international networks and have influence on a global scale. Paradoxically, technology does not simplify war; instead, it complicates it further. Therefore, "network-centric warfare" back-fired on the military, preventing rational responses while consuming itself in analyzing massive amounts of data collected to produce a theoretically ideal, yet impractical response.

Common Technology and their Military Uses

GPS utilizes a constellation of twenty-four satellites that transmit precise microwave signals and enable a GPS receiver to determine its location, speed, direction, and time. Most of the bombs used by the U.S. military are JDAMS (Joint Direct Attack Munitions). These are missiles with inexpensive guidance systems attached to their backs. JDAMs use GPS satellites to guide them to previously programmed locations. They are effective and accurate in hitting the target and minimizing civilian casualties (Muller 2002).

Far infrared technology applied to binoculars and cameras provide visuals at night, making operations in the absence of light possible. An MQ-1 Predator, an unmanned aerial vehicle (UAV), mounted with far infrared surveillance cameras, flies over the city to track the motion of troops and enemy activity in urban areas. The UAV can detect whether an automobile or tank engine is running (or has been recently running) solely from the warmth of the engine.

Radar, a system of electromagnetic waves, complements infrared in surveillance. A synthetic aperture radar carried on a Predator can take a radar image of several city blocks with a ground resolution of thirty centimeters. It looks like a sharp photo taken from directly above. Using the new Joint Tactical Information Distribution System, the image is delivered to the ground troops in nearly real time (Muller 2002). This helps the military to better assess the situation. In terms of communication, cell phones – smaller and more reliable than Morse code and radios – have replaced WWI technology to increase connectivity and mobility.

> "...the advent of the internet horizontally streamlined this flow of information for a more efficient and comprehensive response."

The Internet as a Revolutionary Tool

Internet proves to be a critical tool in efficient communication and in the transfer of bulk data of various mediums, such as images and video. Instant communication allows military personnel to be contacted in a matter of seconds, which is critical in obtaining immediate battlefield intelligence. According to Thomas Friedman in *The World is Flat*, the use of basic tools such as the internet flattens the platform upon which the military networks. The streaming video transmitted by the unmanned aerial vehicle is fed instantly to flat-screen TVs in the CIA, the DIA, the NSA, army intelligence, and air force intelligence. Then, each of those analysts can be integrated into a single chat room so they can type their responses to the situation presented on the streaming video. A transcript of the on-going chat can be visualized alongside the viewing screen so that everyone can analyze the scenario together (Friedman 210). This expansive networking enabled by the internet defies distance for the convergence of timely, comprehensive information that may determine the outcome of important situations.

> "The war in the internet age is occurring at a supraterritorial level, one that is above nations in an intangible realm, such as the World Wide Web."

The internet has not only revolutionized the communication among agencies and the military, but it has also "flattened" the military structure. There has been a change from a vertical chain of command to a horizontal one in order to produce the best response. Friedman provides an example in which the air force, before the globally widespread use of the internet, controlled the UAV (such as the Predator) and used their own analysts to evaluate the situation and then report their findings to the army. This is a vertical structure where each segment of the military has exclusive duties and restricted access to information. However, the advent of the internet horizontally streamlined this flow of information for a more efficient and comprehensive response. As illustrated above, this video is not only viewed by air force analysts, but instantaneously shared with other defense agencies in order to receive important feedback and take appropriate action. For Friedman, "my priority is not who controls the video but how do I create a horizontal response system to extract the most intelligence, from all of us, to understand what the video is showing" (Friedman 210).

Civilian Technology as a Double-edged Sword

Inevitably, this civilian technology is not just accessible to the military. The internet as a cheap, effective communication tool is available to everyone with a computer, including terrorists. War is no longer just fought on the battlefield; it has extended into virtual space. Terrorists also have equal access to cell phones, GPS devices, and weapons to utilize in guerilla warfare.

Recent developments in the Iraq War testify to the ingenious use of basic technological tools by terrorists. Wendy Haig, partner at Iron Horse Ventures, which advises companies and governments on technology initiatives, noted, "British troops conducting raids on insurgents in Basra, Iraq, found printouts of aerial maps from Google Earth detailing the coordinates for British camps in the area. Though dated, the maps revealed the locations of buildings, tents, and other vulnerable areas of British forces… sometimes the most simple or obvious tools prove the most lethal" (Haig 2007). This shows the unexpected vulnerability that the military faces due to widespread technologies that have leveled the playing field for both insurgents and soldiers. The increased availability and access to computers and the internet in even remote parts of the world have made these basic tools become unlikely threats. Even cell phones have assumed a different function in war. Cell phones wired to home-made bombs are primary weapons for suicide bombers who have taken many innocent lives and have wreaked havoc in many countries, from Pakistan to Britain.

Ultimately, the spread of technology caused a drastic transformation of the concept of war. The world's governments are venturing into a new frontier of wars fought in an imaginary realm against an invisible and intangible enemy. Internet is cheap and prevalent. It is hard to retrace or track the flow of information, allowing for communication to occur anonymously and undetected. The internet is also a powerful and dangerous tool for terrorists to spread propaganda and violent ideas to many people, expanding their parameters of influence and making a global impact. A war at the international level is one fought between nations, such as the United States and Iraq. It is a war of territories. In contrast, the war in the internet age is occurring at a supraterritorial level, one that is above nations in an intangible realm, such as the World Wide Web. The ideological war raging on the internet is a war of influence, a one-on-one battle of beliefs. Terrorists are now attacking individuals instead of countries. Thus, the war must not only be won on the ground, but also in the minds of individuals in the world.

The presence of technology in an unequal distribution has plagued the army's efforts to stop the insurgents in Iraq. The infantrymen and tank drivers on the front are given finicky, incompatible equipment – primitive in comparison to the gear at the sprawling military bases, where commanders oversee troops. An Army War College report revealed that "an investigation of the current state of network-centric warfare" affirmed that "frontline troops have a critical need for networked gear – gear that hasn't come yet." The report further asserted, "There is a connectivity gap," that "information is not reaching the lowest levels"

http://www.globalsecurity.org/military/systems/aircraft/images/f-15_mk-84jdam_020507_09.jpg

A fighter plane releases Joint Direct Attack Munitions (JDAMs) that are guided by GPS to target locations.

(Shachtman 2006). The military, working in a top-down structure, limits the access of information for soldiers, who must rely on information given from their superiors. This problem has a detrimental effect on the army because the insurgents are stitching together their own communications network. Using cell phones and e-mail accounts, these guerrillas rely on a loose web of connections. Furthermore, they do not fight in large groups that can be easily tracked by high-tech command posts. Military writer Noah Schachtman states that they have to be "hunted down in dark neighborhoods, amid thousands of civilians, and taken out one by one" (Shachtman 2006).

Technological advancements are not flawless, often proving to be cumbersome in hot, rough terrain. The hot temperatures and blinding sandstorms can prevent machines from working. Also, there can be limited internet connection due to a lack of reception in rural areas. Reports of these setbacks include descriptions of units that "outran the range of high-bandwidth communications relays," downloads which "took hours," and "software [that] locked up" (Talbot 2004). Heavy reliance on these advanced technologies hinders the military's ability to function in a wired war.

Predicting the Variables in Technological Warfare Using "War Games"

"Network-centric warfare" is not the key to rapid victory, proving to be quite unpredictable. The dependence on technology, such as sensors, aerial surveillance, and intelligence data collection, causes "terrible situation awareness" according to Talbot (Talbot 2004). The military analysts are too focused on analyzing the details and often ignore the big picture. Malcolm Gladwell in *Blink* reveals how the Joint Forces Command (JFCOM) run war games behind closed doors for the U.S. military to test new ideas about military organization and experiments to devise new military strategies.

Planning for the war game began in earnest in the summer of 2000 when JFCOM brought together hundreds of military specialists and software experts. Two teams were selected and the war simulation began in the huge, windowless rooms known as testbays where computers simulated the firing of missiles and the launching of planes. The Pentagon realized that "no one would be foolish to challenge the United States head-to-head in pure military combat. Conflict in the future would be diffuse." As one JFCOM analyst put it, "Instead of going after war-fighting capability, we have to go after war-making capability. The military is connected to the economic system, which is connected to their cultural system, to their personal relationships. We have to understand the links between all those systems" (Gladwell 2005). While fighting a war, the military has the capability to use computer programs to evaluate the political situation, taking into consideration diplomacy, economy, and social infrastructure.

However, the military put so much focus on data analysis/integration and computer simulations that they forget about practical, instinct driven responses **(**Gladwell 2005**).** They forgot that the enemy could use guerilla tactics and primitive methods of combat that may catch them off guard. These war games illustrated that the military was so caught up in the mechanics and the process that they never looked at the problem holistically (Gladwell 2005). Regardless of the results from the test of the "network-centric warfare," it is utilized today in the Iraq War and is perhaps attributable to the difficulties that the military faces in restoring order and peace in the region.

The development of technology itself provides advancements in technical warfare, but the *globalization* of technology has opened a new frontier for the course of a war fought with new methods. Technology – such as GPS, sonar, radar, and the internet – has many advantages for it increases the efficiency of combat and connectivity; but, it also creates many variables. It can give equal technical power to terrorists who use such civilian technology to their advantage. War is no longer isolated to the battlefield, forcing the military to approach warfare in the virtual realm. Therefore, the advancement and globalization of technology provide many advantages, but also present greater challenges to victory.

References

Friedman, Thomas L. 2007. *The World is Flat: A Brief History of the Twenty-First Century*. New
York: Picadour.

Gladwell, Malcolm. 2005. Blink*: The Power of Thinking without Thinking.* New York: Little,
Brown and Company.

Haig, Wendy. 2007. Googled by the Enemy.
http://www.businessweek.com/technology/content/feb2007/tc20070206_129775.htm (accessed November 14, 2007).

Muller, R.A. 2002. War with Iraq – Predictable as Chess. *MIT Technology Review*.
http://www.technologyreview.com/Infotech/13014/page2/ (accessed November 14, 2007).

Schachtman, Noah. 2006. Winning—and Losing—the First Wired War. *Popular Science.* http://www.popsci.com/popsci/technology/1b1a2fe0df34b010vgn-vcm1000004eecbccdrcrd.html (accessed November 14, 2007).

Talbot, D. 2004. How Technology Failed in Iraq. *MIT Technology Review.*
http://www.technologyreview.com/Infotech/13893/ (accessed November 14, 2007).