## Should the United States develop and employ strategic information warfare capabilities?

Information technologies have transformed U.S. and, indeed, international society. The ways we socialize, educate and inform ourselves, engage in business and practice our religions have been changed, and in many cases now rely, on digital information and communication. Can warfare—the defense and promotion of our national security and interests—be exempt under any circumstances from developing and employing the latest information strategies? Is this even a choice in the 21st century, much less a hard choice?

Information warfare has been variously defined by different analysts but a standard general definition, as provided by the U.S. Air Force is "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against the actions and exploiting our own information operations." The goal of information war is now frequently described as "information dominance." (1) Major General Kenneth Minihan, stated, "information dominance is not 'my pile of information is bigger than yours'…It is a way of increasing our capabilities by using that information to make right decisions, (and) apply them faster than the enemy can. It is a way to alter the enemy's entire perception of reality. It is a method of using all the information at our disposal to predict (and affect) what happens tomorrow before the enemy even jumps out of bed and thinks about what to do today." (2)

### Pro:

Information warfare is not a new concept that arose with the Internet. Information has always been a decisive factor in deciding the victory or defeat of one military force over another. The rapid conclusion to the Gulf War is attributed at least in part to superior information technology, particularly the use of off-the-shelf Global Positioning System (GPS) technology to orient troops and coordinate simultaneous attacks, even in the midst of sand storms, which severely hampered Iraqi troops native to the desert environment. In addition, communication technologies were networked as never before, allowing the tight coordination of simultaneous or near-simultaneous attacks. According to Colonel James W. McLendon, "satellites, microwave and landlines handled 700,000 phone calls and 152,000 messages a day. ..11 Airborne Warning and Control System (AWACS) aircraft controlled 2,240 sorties a day, more than 90,000 during the war with no midair collisions and no friendly air engagements." (3)

The decisive role that information technology played in the defeat of Nazi Germany in World War II may be less well known. Enigma, the encryption technology of Nazi Germany, fell into Polish hands and was solved in the 1930s, shortly before an open declaration of war. Polish dissidents provided the Enigma machine to England in the early days of the war. In July 1940, Enigma decrypt provided early warning of German plans to invade Britain. By 1944, 90 percent of European intelligence summaries provided to the United States were based on Enigma-derived information. (4) The German Navy used the Enigma machine to manage their highly successful U-boat program. The Allies used the Enigma decrypt to successfully locate and destroy so many U-boats that the German submarine warfare program was completely overthrown, thus further insuring an Allied victory in the European theater.

Enigma is just one of many illustrations of a universal truism: "information is power." There is no question that information technologies have played a critical role and will play an increasing role in all warfare strategies—not just for the United States but for every country. The role of cyberwarfare in the successful conclusion of the Gulf War was a wakeup call for any country paying attention, and they were all paying attention. Unlike weapons of mass destruction, cyberwar has a very small footprint. It requires considerably less resources, utilizes readily available expertise and doesn't carry a major moral stigma--the sense that a country is placing itself beyond the pale in the international arena--that the use of a nuclear, biological or chemical weapon carries. The hard choice before us is not **whether** we use information warfare as a strategic weapon, but **how.**

Perhaps the most devastating innovation to modern warfare is the development of weapons of mass destruction—nuclear and biochemical weapons with the capability to destroy whole armies, cities, even nations. If a country with access to a WMD were to use that weapon against United States troops, the casualty rate would almost certainly be unacceptably high. The result could be a massive defeat with devastating consequences to U.S. national security and defense.

Most analysts agree that if battle against a country with WMD capability cannot be avoided, it must be swift and must result in destruction of WMD stockpiles and staging areas and in strategic paralysis of the enemy so that the enemy is incapable of retaliation using a WMD. This strategic paralysis would probably require a swarm of simultaneous or near-simultaneous attacks directed at critical points of failure for the enemy. Simultaneous or parallel attacks require information warfare technologies, particularly superior electronic communications to coordinate staging, to change strategies in response to enemy countermeasures and to insure that swarms of armed troops attack the enemy and not each other.

In addition, information warfare techniques can be used to mitigate against an imminent WMD attack in many ways. Infiltrating enemy information networks and decrypting their encrypted communiques can be used to discover hidden manufacturing and staging facilities, such as dual-purpose plants that manufacture agricultural products and biochemical weapons. Disinformation techniques can be used to send seemingly private communications intended for interception that deceive the enemy about our ability to retaliate or to deflect an intended attack to an area where the least amount of human damage and geographical contamination will occur. If even the possibility of a WMD attack exists, advanced information technologies must be used to try to prevent or mitigate the damage of such an attack.

Perhaps most critically, the introduction of WMD into warfare means that additional strategies are needed to safeguard soldiers, including the moving of as many troops as possible out of harm's way while still engaging the enemy in battle. This involves an increased use of unmanned aircraft and other distance weapons and more reliance on advanced detection systems to discover and destroy enemy missiles before they reach their intended targets. Information warfare can be engaged in from vast distances, even from the continental United States, where civilians and nontraditional soldiers (retired soldiers or those with physical disabilities) can enhance and to some extent even replace the country's shrinking armed forces.

Information warfare technologies don't involve mass casualties and injuries and thus are more acceptable with the American public and in the court of international public opinion. Given the numerous information media capable of broadcasting graphic images in near real time from any battle, a warfare technique that not only does not provoke adverse public opinion but that is also, as evidenced in the Gulf War, a considerable source of national pride, is a critical strategic weapon to employ. Armies do not declare war, politicians do. And in the United States, politicians require public support to remain in power. Information warfare techniques which do not result in massive casualties and destruction on enemy soil are also considered by some analysts to be less likely to provoke the unleashing of a nuclear, biological or chemical weapon as opposed to massive strikes by conventional missiles.

Finally, information warfare as a strategic initiative is multifaceted and multipurpose. Advanced electronic surveillance technologies can be used to identify and neutralize potential conflicts or weapons of mass destruction facilities. Information warfare, as discussed above, plays a critical role in every aspect of warfare during a conflict. The role of information technology after a conflict is equally critical although not as thoroughly discussed. Information technologies can play a critical role in monitoring a defeated country for compliance with the terms of surrender, particularly with regard to eliminating weapons of mass destruction. Information technologies can also be used to rebuild societies that have been devastated by warfare, particularly to manage the logistics of feeding refugees and rebuilding the physical infrastructure.

"Must we have war at all?" remains the fundamental question that the world's civilizations must ask. Until all nations answer that question in the negative, however, "must we have information warfare?" can only be answered with "yes."

Con:

Conventional warfare techniques, involving missiles and munitions, while devastating in their consequences to individual soldiers and to civilians in the line of fire, have easily understood and predictable consequences. Warfare has probably existed since the emergence of rival prehistoric tribes and its traditional structure of attack and retaliation has been understood and even accepted by both sides. The outcome of a war has had the potential to determine the survival of individual societies, but until the advent of weapons of mass destruction, warfare has not threatened the continuation of civilization itself.

Information warfare technologies have been embraced by countries, including the United States, as a strategic technology contributing greatly to a successful outcome, even in the event that the enemy possesses a weapon of mass destruction. The United States is already engaged in research and development for advanced information warfare capabilities. The soldier of the 21st century is less likely to be slogging through the jungle and more likely to typing at a keyboard. Instead of freezing at the sound of a breaking twig, (s)he will be monitoring enemy movements on a handheld GPS device and relaying those movements instantly to commanding officers. What's wrong with this picture? If we must have war at all, why not a war that is as efficient and bloodless as possible for American troops?

In the rush to embrace these technologies, little attention as been paid to their long-term consequences--the ability of information warfare technologies to transform—even to dismantle—the society that produces them. Perhaps the most dangerous information warfare technology is disinformation. In past wars, disinformation involved elaborate hoaxes requiring considerable time and effort to develop, such as the creation of an entire imaginary army, the First U.S. Army Group, purportedly under the direction of General Patton , which successfully deflected some German troops from the invasion of Normandy. (5)

Current technologies, which allow undetectable editing of digital images and the creation of virtual reality and augmented reality that is part real, part simulation, can now be used with great effect for disinformation. For example, a simulation of an enemy leader can be broadcast to convince the enemy country that its leader has surrendered. Massive virtual casualties depicted in a digital video can persuade panicked citizens that whole cities have been destroyed. In addition, information warfare technologies can disrupt communications, transportation, heating, and water supplies, demoralizing an enemy country and rending its army helpless without massive death and destruction. Information warfare, effectively and massively deployed, could at last bring about the war that is won without firing a single shot.

The United States, like other countries, has a long practice of migrating warfare technologies to civilian uses. The Internet itself began as a defense network. In addition, information technologies such as GPS are often developed as dual-purpose technologies—locating fish in the ocean for fisherman or enemy troop movements in a battle. The use of virtual or augmented reality techniques to distort reality and subvert truthful communication, if acceptable for use in war, will be adopted in U.S. society, perhaps to sell a product or attract followers to a cause. . Adoption of digital disinformation by the government legitimizes its use.

Digital editing techniques can be imperceptible to the naked eye. At its core, a society is a congregation of people who share a common view of reality. What will be the consequences to society when you cannot trust what you perceive with your own eyes and ears, when those in positions of power can deceive others without detection? Information warfare produces no immediate human casualties, but can society tolerate a warfare technology that destroys its integrity?

A key problem with cyberwar technology is that, as Blaine Burnham, Director of the Georgia Tech Information Security Center stated, "that thing that you ship (down the information pipe) is now loose." Digital technologies frequently remain resident on the computers and networks they attack. Bit capturing devices can also identify, capture and study these technologies in transit. According to Burnham, the period of time between use of a weapon and the time when it is re-engineered and turned against the country that first used it is known as the "reflect time." He noted that the reflect time for nuclear weapons was almost a decade, for biological and chemical weapons was even shorter and for information warfare could be months, weeks, even days. (6) Viruses, worms and other malicious software, if used to disrupt enemy networks, could be studied, modified and easily used not just against U.S. troops but against U.S. society at home. More than any previous warfare technology, information warfare has the ability to bring the conflict quickly and severely to American soil.

In addition, information warfare may not be the safest or most efficient of methodologies for conducting war. The blowback factor should not be underestimated. The atomic bomb left nothing to be studied and no enemy troops at the scene capable of retaliation. As mentioned before, information warfare technologies remain resident or can leave a trail that can be studied by enemy troops and since it produces no physical injuries, the troops are physically capable of retaliation. Information warfare may result in a flurry of attacks and counterattacks that exhaust both parties. In addition, retaliation could target vulnerable areas, such as the continental U.S. or centralized command and control facilities. The United States has the greatest reliance on networked information technologies of any country in the world, making us extremely susceptible to blowback attacks.

The current U.S. development and deployment of information warfare technologies has many analysts worried that we are creating increased vulnerabilities for our armed forces in the event of a battle. The U.S. currently relies to a great degree on commercial off-the-shelf technologies (COTS) that can be readily purchased and studied for weaknesses by enemy countries. The increasing reliance on GPS technology since the Gulf War has resulted in a worrisome possible single point of failure that could either be destroyed, or perhaps worse, subverted with false readings, by enemy troops. The extensive reliance on a heavily networked information infrastructure for battle coordination and logistics conversely supplies many points of failure for attack by enemy troops.

Information warfare may become a critical weapon in the next conflict, but unless critical weaknesses are addressed, it may greatly contribute to the destruction of the military forces and of the society itself that it was developed to defend.

**Questions for Discussion:**

1. Deception has always been an important wartime strategy. Churchill and Roosevelt both allowed attacks against their own troops to occur in order to protect espionage and surveillance sources and thus promote a quicker peace. In the 21st century, however, the tools of deception can exist on anyone's desktop and can create undetectable illusions. Can U.S. society tolerate digital deception as a warfare strategy? Do the ends justify the means?

2. Is information warfare truly a "bloodless" weapon? Some uses of information warfare--to delete vaccine inoculation records, so that people are unprotected from a biological weapon or to jam air traffic control facilities—can produce an indirect or even a direct body count. Can you think of others? Does information warfare seem like a better strategy than a missile attack, with regard to the outcome for the victims? Why?

3. A key benefit of an information warfare strategy is the ability to expand the concept of the "soldier" to incorporate those traditionally denied military service because of age or disability. What are the benefits and the drawbacks of "cybersoldiers" working from desktops in the United States?

4. Information warfare provides amazing technologies to the soldier or the airman in the midst of battle. However, reliance on these technologies can mean that if a system breaks down, the battle breaks down. How critical is this problem? What back up plans should the military have if a GPS system breaks down, for example, leaving a platoon lost in an unfamiliar country?

5. If the U.S. government develops information warfare software to destroy enemy computers and that same software "reflects" back to the United States,

destroying many commercial and home computers, should the government have any liability for the consequences?