# Cyber’s impact on military strategy

www.armyupress.army.mil/Journals/NCO-Journal/Archives/2016/November/Cybers-impact-on-military-strategy/

**By Staff Sgt. Matthew Tinsley**
**782nd Military Intelligence Battalion**

November 22, 2016

Within America’s military “cyber” has held status as a powerful buzzword for many years. At all levels of military planning and operations, leaders of units have tried to get a piece of the cyber pie and integrate its concepts into their operations. One of the central questions that has persisted around cyber is how and to what extent will cyber conflict require a reconsideration of strategy. The military exists largely in two broad areas: the strategic level of long-term and large-scale planning, and the tactical level of smaller-scale, short-term operations. Cyber will undoubtedly have an effect on both of these operational domains.

When examining both domains, cyber’s effect on strategy can be examined from a short-term and long-term perspective. The military’s strategic level deals with long-term plans crafted at high levels of leadership. Strategic plans tend to address questions dealing with conducting entire war campaigns. From this perspective, in the short term, new cyber capabilities will require little reconsideration of the basic strategies the military employs. The Department of Defense’s mission is overall national defense, primarily from foreign adversaries. That has not and will not change. Even in the 2015 release of the DOD’s cyber strategy, Defense Secretary Ash Carter compared challenges posed by cyber to old Cold War challenges. The reason for this is that, initially, new technology is viewed from the perspective of what is familiar to the user. The military as a whole simply took cyber and used it to optimize its existing strategies and methods. Cyber has been used in new avenues of foreign intelligence, it gives commanders new ways to view battlefields and it has been integrated into weapons systems. But the base strategies the military employs have yet to really change. The most notable short-term change comes from the military’s job to defend the United States. In the past, attacks on U.S. soil and U.S. infrastructure the military needed to respond to were few and far between, with 9/11 and Pearl Harbor being prominent instances. But with the ever-increasing worldwide

connectivity in the digital age, American infrastructure, government and industry are constantly open to attack from foreign entities and governments. The result is that for some military components, actively defending the United States is a full-time job.

Long-term changes, on the other hand, have the possibility of prompting a massive change to military strategy. The world has already seen hints of possible cyber strategy for the future. Between 2011 and 2013, Iran initiated cyber attacks on U.S. infrastructure, including banks, dams and educational institutions. Although the attacks were minimized, they showed the potential for damage to the nation. One bank, Zions Bancoporation, lost more than $400,000 while its website was down for only two hours. If larger institutions or a large number of financial institutions were targeted for long periods of time, the financial damage could be upward of millions or billions of dollars. Iran targeted infrastructure that could cause physical damage as well. The Bowman Avenue Dam in New York was breached by Iran hackers to the point where they could have controlled sluice gates that hold back water. Luckily, the controls had been manually disconnected for maintenance around the same time, which prevented the Iranian hackers from actually having control over the dam. More devastating cyber attacks were seen in 2008 during the Russo-Georgian War. Russian cyber attacks were coordinated with the Russian invasion of Georgia. As the Russians advanced into the country and fighting ramped up, so did the cyber campaign. Given that it was 2008 and Georgia had a relatively basic technology infrastructure, the Russian attacks were mainly designed to cause confusion during their ground campaign. But given the current situation in the Ukraine, the Russo-Georgian War seems to provide warnings when examined in hindsight. The question for the future is how advanced and efficient these techniques can become. Will we see the capability to shut down entire power grids, communication structures, water systems or dams? If so, and if we do not maintain the ability to defend them, the devastation from such cyber attacks could start and end wars before any ground troops are deployed or kinetic weapons are fired. At the very least, cyber capabilities will become more integrated into strategic plans as the world continues to become more reliant on technology and digital communications.

The tactical side of the equation is relatively stable. In the short term, the strategies employed by ground troops in their operations will remain the same, while new cyber-based capabilities are employed to support those operations. One of the most visible integrations we see today is the ability to quickly and accurately locate targets. Especially given the often chaotic state of urban warfare — where a mix of friendly, hostile and neutral elements are all intermixed — the ability to quickly and accurately characterize all three groups is vital. In reality, the military has been integrating these capabilities into ground operations for a while, but incorporating them into the everyday unit on a large scale is the new challenge. In October of 2015, the Army tested these capabilities on a large scale with a cyber validation exercise that occurred at Joint Base Lewis-McChord, Washington. The 780th Military Intelligence Brigade provided cyber capability support to the 2-2 Infantry Division and the 201st Expeditionary Military Intelligence Brigade. Traditional military units were able to provide adequate support and protection to the cyber elements that aided in target identification and verification. This type of cyber support is used in many other instances, such as drone targeting, and has been used not only for identification of high-value targets but has also aided in identifying and tracking hostages. None of these ideas or strategies are really new, but cyber is accomplishing them in new ways and, at times, accomplishes them more accurately, making ground troops' job easier and safer.

Long-term changes are dependent on the type of technological changes that occur in the future. The drone program has become one of the most visible — and for some, the most concerning — use of modern technology in military operations. Currently, the drones are just planes with no physical cockpit, and the actual act of targeting and firing upon targets is controlled by humans. But many are already talking about the possibility of letting drones be fully controlled by computers. These drones would draw on intelligence sources, verify targets, make decisions about risk and decide whether to fire, all without a human's direct input. These weapons are actually pretty easy to make and have been made already. The questions about implementing these into normal everyday operations come down more to ethics than capability. Should computers be deciding who dies? Are computer databases of laws and treaties good enough for a computer to cross-reference and then decide if international law can be breached? Who is accountable if the computer makes a mistake? At this point, the consensus is that this is a terrible idea. An open letter was presented at the opening of the International Joint Conference on Artificial Intelligence in 2015 warning of the dangers of

weapons under the control of artificial intelligence. This letter was endorsed by the likes of Elon Musk, Stephen Hawking, Steve Wozniak, and more than 40 robotics researchers from around the world. Even the DOD decided to address this topic years ago with DOD Directive 3000.09, which stipulates that all weapons systems must be designed to have “appropriate levels of human judgment over the use of force.” From this, it seems that in the future, cyber will not replace or eliminate the need for human ground troops. How extensively cyber gets integrated with tactical operations has yet to be seen.

Cyber, like all new forms of technology, has affected all aspects of our lives, and the military is not immune from its influence. Computer technology has been integrated into the lives of everyone from the commander in chief all the way down to the enlisted Soldier on a patrol. How far this integration goes in the future is really up to the imagination of technology inventors and innovators. For now, cyber seeks to make the lives of Soldiers easier, more efficient and safer.