Sticks and Stones – Training for Tomorrow's War Today

By Dr. Aaron Brantly, COL Thomas Cook | March 01, 2016

PRINT

'I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones.' – Albert Einstein

Technology is great, when it works the way we want it to. Over the last couple years it seems the ever-mounting stream of hacks could leave even the most stoic of technologists cringing. As researchers at the Army Cyber Institute at West Point, our task is to be forward thinking and anticipate the hill after next. We are one part of the Army's robust effort to address cyberspace issues of today and tomorrow. Along with our cross-service and cross-agency partners we are making progress: we are working our way through a highly disruptive era in technology and politics to find solutions ensuring the security of the United States. At the same time, as we step forward into the complexity of a fully integrated future, we must not lose sight as a military of the fundamentals of fighting and defending the security and interests of the nation. The more the tools and gadgets of modern warfare are challenged by state and non-state actors, the more critical it becomes that our men and women in uniform maintain the fundamental skills of warriors from previous generations.

Networked warfare and cyber warfare are but two of many catch phrases of the last couple of decades rising to prominence. These are concepts that we must continue build on to improve our precision, coordination and efficiency as defenders of the nation's security and interests. Yet despite these advances, the US military must also be prepared to operate in a world where the lights do not turn on, engines do not start, and all our efficiencies leave us with only the rifle in our hands. Our ships, armor, aircraft, satellites, and almost all other military systems are highly dependent on digital systems vulnerable to attack.

As a nation, the US must expect the unexpected by training our military to perform in the absence of technologies they have never lived without. Our incoming officer and enlisted corps are digital natives: they leverage GPS, laser guided munitions and other modern tools expertly. But as recent hacking incidents on cars, ships, supply systems, GPS, and even aircraft indicate, the diversity of threats posed to our systems are immense. While calls to fix the code and secure the systems are being heard loud and clear. The Army and other organizations like ours are working day and night to solve a persistent stream of cyber challenges It is important to remember that we are solving problems as our cyber surroundings change under our feet.

As we write better code, build more robust hardware and develop better cyber warriors for both offensive and defensive operations, our ability to observe, orient, decide, and act across the services and within them will become more robust. At the same time, we must recognize that we are creating puzzles that others will try to solve and that eventually, given enough time, energy and luck, most puzzles are solvable. Technology has enhanced the capabilities of the Army and her sister services. Under the continued direction of President Obama, Secretary Carter, and foresight of Admiral Rogers and Generals Alexander, Cardon, Hernandez and many others, we as a nation have established the foundations of a robust national approach to cybersecurity. This is an evolving process and the Department of Defense (DoD), Federal, state, local, and private entities will necessarily continue to build capabilities improving our aggregate resilience. The problem of cybersecurity is not isolated to the DoD alone and as a nation we must work together to strengthen our mutual security and resilience.

Across the armed services there is a yet another need, specific to our profession. Just as medieval castles layered their fortifications, so too must we train and develop redundancies in our men and women and the systems they use. These redundancies should be well adapted to a world in which the technology we have grown so dependent on fails us. The services must recognize that our need to train in, and for, cyberspace related conflict does not obviate necessary skills found in the historical foundations of military arts. Skills such as celestial navigation, non-computer aided mathematics and many more are critical to maintaining operational effectiveness in the absence of the tools upon which we now so often depend. Robots, drones, and all the science-fiction that has become science-fact is nothing compared to the determined will of a well trained and educated, highly motivated and creative Soldier.

PRINT