EXECUTIVE SUMMARY

INTRODUCTION

The 11th annual "Mad Scientist" Future Technology seminar from 20 – 23 January 2010 addressed the challenge of blended S&T surprise. Specifically, it brought together a dynamic group of scientists, science fiction writers, futurists, academicians and students from the private sector and government to look into the future and explore ideas about the "blending" of science and technology in ways that might challenge the United States. This executive summary provides an overview of the judgments, insights and implications from that seminar.

BACKGROUND

The blending of sciences and technologies by "combining, modifying, harnessing or adapting them in creative ways" has enabled the creation of asymmetric advantages and the ability to render existing capabilities irrelevant. This is a trend almost certain to continue and expand into the future. In order to investigate this trend, four panels of experts were established. Each panel was asked to identify and articulate the nature and potential of the blended technologies they identified, explain their rudimentary components, and provide timelines for their possible development and or employment. Ultimately, it was our desire to look at these technologies from a "Red" perspective and identify potential threat capabilities.

KEY JUDGMENTS

The most significant findings from the seminar are provided below.

- The blending of ***emerging biological technology*** with ordinary human delivery methods, especially in the hands of non-state actors, has the greatest potential to catch the Army unprepared in the short term. ***As early as 2015, we assess that bioengineering will allow adversaries to modify diseases and tailor organisms to produce pathogens against which there is no existing defense or treatment***. This capability may soon be available for less than $5000. A realistic example would be to alter a naturally mutating flu virus. A deliberate modification or creation of such a flu virus could be weaponized for multiple purposes; from debilitating a military force to creating an epidemic that overwhelms a nation's response capability. While there are still significant questions as to what engineered pathogens will really do, the threat of their use by any adversary, from competing nation states through super empowered individuals, is real.

- While certainly not a new phenomenon, ***the emerging threat from electro-magnetic pulse (EMP) weapons, are likely to provide a significantly new challenge***. EMP is the phenomena most commonly associated as a side effect of employing nuclear weapons that destroys electronic systems. However, nuclear detonation is not required to create the effect. ***Blending the technologies necessary to generate an EMP with advances in miniaturization could produce a hand held EMP gun before 2020***. In the more near term, radio frequency weapons currently under development in Europe are already capable of emanating radio waves that could potentially damage the full range of command and control systems from communications to target acquisition systems currently under development. It is expected that EMP weapons will become available to potential adversaries in mortar and artillery rounds soon.

- The ***integration of man and robots*** is already occurring in the conflicts in Iraq and Afghanistan. In the midterm, robotics will continue to advance, especially in Russia, China and India, based upon improvements in nanotechnology, networking and advanced computing/artificial intelligence. ***One of the most significant impacts of this blending will be the flooding of the battlefield with swarms of miniature corrosives, sensors, and explosives that will have the capability to disrupt tempo and cause severe casualties – a more lethal descendent of today's IED***. While powering and computing for swarms remains a challenge, their introduction by our adversaries will pose multiple dilemmas for the Army, including access to and maneuver on the battlefield. Another aspect of robotic swarms is the potential to change the signatures currently associated with them, making them even more difficult to recognize and defeat.

- Increasing ***dependence on social networking systems blended with significant improvements in immersive 3-D technologies will change the definition of force protection and redefine the meaning of area of operations***. Social networking could make the family and friends of Soldiers real targets, subsequently requiring increased protection. Additionally, the mashing of these technologies could potentially hurt recruitment and retention efforts. Some of our more advanced potential adversaries, including China, have begun work in the social networking arena. However, future blending of social networks and Immersive 3-D technology makes it increasingly likely that engagements will take place outside physical space and will expand the realms in which Soldiers are required to conduct operations.

- One of the most disturbing findings was a collective assessment that science and technology was driving potential enemies away from directly attacking the Army. ***The increasing difficulty in protecting information, when merged with the cyber capabilities of super empowered individuals,*** could redefine adversary targeting methods; shifting toward a focus on disrupting transportation, banking, and government infrastructure within the United States and attempt to disrupt the flow of US forces at the strategic level – changing the nature of anti-access at the strategic level and generating greater stress in an increasingly vulnerable U.S. homeland. Russia, China, North Korea, and Iran have robust cyber programs that may be indicators of the difficulties we will face in this arena in the future.

EXECUTIVE SUMMARY

EMERGING INSIGHTS

Insights discussed at the seminar that require examination as we consider S&T within the context of the operational environment are outlined below:

The United States and the Army have significant vulnerabilities that are recognized by our enemies and potential adversaries. Some of these perceived vulnerabilities include: a heavy reliance on automation and the cyber domain; the requirement to sustain military operations over long distances; continued reliance on foreign entities for our own S&T infrastructure and baseline research and development (R&D); dependence on foreign sources of energy, and vulnerable domestic infrastructure. Recognizing that they may be required to compete at some level with the United States, adversary S&T developments can be expected to target these vulnerabilities.

Developments in the field of Nano-energetics represent an emerging "IED challenge". Nano-energetics is essentially the blending of enhanced conventional explosives utilizing Nano-technology to bridge the existing gap between standard chemical reactions. Ongoing work in this area could provide our adversaries with Nano-energetic explosives that may have up to 10 x the power of their traditional counterparts, making them a type of future enhanced "explosively formed penetrator" that will revolutionize ballistics and ordnance.

The blending of precision technology with stealth technology has the potential to increase the effectiveness of precision capabilities. A harbinger of this capability, the "blue dart", was able to make its way through a series of protective barriers to conduct a successful simulated attack against a warship. The current assessment of the operational environment calls for our increased need for precision, while adversaries need to counter precision as a means to "ensure survival and erode an adversary's will over time. Current investments by potential adversaries are likely to enhance this capability as well as challenge current force protection capabilities.

The growing number of foreign scientists and engineers will challenge U.S. technological superiority in the future. Most research and development is conducted overseas. Information networks increasingly facilitate collaboration and the exchange of ideas will enable advancements in unexpected places. From pharmaceuticals to Nano-technology, it is only a matter of time before there is a significant high tech surprise awaiting U.S. military forces.

In the far term, beyond 2030, developments in neuro-cognitive warfare could have significant impacts. Neuro-cognitive warfare is the mashing of electromagnetic, infrasonic, and light technologies to target human neural and physiological systems. Weaponized capabilities at the tactical level will be focused on degrading the cognitive, physiological, and behavioral characteristics of Soldiers. Its small size and localized effects will make it ideal for employment in urban areas. Such technology could be employed through online immersive environments such as 2d Life or other electronic mediums to surreptitiously impact behavior without the knowledge of the target.

The far future will see a reduction in the importance of kinetic effects in warfighting. As advances in technology make it easier to control others through indirect and virtual means, adversaries will invest less in traditional kinetic type weapons systems. Ongoing adversary investments in cyber, space, and non-lethal capabilities will continue and whenever possible will be used with great effect. Current S&T investments show that within the next 25 years kinetic action will become more and more limited. Kinetic action will be used to support other types of non-kinetic operations that will increasingly come to represent the main effort.

IMPLICATIONS

The seminar identified four significant military implications during this session. These implications are outlined below:

1. The employment of EMP weapons is becoming increasingly likely. EMP attacks have the potential to isolate individuals and organizations by denying them the ability to acquire information, communicate and conduct coordination. Especially vulnerable are Soldier and vehicle C4I systems.

2. Biological warfare capabilities are expanding rapidly. Consequence management and the vetting of personnel will become increasingly important as human delivery remains the most likely and efficient means of delivering biological toxins to the force. Correspondingly, there are increasing requirements to develop sensors and analytic capabilities to detect both biological and chemical agents.

3. The infusion of both ground and aerial robotics into military operations will increase in the future. However, primarily the purview of nation states, non-state actors are exploring and acquiring robotics.

4. The "dark web" of the internet provides an increasingly important capability for adversaries who can use it to command, control, and conduct operations. Developing technologies, including social networks, provide fertile ground for the blending of capabilities and placing the Army and its families at greater risk.

THE WAY AHEAD

The panels examined a number of current and future technologies that have the potential to be blended and present significant challenges, as well as potentially cause surprise. While there is room for debate about which technologies can and will be blended, what is certain is that the nature of warfare is changing; shifting increasingly from large scale, kinetic solider-on-solider operations to decentralized non-kinetic operations reliant upon cyber networks, robotics, and/or electronic media to achieve their desired effects. Limited resources, financial or otherwise, make it increasingly difficult for nation states to fund 20th century industrial based warfare. While conventional warfare is by no means obsolete, 21st century warfare will be defined by the adversary's ability to blend existing and nascent technologies as a means to resist or disrupt a numerically or technologically superior force.

The real work of further exploration of these topics and developing solutions lies ahead. The results of this analysis will be used to update the Army's understanding of the future Operational Environment and threats it is likely to contain.