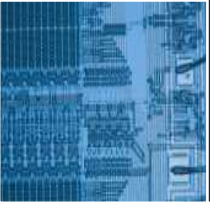


2009

Cyber Warriors

Limited resources increases the risks!



Cyber Warriors Wanted

Each and every day, each and every hour, cyber attacks are waged against a wide variety of targets on millions of computers and networks around the world. These battles rage twenty-four hours a day, seven days a week each and every day of the year. Back in the spring of 2007, U.S. Strategic Command Chief General James E. Cartwright told Congress that "America is under widespread attack in cyber space." In addition, officials in Europe have not hesitated to highlight the growing cyber warfare threat.

For many years, observers believed that the balance of cyber war power was tipped in United States' favor. However, there is strong evidence that this has or is changing. That being said, China, Russia, Iran and India are quickly closing the gap. Now some experts say we are no longer number one - we are number three. The United States has a sophisticated information-warfare program under the control of the Department of Defense (DoD) and growing cyber defenses under the watchful eye of the Department of Homeland Security (DHS).

Most military services in the U.S. have focused on using cyber space for intelligence gathering and monitoring. The most advanced at this is the National Security Agency (NSA). Recently the focus has been expanded to more than intelligence and now includes offensive and defensive capabilities as well as for counter intelligence activities. As the cyber warfare threat environment evolves, new career opportunities will be created. We have seen a very broad spectrum of positions in the cyber warfare domain.

The top three (most frequent openings) job areas are identified below.

Cyber Intelligence Analyst This position is responsible for reviewing and assessing all cyber intelligence gathered by various intelligence agencies and conducting analysis and production of intelligence reports. In addition, the position will identify intelligence gaps in reporting and provide constructive feedback to enhance intelligence gathering performance.

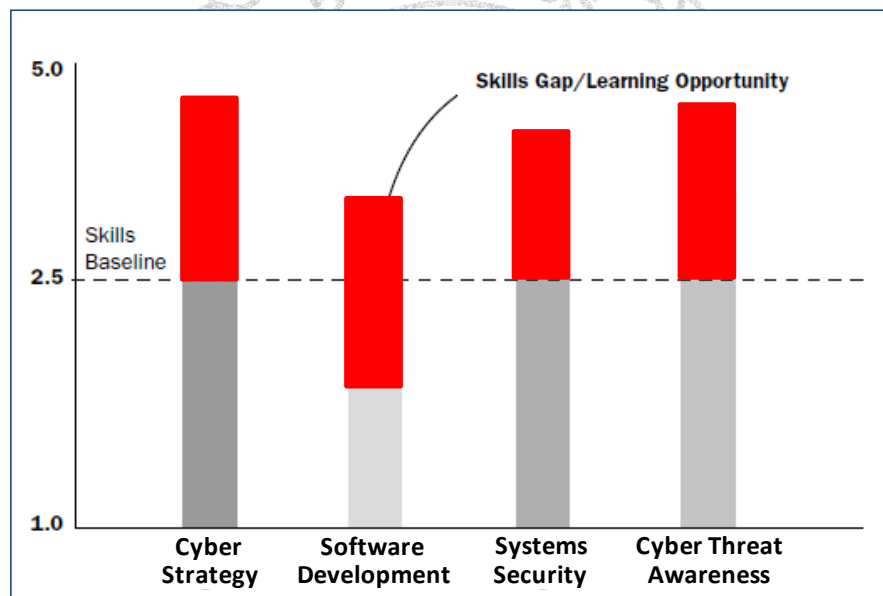
Cyber Operations Director This position is for developing strategies for cyber warfare operations, plans, goals, objectives, priorities, missions, and timelines to execute cyber warfare missions. This officer level position will assist in planning and directing actions for the full range of cyber weapons deployment against computers and network operations.

Cyber Weapons Specialist This technical position will provide technical direction within a team of software developers, software engineering and systems integration personnel that create innovative offensive cyber attack capabilities. In addition, the responsibilities will include identifying and developing cyber software that provide a strategic advantage in the area of cyber warfare/information operations.

One source inside the DoD told us that cyber weapons and defense systems require our service personnel to receive current and relevant training and maintain their level of competency as the threat environment changes. This will insure they are capable of fighting and winning within the domain. Education and training are the foundation for security in this highly technologically advanced military environment. However, this is a huge challenge for the United States and many other countries. These resources are in high demand in the corporate world (private sector) and the increased demand from the military and government (public sector) will make attracting and retaining these resources a challenge.

Critical Skills

When the military creates these new offensive and defensive weapons systems and the cyber intelligence collection capabilities necessary to address this growing threat, they will require employees with skills in these four critical areas.



The gray areas represent the current skill levels in the general technology workforce and the red areas indicate the skill level required in the cyber warfare domain. This simplified example shows how large of a gap exists in the critical skill areas militaries need now. Strong demand for IT labor should continue all but unabated in this downturn economy. As technical talent becomes scarce, military officers must pull out all the stops to attract and keep cyber warriors. Cross-training will be critical to keep resources engaged and will help mitigate the risks of these resources being drawn by the private sector.

In the private sector, the jobs that IT hiring managers say will be most difficult to fill in 2008, due to a lack of workers with that particular skill are listed below.

1. Data management experts
2. Software developers
3. IT security workers
4. Project managers
5. Network managers
6. Help desk staffers
7. Storage administrators



SOURCE: Computerworld's first-half 2008 Vital Signs Survey

This clearly indicates both the military and the business community are looking for the same scarce resources. Since the talent pool for certain IT skills is expected to remain shallow, many believe the stringent requirement for obtaining a security clearance may need to be relaxed. This is a hotly debated solution to the problem and there is no indication that this will take place any time soon.

A military's ability to be successful in the continually evolving and technically challenging cyber threat environment is highly educated resources at all levels and this is even more the case in the cyber warfare domain. Brian from Spy-Ops tells us that, "A new breed of military officer needs a broad based training program in the cyber area in addition to particular areas of expertise." He went on to explain that cyber training must broaden understanding of cyber weapons and strategies and contribute to other military operations that may be used in conjunction with traditional attacks.

Multiple branches in the defense department have established professional cyber force operators and are developing multiple cyber career paths for officers, enlisted personnel and civilians. In addition, the National Guard has reportedly joined this effort and has made the plan a focal point for future recruitment. When you include the intelligence communities (IC) demand for cyber intelligence gathering capabilities and analysts you begin to see how these scarce resources will be in high demand. Finally, the Obama administration stimulus package and the recent announcement of a 60 day information infrastructure security assessment will further drive resource demand. If that picture is not bleak enough, at the current rates of degree attainment the U.S. will produce approximately 48 million new undergraduate degrees by 2025 -- 16 million fewer degrees than the 64 million it would need to match leading nations. To make up the gap, the U.S. would need to produce an additional 781,000 college graduates a year -- a 37 percent increase over current levels. However, this is another aspect to the shortfall in education. U.S. education in Mathematics and Science is falling behind other developed nations with a rating of only mediocre. While The World Economic Forum's 2007-2008 Global Competitiveness Report ranks the U.S. fifth best overall, the quality of math and science education in the U.S. ranks 45 out of 131 countries surveyed.

Conclusion

The Intelligence community released their 2008 threat assessment on February 13th, 2009. In that report it stated, "Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. The Intelligence Community expects these trends to continue in the coming year." This leads one to believe that the United States has been placed at risk due to our failing grades in math and science on our report cards! The availability of educated resources to meet the increasing demand for cyber warriors is highly questionable. The educational requirements coupled with the ability to obtain a security clearance will combine to make this a challenge for military leaders around the world. When you factor in the demand from the business community, the challenge becomes huge. As the cyber cold war heats up, the demand for these highly skilled resources will grow even further.

Influencing Intelligence

INTEL: Last year China graduated around 900,000 scientists and engineers compared to less than 200,000 that graduated in the United States.

INTEL: Spy-Ops, a specialty training company, recently announced its' second graduating class in their Certificate in Cyber Warfare program.

INTEL: Recent cyber attacks appear to be an attempt to take advantage of an ongoing political and economic crisis.

INTEL: The United States military is more reliant on computers and networks than any other military in the world today.

INTEL: China had 210 million Internet users at the end of 2007 and the online population is thought to have become the largest in the world in 2008.

INTEL: The retirement of the baby-boomers in the United States is expected to hit the pool of experienced technical resources hard in the next several years.

INTEL: The IT labor shortage is forcing many businesses to recruit skilled foreign workers to meet their needs. This is not a viable option for the military nor many defense contractors.

INTEL: A 2007 Hudson survey found that 72% of technical and engineering hiring managers say the current talent shortage is impacting their ability to recruit quality staff.

About Technolytics

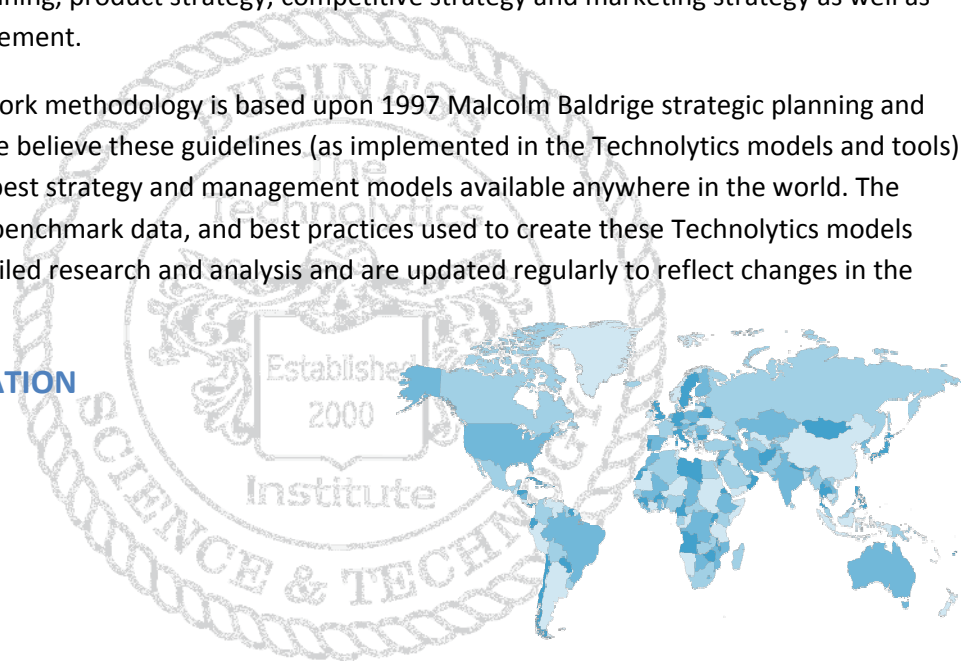
The Technolytics Institute (Technolytics) was established in 2000 as an independent executive think tank. Our primary purpose is to undertake original research and develop substantive points of view on strategic issues facing executives in businesses and industry around the world. Our strategic goals focus on improving business performance, creating sustainable competitive advantage, delivering innovation and technology, and managing security and risk.

Technolytics help guide business executives, industry leaders and government policy makers in shaping the economic, regulatory and risk environment of tomorrow. One of the hallmarks of our service offering is our security and risk scenario planning. Our approach is called Trans-disciplinary Intelligence Engineering (TIE). This approach has been used to develop scenarios for Homeland Security, Corporate Event Planning, Corporate Espionage and Security and for other entities. This technique has been applied to strategic planning, product strategy, competitive strategy and marketing strategy as well as security and risk management.

Our technology framework methodology is based upon 1997 Malcolm Baldrige strategic planning and reporting guidelines. We believe these guidelines (as implemented in the Technolytics models and tools) represent some of the best strategy and management models available anywhere in the world. The knowledge repository, benchmark data, and best practices used to create these Technolytics models have evolved from detailed research and analysis and are updated regularly to reflect changes in the global market.

CONTACT INFORMATION

The Technolytics Institute
4017 Washington Road
Mail Stop #348
McMurray, PA 15317
P 888-650-0800
F 412-291-1193
I www.technolytics.com
E info@technolytics.com



The following is a list of research that will be published in the near future.

1. *Cyber Counter Intelligence*
2. *Cyber Defense Systems*
3. *Cyber Intelligence Acquisition*
4. *Cyber Attack Scenarios*
5. *Cyber Threat Assessment 2009*

