

# Executive Whitepaper

## Cyber Defense Market



September 2009

The Technolytics Institute 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, government and industry around the world.

Our strategic goals focus on improving critical measures of performance, creating sustainable competitive advantage, delivering innovation and technology, and managing security and risk. We operate three centers: [Business & Commerce] – [Security & Intelligence] and [Science & Technology] and serve client in business, government and industry.

Technolytics is not your typical think-tank or consulting company. We are not just involved in the conception of a strategy as many other organizations are. We follow though and monitor and measure the progress being made toward the desired security posture. We work with security product and services providers and help them modify their thinking and adapt to the new management realities to make sure the defined solution works. Our approach, methods and tools are designed to position security products and services that meet the assessed needs of our clients.

### The Technolytics Institute

4017 Washington Road  
Mail Stop 348  
McMurray, PA 15317  
P 888-650-0800  
F 412-291-1193  
I [www.technolytics.com](http://www.technolytics.com)

### Personal Contact

KGColeman@technolytics.com  
P 412-818-7656

An international race has begun to create offensive and defensive cyber warfare capabilities within the militaries around the world. The big problem with cyber warfare is it's new - there has not been a lot of experience with it. Absent that experience, no one is really sure what will take place when an entity attempts to use cyber weapons to their fullest extent. My biggest concern is that with cyber weapons, unlike nuclear weapons, there seems to be little restraint by those who wield this new class of military capability. Cyber warfare and security are at the forefront of modern defense strategies. Strong threads of research and interest are developing in the area, including the understanding of threats and risks to information systems, the development of a strong security culture, as well as incident detection, analysis and post incident investigation. Much of the information about cyber attacks against countries and private sector organizations is kept secret, since if the attackers know which of their operations are being observed or even known about, they will take steps to get their work back into the shadows. In an online poll which was a collaborative effort between DefenseTech.Org and the Technolytics Institute, 43 percent of those responding thought that the United States was not prepared for a cyber attack and 47 percent felt the U.S. was somewhat prepared. We believe that paints a realistic picture of the current state of cyber defenses.

### Market Sizing and Distribution

The 2010 worldwide military and intelligence expenditures are estimated to be approaching \$1.8 trillion. The United States accounts for just over one quarter of that total. President Obama should expect a subsequent defensive budget request in coming months as Cyber Command is established and begins to formalize their operations and capabilities. No one should expect to hear anything about the nation's offensive cyber capacity, or the nation's cyber intelligence spending. In looking at the overall picture (critical infrastructure, government systems and the military plus intelligence) the price tag will have a total in the hundreds of billions of dollars through 2012. Typically when estimating military budgets they are divided into three areas. First Human Resource costs. Second is the maintenance and supply of existing weaponry and capabilities. The third and final area is the development and acquisition of new capabilities. Each of these three areas equate to approximately one-third of the overall budget. However, there are two factors that should be considered when examining cyber. First the human resource costs differ greatly around the globe. For example, China's resource costs are about 70 percent lower than that of the United States. Another important consideration is that the maintenance and operations costs of cyber capabilities are much lower than that of the traditional military capabilities and substantially lower than that of our strategic arsenal.

technolytics

## Current Cyber Threat Rating



Lt. General Keith Alexander, the sixteenth Director of the National Security Agency, stated that even as the military secures its networks, it is more likely that any major cyber attack would target industry such as the electrical grid rather than the Pentagon. Responding to such an attack, he said, would require broad co-ordination between the public and private sectors. The biggest issue/challenge for the government is how to include private sector critical infrastructure organization in the intelligence loop and there is no easy answer to this question!

Cyber warfare has been one of the pillars of Chinese military strategy since the early 1990s. Capital Hill has become very concerned over recent threat assessments that indicate China has and continues to aggressively invested in cyber warfare capabilities. U.S. Director of National Intelligence said, "China has the ability to challenge U.S. interests in traditional and emerging ways."

**NOTE:** The information contained in this document is an opinion based on open source intelligence coupled with our research and analysis. Data is provided for information purposes only and is not intended for investing purposes. Viewers agree that Technolytics, its employees, affiliates, licensors and any independent contractor engaged by the company shall not be liable for any errors in the content of any information provided through, or for any actions taken by viewers or any third party, in reliance thereon.

## The Technolytics Institute

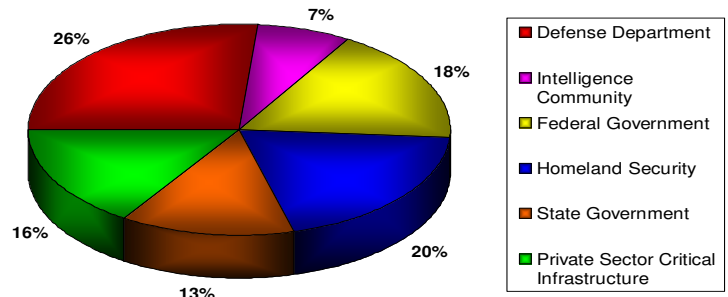
4017 Washington Road  
Mail Stop 348  
McMurray, PA 15317  
P 888-650-0800  
F 412-291-1193  
I [www.technolytics.com](http://www.technolytics.com)

### Personal Contact

[KGColeman@technolytics.com](mailto:KGColeman@technolytics.com)  
P 412-818-7656

## Cyber Warfare Overall Budget Distribution

The overall budget for cyber operations in the military is only expected to grow the existing budget by between 10 and 12 percent. DHS is expected to receive between 15 and 18 percent increase in their budget for cyber defense. These numbers could dramatically increase if more than 18 to 20 percent of our nation's critical infrastructure if found to be obsolete and no longer supported by the vendor community. At this point there are near 90



thousand critical infrastructure systems, subsystems and components identified in the tracking database. That is a clear indicator of the scope of this effort. Given approximately 85 percent of our nation's critical infrastructure is privately owned, many believe protecting it is largely the U.S. private sector's responsibility. I have had dozens of conversations that suggest the private sector may go to the government looking for money to address this threat because of the blur between criminal, terrorist and rogue nations state threats and the magnitude of the investment required to modernize and protect these assets.

## Insights *(A private / detailed briefing on this topic is available, contact Technolytics for information)*

The cyber warfare industry is now forming. We believe that we will see a blurring between traditional information security vendors servicing the private sector and those vendors who are in the defense and intelligence industry. In addition, increased mergers and acquisitions of small and medium sized companies with cyber capabilities will occur in the earlier stages of the cyber defense industry development. Another influencing factor is legislation. Currently, there are at least 18 bills that have been introduced as Congress is struggling with just how to grant government organizations the authorities and regulatory tools they need to protect the country against acts of cyber aggression including—cyber terrorism, cyber espionage, cyber crime and cyber war. The biggest issue is granting the government the authority and flexibility while protecting end users' privacy. The legislative acts could have a profound impact on the distribution shown in the above pie chart. It is also important to note that these are not a one time investments. Another factor that will greatly influence spending on cyber capabilities is if the U.S or one of our allies experiences a substantive cyber attack. The U.S. seems to be operating in reactive posture when it comes to threats not yet fully realized. Spending in this area could be limited at first and grow sharply through 2012 and beyond. Continuous updating of all these systems will be required as the advancement and proliferation of cyber weapons continue and the computer industry delivers new technology and vulnerabilities continue to be found in existing systems and new ones.