

## **QinetiQ/Cyveillance Deal Will Boost Cyberintelligence Market**

**Avivah Litan**

The U.S. government has approved QinetiQ of North America's acquisition of Cyveillance. Gartner expects further deals as firms seek competency in cyberintelligence as a competitive edge in national cybersecurity efforts.

## NEWS ANALYSIS

---

### Event

On 24 June 2009, the Committee on Foreign Investment in the U.S. (CFIUS) concluded that there are no unresolved national security concerns with respect to QinetiQ's acquisition of Cyveillance, a small, privately held cyberintelligence firm headquartered in Arlington, Virginia. The acquisition is now expected to close during July. QinetiQ is a London-based research and defense contracting firm with a separate U.S. division. It plans to acquire Cyveillance for \$40 million with a possible additional \$40 million in earn-outs.

### Analysis

The cyberintelligence market has been relatively slow to take off. Most enterprises don't begin to fathom the usefulness of cyberintelligence until after they have been damaged by an attack that could have been prevented through early detection. But Gartner believes the relative lack of interest in this market is about to change. Over the next five years, the U.S. government will dole out a reported \$17 billion under its newly revived cybersecurity operation, which will defend the U.S. against cyberthreats and cyberattacks to military installations and the U.S. national infrastructure, such as the electrical grid, air traffic control system and defense department networks.

QinetiQ is eager to grab a chunk of the new government business. Cyberintelligence services, such as those offered by Cyveillance, can help spot leaked or stolen secret information that, in the wrong hands, could pose a serious threat to national security. Gartner believes the Cyveillance technology will give QinetiQ a competitive advantage as well as enhance its cyberintelligence-gathering capabilities. We expect other defense contracting firms will copy QinetiQ by trying to develop or acquire their own cyberintelligence services.

Under the terms of the acquisition, Cyveillance will operate as a separate business unit within QinetiQ of North America, and will continue to focus on the commercial market. The current Cyveillance management team and staff will target commercial organizations that seek protection from various cyberthreats, including "phishing," "pharming" and targeted malware, as well as other illegal activities that can be spotted on the Internet, such as threats against company executives or the sale of counterfeit goods. The QinetiQ North America and Cyveillance team will form a partnership to introduce Cyveillance services and solutions to the federal government market by leveraging Cyveillance's technology infrastructure, including its proprietary search engine, heuristics analysis and data-gathering tools.

## RECOMMENDATIONS

---

### Commercial companies and government agencies concerned with national security:

- Consider investing in cyberintelligence to extend your security activities beyond the perimeter of your enterprise network. Most organizations are only staffed to deal with security functions that guard information and assets within their organizational boundary.
- Perform a cost-benefit analysis for cyberintelligence services. Priced at less than \$150,000 a year for most small-to-midsize implementations, these services can be a bargain if companies quickly move to address the threats they unearth.

- Identify the types of threats you are looking for, and plan how you will address any information they uncover. The detection of threats in itself will not necessarily protect your company's assets and resources.

**Cyveillance customers:**

- Expect an improvement in service due to increased resources being brought to bear on Cyveillance's commercial offerings.

**RECOMMENDED READING**

---

- "Brand-Monitoring and Anti-Phishing Vendors" — Although brand-monitoring technology is commoditizing, each vendor has its own analytical focus, service differentiators and challenges. **By Arabella Hallawell and Avivah Litan**
- "Evaluating Brand-Monitoring and Anti-Phishing Services" — Use six main evaluation criteria to select the brand-monitoring service best suited to your organization. **By Arabella Hallawell and Avivah Litan**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

## REGIONAL HEADQUARTERS

---

### **Corporate Headquarters**

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

### **European Headquarters**

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

### **Asia/Pacific Headquarters**

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### **Japan Headquarters**

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### **Latin America Headquarters**

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509