(U//~~FOUO~~) Datawar

UNCLASSIFIED

From Intellipedia

(U) This page has not been edited since February 13, 2009. Please help with completing or updating the page if it has intelligence value

(U) See Intellipedia:Abandoned pages for more information about pages with this banner.

(U) See the discussion page for more information about the status of this page.

This topic is of one of many emerging issues identified by (b)(3) This and several other emerging issues are grouped in a category that describes New Weapons.

(b)(3)

Datawar

Issue

How might networked databases become a new theater of conflict?

Discussion

Networked databases are exploding in cyberspace, underwritten by orders-of-magnitude increases in:

- **Storage.** The cost of data storage is dropping to the point where it is practically free. Databases even retain voice communications, which are even easier to store given VoIP (Voice Over IP)protocols. Many large organizations no longer limit the size of email boxes. Increasingly, whatever goes into a database stays there – or in some other database– indefinitely.
- **Search.** Search engines are fundamental to everyday life in knowledge economies such as the US, Europe and the upper echelons of industrial and developing economies. They allow access to the 400 million host sites now on the web (which increases by 20% a year). Reflecting their value, the most advanced search engine, Google, rose from nothing to a $100 billion a year corporation in less than a decade.
- **Identity.** Personal interactions are increasingly traceable. We leave digital trails when using technologies ranging from biometric scanners to web browser cookies to the "electronic money" of debit and credit cards. These electronic trails capture what we used to do anonymously. For example, when we commute to work, from the credit card we swipe to buy gas, to the transponder that collects our toll, to the cell phone record of our calls and location along the way, to the RFID-embedded pass card we use to enter our building – all of these actions routinely leave a detailed electronic trail of our specific activities.
- **Mining.** XML (Extensible Mark-Up Language, a programming language similar to HTML that provides a common frame of reference for databases), makes it easier to mine across databases. While public initiatives like TIA (DARPA's Total Information Awareness program) were slowed by political pressure, the underlying technologies are speeding ahead. Even when access to data is restricted, advanced algorithms can infer information by combining data from multiple sources.
- **Routine use.** Even elementary school report cards are stored in networked databases. Medical records, manufacturing orders, census data – practically every major interaction in business and government – are now available via networked databases (to those with access, of course). Data that was once protected simply by its paper nature, is now accessible due to its digital nature and its inclusion in networked databases. These networks of databases are not mere technological toys. Businesses and governments do not build and maintain huge databases and then network them for fun. Rather, these networks are modern fulcrums of competitive advantage. Take the world's largest retailer, Wal-Mart, for example. Wal-Mart leverages a global network of databases to produce its competitive advantage. Wal-Mart integrates logistics networks with financial databases through a proprietary information network. The end result is a retail colossus.

Wal-Mart is America's largest private truck fleet operator, energy consumer and real estate developer. It has over one million employees, thousands of suppliers, hundreds ofdistribution centers and annual revenues equal to the GDP of Australia. Not only is Wal-Mart the largest customer for giants such as Disney, Kraft, Revlon and Procter & Gamble, all these firms (and many others) manage their inventories through Wal-Mart's networks; all of their purchase, inventory and shipping data exist within Wal-Mart's continuous replenishment program. These suppliers – plus Wal-Mart -- leverage their combined networks to produce a combined competitive advantage. They all place their databases on the same network, which lowers overhead costs for everyone. It also cuts indirect costs by giving sellers and buyers visibility into each other's data. They compare their plans, problems, schedules and opportunities with everyone else in the network. By owning this common network, Wal-Mart gains a competitive leverage over prices and suppliers. If anyone wanted to destroy Wal-Mart, blowing up a distribution center or superstore would do little strategic damage. Corrupting its network of databases, however, would ruin the corporation. Wal-Mart simply could not operate if forced to rely on paper and telephones for every transaction. In the same vein, an explosives attack on the United States (e.g., the World Trade Center), despite the human toll, would not destroy the US economy. A successful attack on our networks of databases, however, would be devastating. Even an attack that brought into question the validity of data would have significant and potentially devastating consequences. A "bug" that was developed for (b)(3)

example that could undermine the validity of the banking or financial industries would have serious worldwide impact. While many people have looked at targeting and defending stand-alone databases in the past and others have looked at network warfare, the growth of networked databases, crucial to the economy and government of every advanced society, may be an area of underserved examination. It is more than the sum of networks and data; it is a new "animal" that requires focused examination.

Retrieved from (b)(3)

Categories: Abandoned since 2009 | (b)(3)

UNCLASSIFIED

- This page has been accessed 835 times.
- 3 (b)(3)
- This page was last modified 14:35, 6 March 2018 by (b)(3) Most recent editors: (b)(3) and others.

(b)(3)

Use of this U.S. Government system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse actions.

(b)(3)