



Left-click on blue, underlined text for links.¹

June 9, 2007

CONTENTS

[Apple's iTunes Raise Privacy Concerns](#)
[Certified Email Has a Price](#)
[Cyberwarfare 2: Realistic Appraisals](#)
[eBay to Halt Sale of Ivory](#)
[Emails Save "Jericho"](#)
[Leadership Watered Down 2](#)
[Predators Targeted by Libraries](#)
[Rainbow's End](#)
[Sweden Embassy 2nd in Virtual Diplomacy](#)

CYBERWAR 2: REALISTIC APPRAISALS

Darry D Eggleston

The news about the cyberwar attack on [Estonia](#), last week, continues to add clarity to what happened and what could happen.

Information Week ("Cyberwarfare: A Realistic Appraisal," June 4, 2007, pp. 49 – 50) states that "Communication and cooperation are keys to defense.

"Distributed denial-of-service attacks are particularly difficult to prevent and require a lot of coordination to contain the damage when multiple sites are hit. In order to weather the 128 strikes launched against its cyberinfrastructure, Estonia sought help from not only its Computer Emergency Readiness Team, established late last year, but also the TransEuropean Research and Education Networking Association and Computer Emergency

¹ Published for the New Users Group of the Tampa Bay PC User Group < <http://tbpcug.org> >. Permission to reprint articles is granted if all of these conditions are met: (1) the author is credited, (2) the article is published in full, without unauthorized editing of content, and (3) a link to or PDF of the reprint is sent to DarryD@darryd.com.

Readiness Teams in other countries, including Finland and Germany, according to ENISA [European Network & Information Security Agency].”

[ENISA](#) reported, “Events in Estonia highlight that pro-active security needs the support of Incident Response (IR) capabilities in the moments of crisis. Cyber attacks against Estonia, mainly in the form of Distributed Denial of Service (DDoS) attacks, primarily targeted the Estonian Government and police sites. Private sector banking and on-line media were also heavily targeted and the attacks affected the functioning of the rest of the network infrastructure in Estonia. As a result, the targeted sites were inaccessible outside of Estonia for extended periods in order to subdue the attacks and to maintain services within the country.”

The [Washington Post](#), (“For Estonia and NATO, A New Kind of War,” by Anne Applebaum, May 22, 2007) reported “... the attacks’ precise origin cannot be determined: Unlike classic terrorism, the essence of modern cyberwarfare is its anonymity. Though some attacks did appear to come from PCs belonging to the Russian presidential administration, others came from as far afield as Brazil and Vietnam.

[SearchSecurity.com](#) (“Experts doubt Russian government launched DDoS attacks,” by Bill Brenner, 18 May 2007) states, “Some experts are dismissing speculation earlier this week that hackers sponsored by the Russian government were behind a series of blistering distributed denial-of-service (DDoS) attacks in the Baltic country of Estonia.

It quoted Graham Cluley, Senior Technology Consultant, Sophos (the security software firm), as asking “If you were the Russian government and wanted to launch an attack against Estonian authority Web sites ... would you really use your own PCs to do it?”

However, *Information Week* (“Cyberwarfare: A Realistic Appraisal,” June 4, 2007, pp. 49 – 50) reported, “... last month, a report from the Department of Defense said the People’s Liberation Army of China is building up its cyberwarfare capabilities, even creating malware that could be used against enemy computer systems in first-strike attacks.

But talking about cyberwarfare is not a new discussion in the Department of Defense.

The [Armed Forces Press Service](#) (“Intel Chief Addresses Longer-Range Threats to U.S.,” by Jim Garamone, March 6, 2001) reported on Vice Admiral Thomas Wilson, Director of the Defense Intelligence Agency, testifying before

the Senate Select Committee on Intelligence in March of 2001 when he talked about cyberwarfare.

Among the things he said were:

“The United States is the world’s sole remaining super power. America faces challenges and threats that span the spectrum of warfare...

“The news media call information operations “cyberwar.” High profile hacker attacks such as the Love Bug show how vulnerable an information society can be. But information operations are more than just computer warfare. It can include electronic warfare, psychological operations, physical attack, denial and deception, computer network attack and the use of more exotic technologies such as directed energy weapons or electromagnetic pulse weapons.

“Software tools for network intrusion and disruption are becoming globally available over the Internet, providing almost any interested U.S. adversary a basic computer network exploitation or attack capability.”

“To date, however, the skills and effort needed for adversaries to use tools and technology effectively, such as intensive reconnaissance of U.S. target networks, for example, remain important limits on foreign cyber attack capabilities.”

So, if you’re having trouble sleeping at night with worry over what lies over the horizon for mankind, perhaps cyberwarfare — rather than global warming — should be your *terreur de jour*.

EBAY TO HALT SALE OF IVORY

[Smart Computing](#) (“eBay poised to halt sale of ivory on its Websites,” by Marlowe Hood, June 5, 2007) reported:

“eBay is set to ban ivory trade from its Websites, as pressure mounts to eradicate illegal traffic in endangered species from the Internet, participants at the world forum regulating wildlife commerce said Tuesday...

“Conservation groups have, in the past, been highly critical of eBay for not enforcing its own rules forbidding the sale of wildlife products made from protected species.

“In a follow up study in February focusing on ivory, IFAW [International Fund for Animal Welfare] catalogued more than 2000 ivory items on 8 national Websites, only 6% of them offering evidence that they complied with international law.

“When the German eBay site instituted stiffer rules requiring that proof of certification be posted along with photos of the objects, the number of ivory items displayed at any given time dropped from approximately 400 to 40....”

RAINBOW'S END

Kathy Otto

This is a true story that happened to my daughter and I.

About a year ago, after a summer storm, my daughter and I were looking out the big picture window of our living room.

All of a sudden we both noticed the most beautiful rainbow and suddenly realized that the END of that rainbow was directly in front of us. We were both amazed to see such a sight and were thinking “How many people actually see the END of the rainbow”?

After several minutes of gazing at this amazing sight she said to me “I don't see the pot of gold, I guess there really isn't one”.

I replied, “I still believe there is a pot of gold at the end of the rainbow, we just happen to be on the wrong end!”

CERTIFIED EMAIL HAS A PRICE

Darry D Eggleston, June 7, 2007

Between *phishing*², scams and hoaxes, the cost of sending real emails is increasing for commercial firms. Given the magnitude of the threats,

² *Phishing*, pronounced “fishing,” is a scam to steal valuable information such as credit cards, social security numbers, user IDs and passwords. Also known as “brand spoofing,” an official-looking email is sent to potential victims pretending to be from their ISP, retail store, etc., and that due to internal accounting errors or some other pretext, certain information must be updated to continue the service.

commercial certification software seems to be the only sure way — at this time — to assure an email is from the stated sender.

The Tampa Tribune (“E-Mail Now Has A Price,” Business, June 7, 2007, p. 1) reports, “Four more Internet service providers will start charging banks, e-commerce sites and other large e-mail senders for guaranteed delivery.

“In deals to be announced today, Goodmail Systems is expanding its Certified Email program to Comcast, Cox Communications, Time Warner Cable’s Road Runner and Verizon Communications. Yahoo and Time Warner’s AOL became inaugural participants last year.

“Individuals, businesses and organizations will be able to continue sending messages free, but they risk finding their missives caught in increasingly aggressive spam filters.”

What effect this will have upon personal email would seem to be minimal if one uses the argument, “What smart person is going to pay money to send jokes and greetings to friends?” However, clubs, religious organizations and volunteer groups may find that paying to email would be cost-effective.

PREDATORS TARGETED BY LIBRARIES

The Tampa Tribune (“Library Computers Throw The Book At Online Predators,” *Nation/World*, June 7, 2007, p. 2) reported that the Hillsborough County, Florida, libraries are starting to use a program called “Netsmartz.”

“Created by the National Center for Missing and Exploited Children, [Netsmartz](#) is a computer software program that aims to teach children age 5 and older how to avoid the danger of Internet sexual predators.

“Starting Monday [June 14], all computers in Hillsborough County public libraries will feature the program. Children who use the computers will be encouraged to complete the Internet safety lesson before logging online.

“The Netsmartz lesson varies based on age group and takes 20 minutes to complete. Younger children get a lesson in safety from Clicky the Robot; teenagers will watch videos that feature real-life stories from teens who have been targeted by Internet predators.”

- Children who complete the program will receive a certificate and vouchers for free admission to local attractions, such' as Busch Gardens and The Florida Aquarium.
- Eventually, the program will be put on public computers available at county Parks and Recreation centers.
- Several Hillsborough County libraries will offer computer safety workshops this summer for parents.

EMAILS SAVE "JERICHO"

The Tampa Tribune ("Fans persuade CBS not to cancel Jericho," Nation/ World, June 7, 2007, page 5") reported, [the TV show,] "'Jericho' fans who slammed CBS with protests over the drama's cancellation have won the battle; it will return next season..."

"It was an unusual display of viewer might since networks usually put ratings ahead of even the most passionate well-organized fan base. But CBS said the show deserve another chance, although cautioning it must prove it has wider appeal.

In an internet-posted letter to the fans of the show, CBS Entertainment president Nina Tassler [wrote](#), "Over the past few weeks you have put forth an impressive and probably unprecedented display of passion in support of a prime time television series. You got our attention; your emails and collective voice have been heard."

What is important to observe here is that the "voice of the people" can be heard, but it needs to be targeted. Signing petitions does not work, but getting the masses to *make the time* to send emails reaped rewards in this case.

APPLE'S ITUNES RAISE PRIVACY CONCERNS

According to the [BBC](#), June 1, 2007, "The launch of music tracks free of digital locks on iTunes has been overshadowed by the discovery that they contain data about who bought them.

“The tracks without the digital locks, known as Digital Rights Management (DRM) technology, officially went on sale on 30 May under the iTunes Plus banner.

“Apple uses a technology known as Fairplay to limit what people can do with downloads. Fairplay can be circumvented by burning tracks to a CD and then converting them to another format.

“News site [Ars Technica](#) was among the first to discover that downloaded tracks free of Fairplay have embedded within them the full name and account information, including e-mail address, of who bought them.

But this is rather old news resurfacing as the sales began at iTunes.

[CNet](#) reported on January 13th, “A new version of Apple Computer’s popular iTunes software, released Tuesday, is drawing barbs from privacy advocates for sending information about computer users’ playlists back to Apple.

“The new music software includes a “MiniStore” window, which provides recommended links to Apple’s music download service when a listener actively clicks on a song in their personal play list, including songs that haven’t been purchased from the iTunes store.

“To provide those recommendations, the software ... also transmits a string of data that is linked to a computer user’s unique iTunes account ID.

“Because iTunes users typically sign up for the music store with an e-mail address and a credit card number, the account ID number could in theory be linked to that information, as well as a user’s purchase history, said Apple expert Kirk McElhearn.”

The question remains, “Will iTunes remove the info or retain it?”

LEADERSHIP WATERED DOWN 2

As I reported, in the [5 June ExcelNet News](#) (“Leadership Watered Down”), the leadership of Tampa, Florida, did less than a stellar job of conserving water although each member made repeated pleas for the city’s people to do so.

In a followup, *The Tampa Tribune* (Nation/World, June 8, 2007, p. 11) got these explanation from one of those ‘leaders’.

“City Council Member Tom Scott on the report that he used 307,672 gallons of water a year, the most of any council member and about 3 times the amount used by the average Tampa household, said, ‘I’m shocked by that, I’m really shocked. But there’s a leak and my mother-in-law washes all those clothes.’”

SWEDEN EMBASSY 2nd IN VIRTUAL DIPLOMACY

According to News.com.au [Australia] (“Sweden opens Second Life embassy,” May 30, 2007), “Sweden has become the second country to open an embassy in the virtual world Second Life.

“Created to promote The Nordic state’s image and culture, the embassy does not offer any real or virtual consular services but provides information on its real world counterparts.

[Second Life](http://SecondLife.com) is an Internet-based, world where users create characters known as [avatars](http://avatars.com). Based in San Francisco, it is a fast-growing virtual community with more than 6 million “citizens.” It has its own currency, the Linden Dollar, which can be exchanged for US dollars. SL citizens own property, socialize, learn and interact.

“The [Swedish] embassy includes a room dedicated to Raoul Wallenberg, who helped save thousands of Jews in World War II; an art exhibition, and radio news via iPOD.”

According to [Minivan News](http://MinivanNews.com) (“Maldives Opens World’s First Virtual Embassy,” by Will Jordan, May 22, 2007), “The Maldives’ Virtual Embassy is located in the Diplomatic Quarter of Diplomacy Island in Second Life, an on-line space designed to allow new avenues for diplomatic representation and negotiation, especially for small and developing countries that have limited diplomatic outreach in the “real” world.”

“Maldives or Maledives, officially the Republic of Maldives, is an island nation consisting of a group of atolls in the Indian Ocean,” according to [Wikipedia](http://Wikipedia.com). The [Republic of Maldives](http://RepublicofMaldives.com) requires no prior visa.



The front of the Maldives' virtual embassy