



COMPUTOPICS

Vol. XLX No. 6

January 2010

UPCOMING EVENT



GUEST SPEAKER
Joey Ponthieux
**"3D Animation and
Modeling For Aerospace"**
February 8, 2010
7:30 – 9pm

IN THIS ISSUE

- Upcoming Events (Page 1)
- Quick Updates (Page 2)
- Science Fair Judges Needed (Page 2)
- Mid-Year Budget (Page 3-4)
- Essay/Book Reviews: How I Spent
Computer Security Day (Page 5-12)
- DC ACM Calendar at a Glance (Page 13)

As always, this lecture is free of charge and open to the public. ACM membership is not required to attend, nor is an RSVP necessary. Please feel free to bring friends and colleagues.

Mr. Ponthieux's talk revolves around 3D animation and modeling for the aerospace industry, from the 1980's until today. He will discuss the equipment and capabilities (or lack thereof) from his early career through projects including Hyper-X, the Viking 25th Anniversary, TDT Tunnel, and his current efforts with the ATOL lab and their task to assist in the redesign of the National Airspace Management System. The lecture will reveal the importance of 3D animation in providing promotional support for these projects and/or concepts and how CGI has taken on an increasing role in prototyping complex ideas rather than just promoting them. This event will be co-sponsored by [DC-SIGGRAPH](#).

About the speaker: Joey Ponthieux is a professional 3D animator with a background in Television Broadcasting, Aeronautics and Space Research, and traditional Graphic Arts. He is self trained in multiple CGI disciplines including Modeling, Motion, Texturing, Lighting, Scripting, and Compositing. He is currently a 3D animator in the Data Visualization and Analysis Lab at NASA Langley Research Center.

Location:

The New America Foundation
1899 L Street NW, Washington DC
Suite 400 (4th Floor)
Closest Metro: Farragut North (Red Line)

Parking:

One recommended garage is on 19th St.
between M and L streets for \$7.00 (after 5pm).
Free street parking is available starting at
6:30pm.

OTHER UPCOMING EVENTS

Monday April 5

George W. Arnold, NIST
"Smart Grid Interoperability"

Monday May 17

Allen Tucker, Bowdoin College,
Maine
"Is There A Good Programming
Language Out There?"
(ACM Distinguished Speaker)



MEMBERSHIP RENEWAL DELAYED

The annual renewal process for Members and Associate Members has been delayed due to unforeseen technical difficulties.

When the website is ready, all members will be contacted via email regarding the process. Thank you for your patience in the meantime.

QUICK UPDATES

Finances

Balance Sheet as of Jan. 6, 2010

Checking Account	\$3,840.89
Money Market (Savings)	\$15,122.34
Certificates of Deposit	\$10,273.70
	\$20,661.32
Other Assets	\$551.19
Total Liabilities	\$0
NET WORTH	\$50,449.44

Membership

As of Jan. 6, 2010, the DC ACM had 163 registered members. This total number includes 86 Members and 77 Associate Members.

Professional Development Seminars

The Spring 2010 Series of the DC ACM Professional Development Seminars will be held the week of March 15-20 at George Washington University. The PD Committee has been exploring a partnership with DC-SIGGRAPH to offer seminars oriented towards graphics arts professionals. Stay tuned for more details.

Executive Council Meetings

DC ACM EC Meetings have normally been held on the fourth Monday of the month.

However, the EC has decided to change their monthly meeting to the fourth Wednesday of the month for the foreseeable future. The location (Radio Free Asia conference room) remains unchanged.

Did You Know...?

The DC ACM website's "Archives" tab has a lot of resources from the past two years:

- Events in 2007-2009: Often including presentation materials
- Photos
- Videos
- Meeting Minutes
- CompuTopics Sept. 2008 to present

DC ACM To Award Student Memberships For Outstanding Projects in Five Regional Science Fairs

VOLUNTEERS NEEDED

Judging at the regional science fairs is easy and fun: talk to the students about their projects and if they seem interested in computers, and their project shows some talent or motivation, give them a student membership to ACM. Last year we had nine volunteers at five fairs -- check out the April issue of CompuTopics (pages 3-4) for details.

Please contact Awards Chair [Mark Nolan](#) if you are interested in volunteering in any of these regional fairs. We need 1-2 judges each:

[Northern Virginia](#) (Wakefield HS, Arlington, VA)
March 5-7, 2010

[Washington DC Mathematics, Science, and Technology Fair](#) (McKinley HS)
Date unknown

[Montgomery County](#) (held at Univ of MD in College Park) March 19-21, 2010

[PG County](#) (Community College, Largo, MD)
Date unknown

[Fairfax County](#) (Robinson Secondary School)
March 19-21, 2010

Message from the CompuTopics Editor

It has been a pleasure to revive CompuTopics, the newsletter of our chapter since 1960. I have attempted to guide CompuTopics into the digital world by distributing it as a PDF rather than the traditional postal mailing. Besides saving the chapter money, it also makes it more widely available to anyone who visits our website. (Ironically, the printed copies we bring to public events for non-members are also quite popular.) The PDF format also allows us to use hyperlinks and color photos.



I will soon be stepping down as Communications Chair. While members can still get information on the chapter through the website, email, Twitter, Facebook, etc., I hope that CompuTopics will continue to be a flagship publication for our chapter.

-- Cora Dickson

BUDGET SPOTLIGHT

DC ACM Mid-Year Budget Review

Acct	Name	Actual Income/Expenses 2008-2009	2009-2010 Budget	Actual Income/Expenses as of 1/6/10
Income				
501	Membership Dues	\$824.00	\$840.00	\$41.00
502	PD Registration Income	\$21,335.00		\$4,560.00
503	PD Refunds (negative)	\$840.00		-\$30.00
504	Sponsorships	\$6,000.00		
505	Interest Income	\$1,292.70	\$100.00	\$125.22
506	Meeting Income	\$4,050.00		
507	Miscellaneous Income	\$751.81		
508	Donations	\$100.00		
	Total Income	\$35,193.51	\$940.00	\$4,696.22
Expenses				
601	Speaker Honoraria	\$4,700.00	\$4,250.00	\$1,300.00
602	Speaker Travel	\$780.61	\$3,000.00	\$979.14
603	Speaker Food and Lodging	\$1,427.85	\$2,450.00	\$1,074.02
604	Meeting Room	\$2,308.07		
605	Meeting Audio/Visual	\$377.19		
606	Meeting Food	\$10,774.09	\$450.00	\$314.82
610	Awards	\$1,823.45	\$2,000.00	\$66.25
611	Scholarships			
621	Printing	\$929.23	\$280.00	\$140.14
622	Mailing/Postage	\$244.50	\$170.00	\$206.47
623	Stationery/Paper	\$769.71		
624	Other Office Supplies	\$254.07		
625	Archive Expense	\$827.22	\$1,200.00	\$684.00
626	Web Site	\$408.23	\$480.00	\$96.71
628	Miscellaneous Expenses	\$446.00	\$100.00	\$202.80
631	PD Books	\$2,100.13	\$1,200.00	\$412.82
632	PD Handouts		\$350.00	
633	PD Food	\$1,329.70	\$2,100.00	\$189.24
634	PD Publicity	\$8,856.90	\$3,500.00	\$2,316.99
641	Bank Fees	\$649.29	\$240.00	\$145.22
	Equipment	\$688.99		
	Total Expenses	\$39,695.23	\$21,770.00	\$8,118.62
	Contingency (~10%)	N/A	\$2,177.00	N/A
	Total Expenses w Contingency	N/A	\$23,947.00	N/A
Net Profit or Loss		-\$4,501.72	-\$23,007.00	-\$3,422.40

The DC ACM Standing Rules specify that the Executive Council will conduct a mid-year budget review and make adjustments as necessary. The above chart shows the consolidated budget request made in July 2009 and the actual income and expenses to date.

While we underestimated our income, we also overestimated the expenses for the Fall PD Seminar (due to low enrollment), and thus are not experiencing as great a loss as may have been indicated by the initial budget.

CONT'D ON PAGE 4

Now let's take a closer look at some of the individual program budgets, particularly the ones with large expenses and no source of income.

Professional Development – Fall Seminars

	Budget	Actual
PD Registration Income		4560
PD Refunds (negative)		-30
Total Income	0	4530
Speaker Honoraria	1500	500
Speaker Travel	500	188
Speaker Food and Lodging	350	273.66
Mailing/Postage		44.47
Miscellaneous Expenses		10
PD Books	1200	412.82
PD Handouts	350	0
PD Food	2100	189.24
PD Publicity	3500	2316.99
Bank Fees	240	117.24
Total Expenses	9740	4052.42
Contingency (10%)	974	N/A
Net Revenue or Loss	-10714	477.58

Programs

	Budget	Year to Date
Speaker Honoraria	2750	800
Speaker Travel	2500	791.14
Speaker Food and Lodging	2100	800.36
Meeting Room	0	0
Meeting Audio/Visual	0	0
Meeting Food	450	314.82
Printing	50	0
Miscellaneous Expenses	100	192.80*
Total Expenses	7950	2899.12
Contingency (10%)	795	N/A
Net Loss	-8745	-2899.12

* Includes depreciation for LCD Projector.

Secretary

	Budget	Year to Date
Printing	30	22.42
Mailing/Postage	10	0
Archive Expense	1200	684
Total Expenses	1240	706.42
Contingency (10%)	124	N/A
Net Loss	-1364	-706.42

Communications

	Budget	Year to Date
Printing	200	117.72
Mailing/Postage	140	140
Web Site	480	96.71
Total Expenses	820	354.43
Contingency (10%)	82	N/A
Net Loss	-902	-354.43



HOW I SPENT COMPUTER SECURITY DAY

or

A TALE OF TWO LIBRARIES

By Dr. Kent L. Miller
Vice Chair, DC ACM

BOOKS REVIEWED

[1] *Silence on the Wire*, Michal Zalewski, No Starch Press, San Francisco, CA, 2005, 212 pages.

[2] *Building Internet Firewalls*, Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, O'Reilly & Associates, Sebastopol, CA, 2000, 896 pages.

[3] *The Executive Guide to Information Security: Threats, Challenges, and Solutions*, Mark Egan with Tim Mather, Symantec Press, 2005, 306 pages.

[4] *Chinese Information-War Theory and Practice*, Timothy L. Thomas, Foreign Military Studies Office (FMSO), Fort Leavenworth, KS, 2004, 178 pages.

Computer Security Day

For many years the Association for Computing Machinery (ACM) has cosponsored the Computer Security Day Association (CSDA). As the [CSDA website](#) explains:

Computer Security Day was started in 1988 to help raise awareness of computer related security issues. Our goal is to remind people to protect their computers and information. This annual event is held around the world on November 30th although some organizations choose to have functions on the next business day if it falls on a weekend.

Naturally, the DC Chapter of the ACM (DC ACM) likes to help out. Of course, it is one thing to remind the general public, and quite another to address the sort who join the ACM.

As to the former, we note that most members of the general public do not really care about computer security until something bites them (e.g. identity theft). Now, as any teacher can tell you, students remember more of a lecture that is dramatic or funny. So, to remind John Q. Public of the dangers of, say, "phishing" or "social engineering," the following should work:

Lecture: Regale audience with the lurid tale of Kevin Mitnick: how he talked people into giving him passwords, which he used to break into networks; how he listened in on FBI phone calls to avoid capture, leaving doughnuts for them to find; and how, when finally captured, he was kept in solitary confinement and prevented from using a phone, because law enforcement officials convinced a judge that he had the ability to start a nuclear war by whistling into a pay phone.

Lesson: Don't give away your password. OK? And never to someone who can whistle.

But many who join the ACM have professional responsibilities. Members include computer scientists, engineers, system administrators, IT executives, etc, all of whom are aware of security issues. For a sophisticated audience, we need a story with more substance: one that illustrates the vulnerabilities, offers lessons on defense, shows how to integrate information security into executive level planning, and looks into the future. For this we need:

A Tale Of Two Libraries

The first library was at a major university. Once upon a time, in said library there was a librarian with time to read. Indeed, he read books that inspired him to sally forth and conquer an empire. Along the way, he annihilated millions, including many of his own followers. In time, he passed away, leaving a legacy of gargantuan government, staffed by nervous survivors, defensive about the legitimacy of their rule.

The second library was one modern one: electronic, open source, and tree friendly. This library posted some books found in the first library, and even included writings of the first

librarian. But this was a radical library, run by radical librarians, who did something, well, radical. They rejected the pretensions of the first librarian and those of his successors. Alarmed, the survivors struck back, suppressing the second library: first with old-school censorship; and later with shiny new Information Warfare.

Yet there was something about this spat that was strange, ironic, and even newsworthy. And so it happened that on February 5, 2007, the International Herald Tribune announced:

ONLINE MARXIST ARCHIVE BLAMES CHINA FOR ELECTRONIC ATTACKS

If ever there was a believer in the power of the written word, it was a best-selling author and former librarian, Mao Zedong.

As Mao explained to an early chronicler of his life, Edgar Snow, "Three books especially deeply carved my mind, and built up in me a faith in Marxism, from which, once I had accepted it as the correct interpretation of history, I did not afterward waver." Those books, he said, were a book about the history of socialism, a book about the history of class struggle and "The Communist Manifesto" by Karl Marx and Friedrich Engels.

According to the Marxist Internet Archive at www.marxists.org, an online community that produces and organizes an ever-growing Marxist library, the wheel has turned full circle.

People at the site say they suspect the Chinese government is behind computer attacks that are jeopardizing the site's ability to provide Marxist texts, and might force the library to stop providing material written in Chinese.

Here is the play-by-play, according to the Marxist Internet Archive.

January 10 - 13: Sporadic reports come in from volunteers in Australia and Asia that the MIA is not accessible for a few hours, and then comes back.

FIRST ATTACK

January 15: MIA detects a series of DoS (Denial of Service) SYN floods from various Chinese networks. Unlike the attacks of the previous few days, these are constant. These attacks cause our server to have a kernel panic and crash. Just as soon as the server reboots, the SYN floods

[CVE-1999-0116] cause another crash, and this continues constantly.

First, we write a crude script that blocks every SYN flood attempt, every minute. This is successful only for a short period, as the sheer number of Chinese IPs sending the SYN floods is too large to overcome. Next, we figure out that the SYN floods are exploiting a vulnerability in the Linux kernel (version 2.4.23), and we rebuild the Linux kernel to version 2.4.34, which overcomes these attacks. Meanwhile, the nature and origin of the attack, our previous history with the Chinese government (censorship, etc), and the experience of others suggest that this maybe politically motivated and directed by the Chinese government.

1 hour sample of attacking IP origins

*222.35.30.105 China Railway Telecom, Beijing
60.16.220.61 CNC Group, Liaoning Province Network, Liaoning
121.34.136.245 China Net, Guangdong Province Network, Guanzhou
222.240.83.89 China Net, Changsha Node Network
122.4.213.41 China Net, Shandong Province Network, Jinan
203.192.13.2 Xinhua News Agency
221.216.207.194 CNC Group, Beijing Province Network, Beijing
221.6.37.60 Nanjing Medical University, Nanjing Jiangsu Province Network, Nanjing
221.226.2.213 China Net, Jiangsu Province Network, Jiangsu
61.233.167.159 China Railway Telecom Center, unknown city*

At this point, however, our 4 year old server heaves under the strain. The string of constant reboots has taken its toll: the server reports a Machine Check Exception of a CPU context corruption, causing further crashes. This process further bludgeons the damaged server, and subsequent boots cause a failure in the RAID, forcing a rebuild of the array. During further crashes, one of the disks fails, causing future rebuilds of the array to be quite hopeless.

January 16: [W]e resolve on the kind of server to buy to meet our needs.

January 20: Marxists.org is redirected to our mirror servers. On the following day, a round robin DNS is setup between three MIA mirrors.

SECOND ATTACK

January 21-24: Mirror sites find a change in tactics, now a more crude Denial of Service attack is launched: Chinese sources download in mass material from the Chinese section. The German mirror combats this by limiting the number of connections to the server. Nevertheless, server load remains extremely high.

But how did the attacker know that a SYN flood would work?

Preparing The Attack

Many operating systems, networks, and the Internet itself have congenital defects. They were designed by honorable

people who implicitly trusted one another. The result is a great number of vulnerabilities, some of which are impossible to fix without a complete redesign---something unlikely to happen in the near future.

The book, *Silence on the Wire*, by Michal Zalewski, is about passive surveillance, namely, the art of quietly mapping out a target network, tracking individuals, and collecting confidential information---all without alerting the intended victim. Most of the book is printed in a small font that may cause eyestrain, so you may want reading glasses to magnify the text. That said, Zalewski covers a lot of ground. His treatment of vulnerabilities is organized into four parts: multi-user systems, traffic over local area networks, traffic over the Internet, and vulnerabilities of the Internet as a system.

What interests us here is that data is transmitted in packet form, and packets have a header and a payload. A header contains a number of fields which are populated with source address, destination address, checksum, and other useful info. A payload is zero or more bytes of data.



Now, packets are typically nested like Matryoshka dolls. Usually, the outermost packet is an Ethernet frame; the payload of which is an Internet Protocol (IP) packet; and the payload of the IP packet is either a User Datagram Protocol (UDP) packet or a Transmission Control Protocol (TCP) packet. The payload of a TCP or UDP packet is often a packet from a higher level protocol such as Telnet, FTP, SMTP, etc. Protocols are defined in the Request For Comments series of Internet documents, e.g., Ethernet (RFC 1042), IP (RFC791), UDP (RFC 768), TCP (RFC793), etc.

The key point is that packet headers are written by the sending operating system, and are subsequently rewritten along the way by a variety of devices. Since, the standards are less than air-tight, designers of operating systems, switches, routers, firewalls, and other equipment, have discretion as to how to populate and rewrite the header fields. Because no two designers think alike, packet headers inadvertently serve as fingerprints that allow an observer, to learn a great deal about a target network.

Of course, sometimes equipment fails or is badly designed, and the result is a malformed packet. Zalewski has posted on-line a [Museum of Broken Packets](#) (MOBP) containing many curious examples together with commentaries. The MOBP also contains a packet used for espionage---it can pass through a firewall and map out the internal network.

In the case of the Marxist Internet Archive, the attacker most likely inspected packet headers to determine that the MIA server was running Linux kernel 2.4.23.

Once the target was characterized, the next question would be how to attack it. The easiest way to determine that, would be to read bug reports, thereby benefitting from the experience of others. You can find CVE-1999-0116 by going to <<http://cve.mitre.org>>. A more costly but effective way---an institutional way---would be to build and staff a research center to run experiments and serve as a knowledge repository. In the case of the MIA, the attacker would have known that a SYN flood would crash the target OS.

Attackers, unlike designers, do not feel obliged to follow standards. They frequently populate

header fields with bogus or malformed info. One trick, used to deflect blame, is to populate the source address field with the address of an innocent third party. This is called spoofing.

The implication of spoofing, to appropriate the righteous argot of Marxists, is this: The miserable, proletarian computers in China could have been exploited by capitalist, imperialist computers elsewhere, in order to oppress the radical computers at the Marxist Internet Archive. After all, in Asia nearly all PCs run MS Windows, are infested with viruses, and are all but undefended. Indeed, the International Herald Tribune went on to say:

"We are not 100 percent sure this is the Chinese government; there are a lot of possibilities," said Brian Basgen, who has worked on the archive since 1990. But he noted that the archive had been temporarily banned by the Chinese government before, about two years ago.

"There is a motive," he said. "They have done it to us in the past. What they are doing is targeting just the Chinese files."

Preparing The Defense

System administrators bear much of the responsibility for defending their equipment and information. And defenders, from ancient times to this very day, start by marking out a perimeter; and within that perimeter constructing a layered defense each with its own perimeter; and forcing all traffic through a perimeter to pass through well-guarded choke points.



The book, *Building Internet Firewalls*, by Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, provides an invaluable guide to network security. They discuss security strategy, how to build firewalls, how to deploy Internet services, how to write a security policy, and how to monitor your system and respond to incidents.

Firewalls are the choke points between the Internet and your perimeter network; and between your perimeter network and your inner networks.

Zwicky, et al, recommend that Internet services be provided by "Bastion Hosts" located on your perimeter network. They discuss in great detail how to protect services for: web (HTTP), mail and news (SMTP, POP, IMAP, NNTP), files (FTP, NFS), remote access (Telnet), naming and directory (DNS, NIS, LDAP), authentication, etc.

Of course, security must be maintained. Open-source software is available that can scan target networks (e.g. NMAP and its graphical front-end ZENMAP). You should scan your own networks periodically to determine its topology, and what all is connected to it. You may be surprised to find laptops at the law firm next door and PCs at the apartment block across the street. You will also want to know what software patches are needed.

Mobile computing and wireless networking have made defense much harder. One must beware of users attaching wireless access points to internal networks, thereby allowing any war-driver to bypass the firewall. Worse yet, since every laptop becomes a potential weakest link, it is necessary to deploy firewall rules in every laptop, e.g., rules that close all unneeded ports and block all inbound connections.

Technology by itself is not enough. A security policy must be drafted and enforced. There must be a plan for purchasing the right equipment and hiring the right staff; and this must be paid for out of a budget. But policy, planning, and budgeting are tasks allotted to executives.

So, it is to the care and feeding of executives that we turn next.

General Mirror For The Aid Of Executives

The MIA is a small, albeit far-flung operation, so its board can dispatch the above mentioned executive tasks fairly quickly. But how would one protect a large operation, such as a bank, airline, or government agency?

Without a commitment to information security at the executive level, little can be accomplished. A system administrator can certainly draft an

information security policy, but it will impossible for him to enforce it without the cooperation of the legal and human resources departments. In short, executives are needed for policy, resource allocation, and coordination.

So, how do we get executives interested in information security? At first blush the prospects are bleak.

Most executives in business and government started out in business school. A degree in science, technology, engineering, or mathematics is rather the exception. Now those of you who have had the honor of teaching computer science to business majors may recognize the following four-step dance, that we shall call...

The Business School Foxtrot

REPEAT

{

STEP 1) PLAN. Read the university president's strategic plan that establishes the: student retention quota (90%); departmental GPA quota (3.28); and teacher evaluation quota (5.82 on a scale from 1 to 7).

STEP 2) PREPARE. Introduce yourself to students who: lack prerequisites, know they cheat without expulsion, and know they can get rid of tough teachers; and announce that all assignments will be group projects (thereby making official what will happen anyway).

STEP 3) TEACH. Begin your lecture, and watch them lean back and say "I could hire someone to do that," just before tuning out.

STEP 4) GRADE. Identify the kid who cuts class, then make quota by giving everyone else a 4.00.

}

UNTIL (jaded || retired || fired);

Business schools practice what they preach: find out what your customers want (high grades, low effort), deliver it efficiently (grade group presentations during class), and charge what the market will bear (kids do not care as long as mom pays).

One may then wonder if there is any hope of an executive learning more than a slogan or two about information security.

To be fair, the majority of executives work hard and keep their eye on the ball. But what is the ball? Traditionally, industries that supply commodities (e.g. agriculture, forestry, mining, structural steel) compete on cost, so the above mentioned ball is accounting and cost reduction. Industries that supply consumer goods (e.g. apparel, consumer electronics, cosmetics, fast food) compete on product features, so the ball is market research, product design, and advertising. Put simply, executives with marketing and accounting skills have the greatest influence on the top and bottom lines, respectively.

Consequently, what executives most readily grasp about computers and networks are opportunities that relate to marketing and accounting. Computers present an opportunity to reduce cost by automating vast amounts of clerical labor; while networks present an opportunity to expand sales by creating a whole new distribution channel.

Executives do not normally focus on information security until after a threat emerges that impacts their area of interest (e.g., a denial of service attack that hurts on-line sales); or unless government regulation forced the issue (e.g. HIPAA for protection of medical data, Gramm-Leach-Bliley Act (GLBA) for protection of financial data).

So the question becomes: How can executives make rational decisions about an issue as unfamiliar and peripheral (to them) as information security? The answer lies in adapting a process well-known to them.

During most of the year executives execute a plan while staying within budget. However, once a year, they step back and ask "Does any of this make sense?" They follow a top-down approach like this:

- 1) Define the scope of business;
- 2) Form a business strategy;
- 3) Support the business strategy with a set of functional strategies (e.g. marketing strategy, manufacturing strategy, financing strategy);

4) Derive resource requirements (e.g. manpower and capital); and

5) Integrate all that into an Annual Plan and Budget.

The remainder of the year, they execute this Annual Plan & Budget as efficiently as possible, making adjustments as needed.

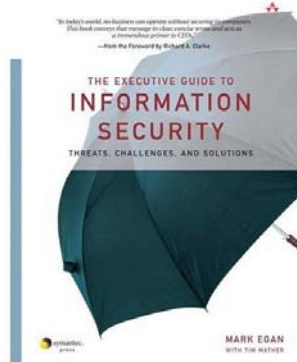
So, executives should go back and ask "Do we need an information security strategy to support our business strategy?" If so, then they should form one (step 3), then derive corresponding resource requirements (step 4), and finally integrate all that into the Annual Plan and Budget (step 5). Then go execute the new plan.

Mark Egan with Tim Mather have come to the rescue by writing *The Executive Guide to Information Security: Threats, Challenges, and Solutions*.

To motivate executives, Egan and Mather start by describing a number of challenges that the executive will face. These should be familiar to most readers.

Growing demand for e-commerce is imposing tougher requirements for ease-of-use and information security. Attacks are increasing in number and sophistication. There are no vendors with turn-key solutions, only vendors with point solutions. There is a shortage of qualified information security staff. Government regulation is on the rise (e.g. HIPAA and GLBA). The popularity of wireless computing and a mobile workforce is exposing more systems to attack.

The main resource requirements are: people, processes, and technology. These are discussed in some detail and helpful check lists are provided to let the executive: evaluate his present situation, decide where the business needs to go, and then build a plan and budget to get there.



Egan and Mather conclude with a look at the future. They predict future threats that will be more complex and spread faster. They see a shift in hacker demographics away from the amateurs, and towards organized crime, terrorist organizations, and nation states.

It is to the shift towards state sponsored hacking that we now turn.

Information Warfare

The United States does not meet the dictionary definition of an empire. That said, the United States Government (USG) has cobbled together an international system of unprecedented scale and complexity---well beyond what the House of Habsburg could have imagined. And, significantly, the governments that participate in the current system, do so willingly, and mainly because they can obtain the benefits of prosperity and security with little loss of self-determination.

Let us focus on security.

When DoD was created in 1947 by act of Congress, the GDP of the US constituted 50% of the economic output of the entire world. At that time, every Service (Army, Navy, Marines, Air Force) could afford its own unique equipment, its own industrial base, and its own political constituency. Since then US GDP has declined to about 20% of global output---not because the US declined in absolute terms, but because the international system helped others catch up.

Securing a planet is not cheap. US and allied leaders have struggled mightily to economize. Robert McNamara imposed the Planning, Programming, Budgeting and Execution (PPBE) Process (see JP 5-0 Joint Operation Planning, 26 December 2006). A new procurement process favored multi-national, multi-service, multi-mission systems (e.g. F-4 Phantom II, aka "The World's Largest Distributor of MiG Parts"). Engineers tackled the daunting problem of interoperability with NATO allies. The Joint Chiefs of Staff (JCS) formalized the Joint Doctrine and released it in a set of Joint Publications.

However, the need for joint and multi-national forces spanning the globe, led to an almost inconceivable demand for information systems. It led to something amazing:

The Global Information Grid (GIG)

The [DoD's] globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (JP 6-0 Joint Communications System, 20 March 2006, Glossary)

This sprawling federation of systems is what allows airman in California to operate Unmanned Air Vehicles (UAV) over Afghanistan, collect still and motion imagery called Combat Camera (COMCAM), and identify targets. Indeed, the GIG is what enables any friendly combatant to identify targets and submit them to the Joint Targeting Coordination Board (JTCB), which will prioritize them, cut Air Tasking Orders (ATO), and generate sorties from any Service with strike aircraft.

Responsibility for Global Network Operations (GNO) and defense rests with the Commander United States Strategic Command (CDRUSSTRATCOM). The priority component of the GIG is the National Military Command System (NMCS) which connects the President, SecDef, and the JCS. Another component is the Nuclear Command and Control System (NCCS) which connects the President to the nuclear forces.

The GIG is highly valuable. A loss of the NMCS might decapitate the military. A hacker able to gain control of the NCCS might disarm and preemptively attack the United States.

This brings us to the matter of Information Operations (IO).

US Information Operations

IO has recently been reorganized to incorporate recent combat experience. According to Joint

Doctrine (JP 3-13 Information Operations), IO consists of five core capabilities: Psychological Operations (PSYOP), Operations Security (OPSEC), Military Deception (MILDEC), Electronic Warfare (EW), and Computer Network Operations (CNO). The first three have been



around for thousands of years. EW has been around for a century, while CNO is the most recent.

CNO, along with EW, is used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure. For purposes of military operations, CNO are divided into Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE).

Americans seem primarily concerned with maintaining information superiority and information availability, to dispel the "fog of war" described by Carl von Clausewitz.

But to complete the Tale of Two Libraries we need to look at China.

Chinese Information-War Theory

The recent "informationized" wars in the Balkans and the Iraq attracted military observers from many countries, including China. The Chinese noted with interest the counter-measures fielded by the Serbs.

During the late 1990's it became clear that Information Warfare (IW) was having a growing influence on Chinese military thinking.

At first Chinese IW theory followed that of the Americans. But the Chinese quickly evolved IW theories with "Chinese characteristics"---ones that Americans are notoriously ill-equipped to understand---such as: stratagem, People's War, and the use of the Marxist-Leninist dialectic thought processes in evaluating the operational environment.

Chinese historiography revels in the stratagems that courtiers use to gain power, and commanders use to win battles (e.g. "Records of the Historian," SiMa Qian, and "Art of War," Sun Zi). Indeed, a fascination with stratagem is thoroughly imbedded in Chinese culture (e.g. "Romance of the Three Kingdoms," and "The Secret Art of War: the 36 Stratagems"). It would jar most Americans to hear ordinary Chinese say that "Family, business, and war are all the same." The dictionary definition of "stratagem," as an artifice or trick in war for deceiving the enemy; does not really match the Chinese concept, which is more about controlling the opponent's perception of reality, and regulating his level of fear.

The doctrine of People's War envisions organizing "the masses" into a guerilla war against an invader. When applied to IW, it envisions organizing millions of civilians with laptops into a massive hacking campaign---in support of IW operations by the People's Liberation Army (PLA) and militias.

Marxist-Leninist dialectic thought processes have led China to organize IW very differently that the US.

[Timothy L. Thomas](#) (shown at right), author of *Chinese Information-War Theory and Practice*, had rendered us all a service by collecting and analyzing a good number of Chinese IW papers, published 1995-2003, and translated by the Foreign Broadcast Information Service (FBIS).



Thomas has chapters on the Chinese views of IW in Kosovo and Iraq.

The Chinese fascination with stratagem has resulted in an strategy-stratagem-IW integration, and Thomas give many examples. He notes that Chinese IW theorists have discussed the possibility of automating the application of stratagems in IW. Chinese have recognized the congenital vulnerabilities of the Internet, and note the need for a secure alternative.

During the major combat phase of the Iraq war, Chinese commentators did a poor job of analyzing the campaign. Senior officials have recognized this weakness and have since gotten serious about IW. Thomas discussed the case of the Second Artillery Corp, China's strategic nuclear forces, which have become a focus of IW simulation and training exercises.

A little disturbing is the Chinese notion that there is no distinction between war and peace in IW, something that a few Americans (e.g. system administrators at the national laboratories responsible for nuclear weapons development) have begun to appreciate.

Coda

So why might the Chinese government get organized for IW, and then attack a library, let alone a Marxist one? The International Herald Tribune explains:

While some might find it odd that the government created by Mao's Communist Revolution would be behind an effort to deny access to the texts so important to its founding, Basgen said he did not.

"It is ironic for people who don't know what is going on in China," he said. "The Chinese so-called Communist government has nothing to do with communism. It has been going toward capitalism for a long time."

The Marxist archive does not even consider Mao to be a true Marxist. He is considered a "reference writer," along with other authors like Adam Smith, Stalin and Jean-Jacques Rousseau. Basgen said Mao was excluded because he failed a key question: "Did he serve to liberate working people?"

In the long view of history, Chinese Communism is just another dynastic cycle: established by conquest, ending in corruption, and ever touchy about its legitimacy.

It seems that an undeclared war has begun. State sponsored hacking is on the rise. If your organization has valuable information, you would do well to cultivate a commitment to information security from those at the executive level.

DC ACM CALENDAR AT A GLANCE

January 27	Executive Council Meeting (open to all members)
February 8	Guest Speaker Joey Ponthieux, "3D Animation and Modeling for Aerospace"
February 24	Executive Council Meeting (open to all members)

Sponsorship Opportunities

Your company's logo could be here!

Renewable Annual DC ACM Sponsorships

Bronze: \$500

Silver: \$1,000

Gold: \$5,000 (one per year)

All sponsors will be prominently recognized for one year on the DC ACM website, on the membership pamphlet, and at major events. Please email fundraising@dcacm.org if your company is interested.

Special corporate sponsor benefits for the Fall 2009 and Spring 2010 Professional Development Seminars	
Bronze	5 employee discounts
Silver	10 employee discounts
Gold	unlimited employee discounts

Note: The discount is equivalent to the DC ACM Member Discount and will apply to one seminar. An employee may use multiple discounts if authorized by the sponsor's management.

All sponsors/donors will receive a letter from the DC ACM Chair verifying the receipt of their donation.

About DC ACM

<http://www.dcacm.org>

The Washington, D.C. Chapter of the Association for Computing Machinery (DC ACM) was formally established on November 1, 1958. We are a local professional chapter of the Association for Computing Machinery (ACM), which was founded in 1947. Currently there are more than 2,200 ACM members in the Washington Metropolitan Area.

The DC ACM is a non-profit 501(c)(3) association (EIN 526066536) that supports educational activities and career development for the local IT professional community, as well as nurturing future generations of computer scientists, network engineers, and tech policy specialists in the Washington, D.C. area. Among other activities, we give awards to junior and senior high school students for exceptional science fair projects in the computer science field and we sponsor educational lectures for the general public.

DC ACM Executive Council

Click on the name to email.

Chair	Benjamin Schultz
Vice Chair	Kent Miller
Treasurer	Teresa Hone
Secretary	Andrew Conklin
Member at Large	Mackenzie Morgan
Communications	Cora Dickson
Membership	Isaac Christoffersen
PDC	Eric Noriega
Programs	William Fielder
Awards	Mark Nolan

Executive Council Meetings are held once a month. They are open to all interested parties, though only EC Members have voting power on any motions raised in the meeting.

Location:

Radio Free Asia
2025 M Street NW
Between 20th and 21st Streets
Ground Floor Conference Room

Closest Metro Stations: Dupont Circle and Farragut North, Red Line

Parking: Free on the street after 6:30pm; garage next door to the meeting room charges \$5.00. Another garage on 19th Street is open until midnight and if you enter after 5pm it costs only \$7.00.

Become an Active Chapter Member

- Join the Professional Development Committee
- Join the Website Team
- Come to DC ACM meetings and events! They are always metro accessible.