and you will know us by the trail of frames

Officially disapproved by THE MAN

one furious wire [the theory and practice of network subversion and hostile computing]

Give, Sympathize, Control.
Infiltrate, Destroy, Rebuild.

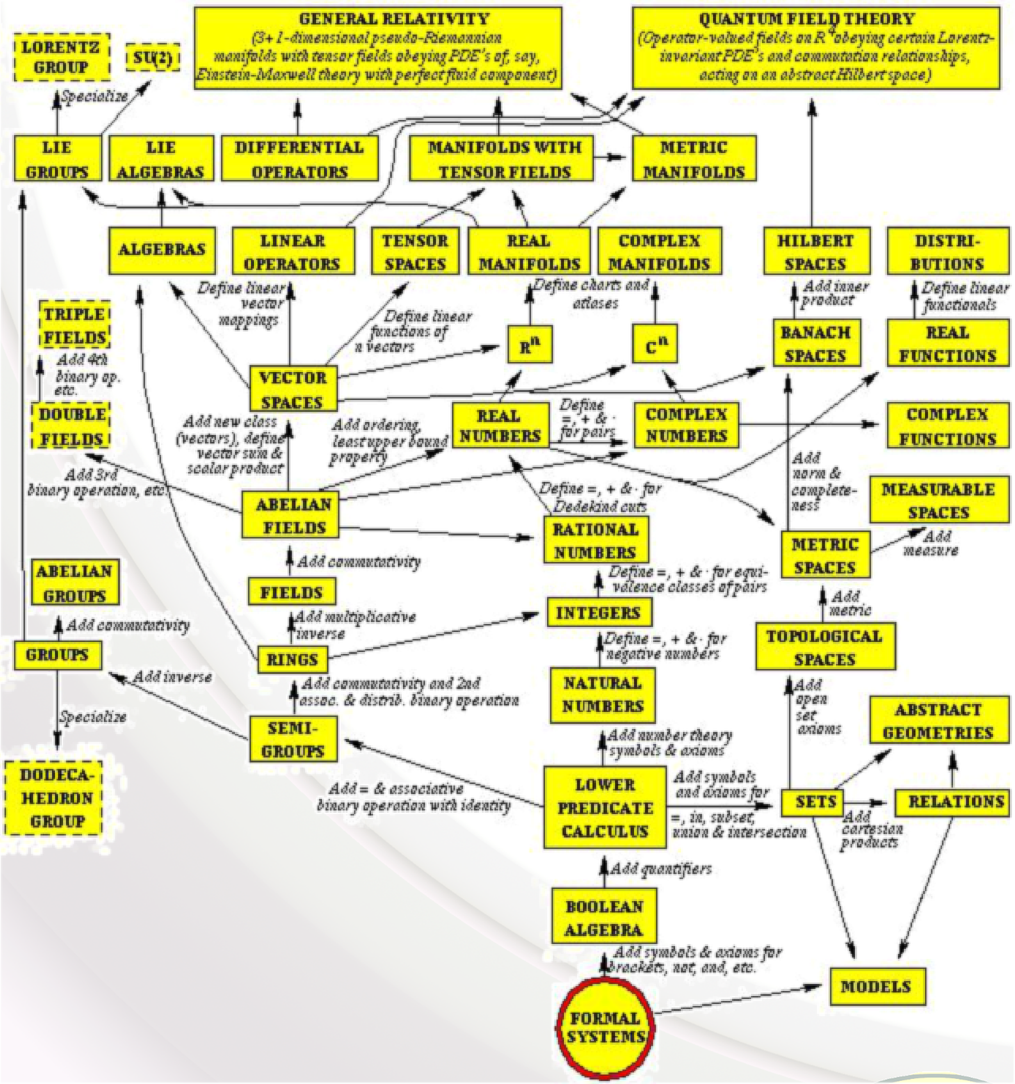
Not so much a “focused talk” as...discoursing volubly

- In the spirit of this hacker collective, there's less an agenda to this talk than something of an information firehose. Alternate titles considered:
  - “Higgs, Hertz, and HTTPS”
  - “Another day gone. Goddamn Wikipedia.”
  - “T. S. Eliot's *The Wasteland*”

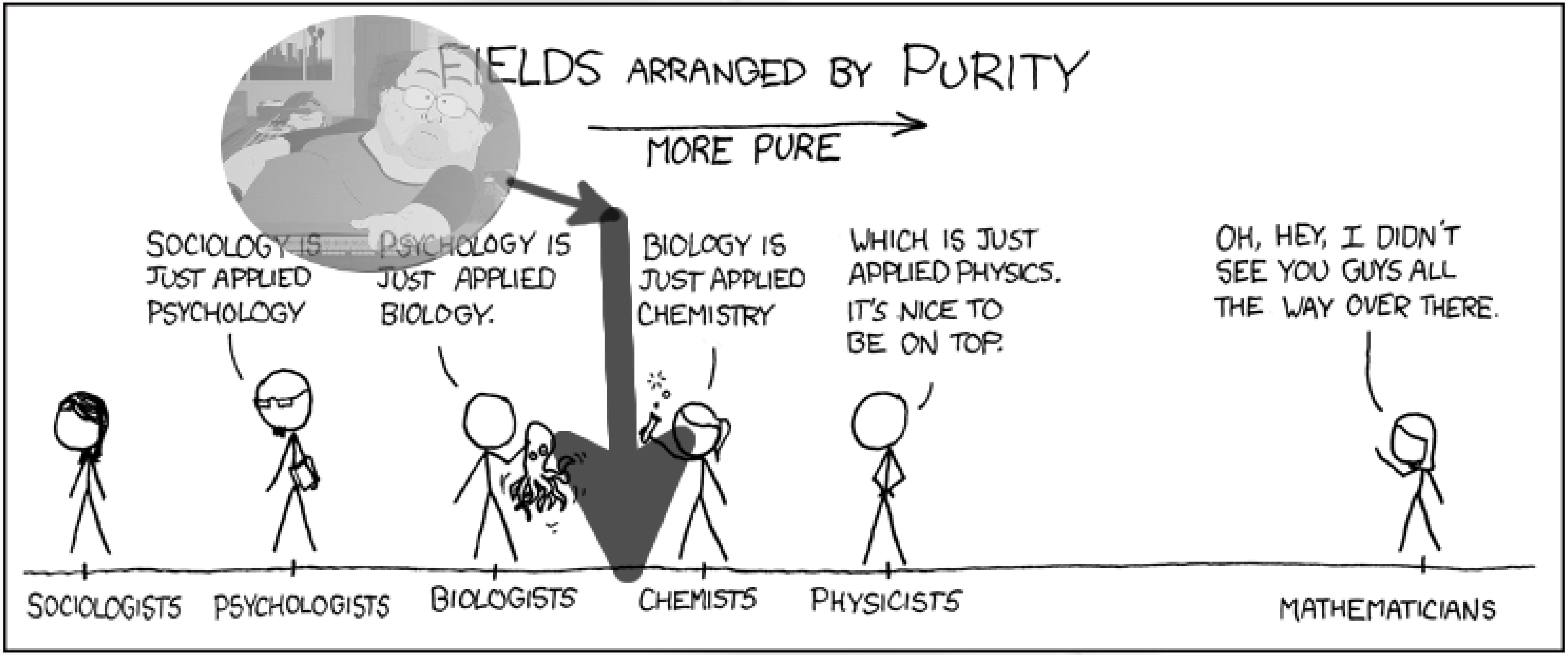
- Don't feel let down. Network security sucks. Its last good result was [Landi 1992]. The field's packed with canards and shysters.

- Five parts, loosely connected at best. I left more out than I put in, believe me. Try to keep up. Have fun.

- I'm not an expert on everything we'll discuss. Jump in whenever. Answer and ask questions!


GENERAL RELATIVITY
(3+1-dimensional pseudo-Riemannian manifolds with tensor fields obeying PDE's of, say, Einstein-Maxwell theory with perfect fluid component)
QUANTUM FIELD THEORY
(Operator-valued fields on R⁴ obeying certain Lorentz-invariant PDE's and commutation relationships, acting on an abstract Hilbert space)
LORENTZ GROUP
SU(2)
Specialize
LIE GROUPS
LIE ALGEBRAS
DIFFERENTIAL OPERATORS
MANIFOLDS WITH TENSOR FIELDS
METRIC MANIFOLDS
ALGEBRAS
LINEAR OPERATORS
TENSOR SPACES
REAL MANIFOLDS
COMPLEX MANIFOLDS
HILBERT SPACES
DISTRI-BUTIONS
Define linear vector mappings
Define linear functions of n vectors
Define charts and atlases
Add inner product
Define linear functionals
TRIPLE FIELDS
Add 4th binary op. etc.
DOUBLE FIELDS
Rⁿ
Cⁿ
BANACH SPACES
REAL FUNCTIONS
VECTOR SPACES
REAL NUMBERS
Define =, + & · for pairs
COMPLEX NUMBERS
COMPLEX FUNCTIONS
Add new class (vectors), define vector sum & scalar product
Add ordering, least upper bound property
Add 3rd binary operation, etc.
ABELIAN FIELDS
Define =, + & · for Dedekind cuts
Add norm & complete-ness
MEASURABLE SPACES
RATIONAL NUMBERS
METRIC SPACES
Add measure
ABELIAN GROUPS
Add commutativity
FIELDS
Define =, + & · for equi-valence classes of pairs
Add metric
Add commutativity
Add multiplicative inverse
INTEGERS
GROUPS
RINGS
Define =, + & · for negative numbers
TOPOLOGICAL SPACES
Add inverse
Add commutativity and 2nd assoc. & distrib. binary operation
NATURAL NUMBERS
Specialize
SEMI-GROUPS
Add open set axioms
ABSTRACT GEOMETRIES
Add number theory symbols & axioms
DODECA-HEDRON GROUP
Add = & associative binary operation with identity
LOWER PREDICATE CALCULUS
Add symbols and axioms for =, in, subset, union & intersection
SETS
RELATIONS
Add cartesian products
Add quantifiers
BOOLEAN ALGEBRA
Add symbols & axioms for brackets, not, and, etc.
MODELS
FORMAL SYSTEMS

You know that guy using valuable science time to hunt win32 exploits?


FIELDS ARRANGED BY PURITY
MORE PURE
SOCIOLOGY IS JUST APPLIED PSYCHOLOGY
PSYCHOLOGY IS JUST APPLIED BIOLOGY.
BIOLOGY IS JUST APPLIED CHEMISTRY
WHICH IS JUST APPLIED PHYSICS. IT'S NICE TO BE ON TOP.
OH, HEY, I DIDN'T SEE YOU GUYS ALL THE WAY OVER THERE.
SOCIOLOGISTS
PSYCHOLOGISTS
BIOLOGISTS
CHEMISTS
PHYSICISTS
MATHEMATICIANS

Don't be that guy.

"Studying compilers makes you a better programmer.
Studying computer architecture makes you a better person."
--Brian Ouellette, 2012-07-16

Part 1: I Sing the Battlefield Electric

(The Burial of the Dead)

PRIMARY SOURCES

- Leon-Garcia and Widjaja, “Communications Networks” 2004
- Ward and Halstead, “Computation Structures” 1990
- IEEE 802.3 and 802.11 standards
- Feynman, “Lectures on Physics” 1970
- Fleisch, “A Student's Guide to Maxwell's Equations” 2008
- Bardwell, “I'm Going To Let My Chauffeur Answer That” 2003
- Spurgeon, “Ethernet: The Definitive Guide” 2007
- Skolnik, “Introduction to Radar Systems” 2003
- ITU, ANSI, and ISO standards, FCC policy
- Wikipedia by the assload
- Black, “The Finest Machine” 2013(?)

Why Digital Communications?

- Reliable transmission: arbitrary fidelity at finite cost.
- Digital decouples channel from absolute physical waveform
  - A finite signal, digitized,
    can be reliably transmitted
    in **any** digital system
    (right: IP over Avian Carrier, IpoAC, RFC 1149)

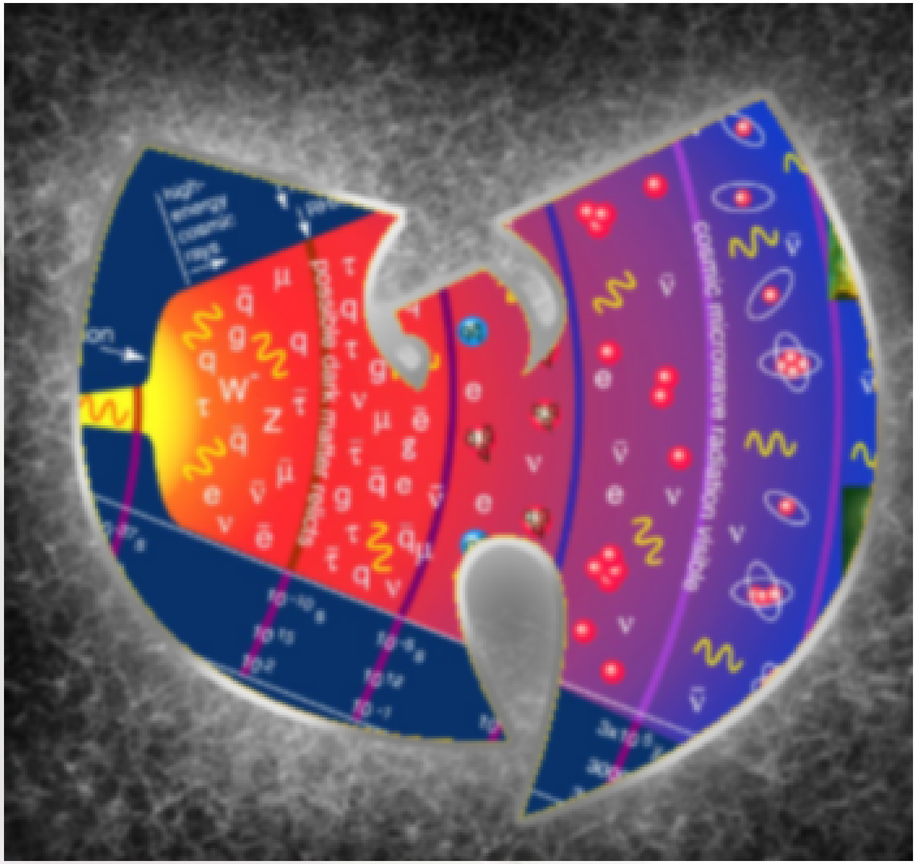
- And of course, perfectly reproducible retransmission.
  - Originally important for telco long-distance (L2 repeaters)
  - Now critical for peer-to-peer file sharing (L5+ repeaters)
  - Bittorrent sucks on VHS
    (right: Weatherputer!)

Never underestimate the bandwidth of a station wagon full of tapes hurtling down the highway.

Our story begins ~13.7 billion years ago...

It is a time of quarks, gluons, radiation and other precursors of dinosaurs(*).

It is also the time of the WU-TANG CLAN, who are forever.



* "Terrible lizards"

Physics Review – Force

aka “Why Electromagnetics?”

- Four fundamental interactions: N_s, N_W, Em, G
- $\alpha_s = 10^2\alpha = 10^6\alpha_W = 10^{39}\alpha_g$ (actual $\alpha_s = 137\alpha$)
- Via gauge bosons: γ, g, $W^\pm$, Z^0, (maybe) G
- Gravity: too weak, affects all particles
- Weak nuclear: too short-range (heavy W, Z)
- Strong nuclear: too strong (can't create a strong nuclear force potential)
- Affects p, $\bar{p}$, $e^\pm$, $\mu^\pm$, $\tau^\pm$, $W^\pm$ ($Q \neq 0$, $Q = (k \in \mathbb{Z})e$)

Notes regarding previous slide

- Gravitation matters relative to electricity for the same reason electricity matters relative to the strong force: net charge at a distance is almost always 0

- Gravity works only in one direction – attraction – while electromagnetics work in two – attraction/repulsion. Chromodynamics work on three – short-range attract/repulse, long-range impotence, self-interaction (we're ignoring degeneracy pressures).
  - SLAC deep inelastic scattering experiments

- Very much less input energy is required to ionize (strip an electron) an atom than to remove a proton.

- Neutron decays into p + W^-, W^- into e- and e-antineutrino via d->u (B^-).
- Proton decays into n + W^+, W^+ into e+ (positron) and e-neutrino (B^+, requires $2m_ec^2$).
- Proton merges with inner-shell e- in K-capture, releasing monoenergetic neutrino.
- W, p, e are charged.

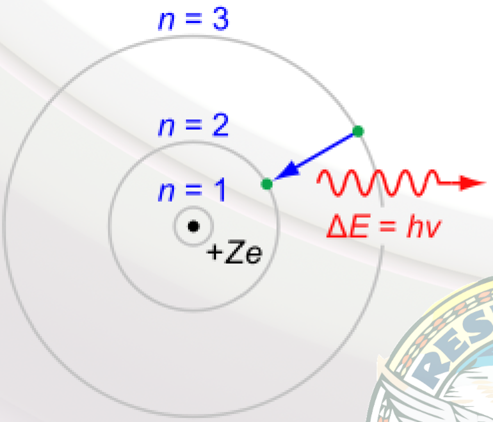
Physics Review – Photons

Never have I known a finer gauge boson

$$E = mc^2 = \sqrt{p^2 c^2 + m_0^2 c^4}$$

$$p = \frac{E}{c} = \frac{h\nu}{c} = \frac{h}{\lambda}$$

- A pleasant force carrier to work with
- Spectrum of emission allows precise control of energy
- Zero rest mass implies negligible minimum energy investment
  - Higgs doesn't couple to photons – this is the source of QED symmetry breaking
  - Still affects the stress-energy tensor, and is affected by gravity (lensing)
- Don't decay (can produce virtual particles)
- No self-interaction (unlike gluons): no three-pronged Feynman diagrams
- “Inelastic scattering” (Compton effect) is absorption followed by emission of a lower-energy photon
- Two polarizations (helicities), three params (**k**-vector)
- Nothing can propagate more quickly
- Energy comes from relativistic momentum



Notes regarding previous slide

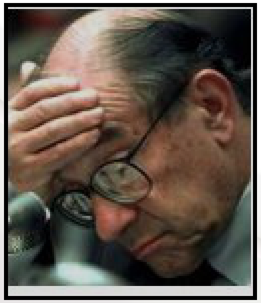
- Photons only couple with things having charge.
  - H^0 (Higgs boson) does not have charge.
  - Photons are restricted to two helicities. Other electroweaks have helicities + mass.
- Z boson couples to charge + weak isospin, and carries weak isospin.
  - H^0 has weak isospin.
- W boson couples to charge + weak isospin, carries charge and weak isospin.
- Gluons couple to color charge and carry color charge.
- Wave vector points in the direction of media in isotropic media.
  - In anisotropic, this is not maintained.

Physics Review – Waves

- A disturbance in spacetime which transfers energy
- Electromagnetic and mechanical
  - The former is propagated by a field and strictly traverse, the latter by material and has three components (traverse, longitudinal, surface)
- Electromagnetic waves are mediated by photons (the quantum of emag interaction) at the speed of light in that substance.
- Electrically-charged particles are affected (accelerated) by the electromagnetic field.

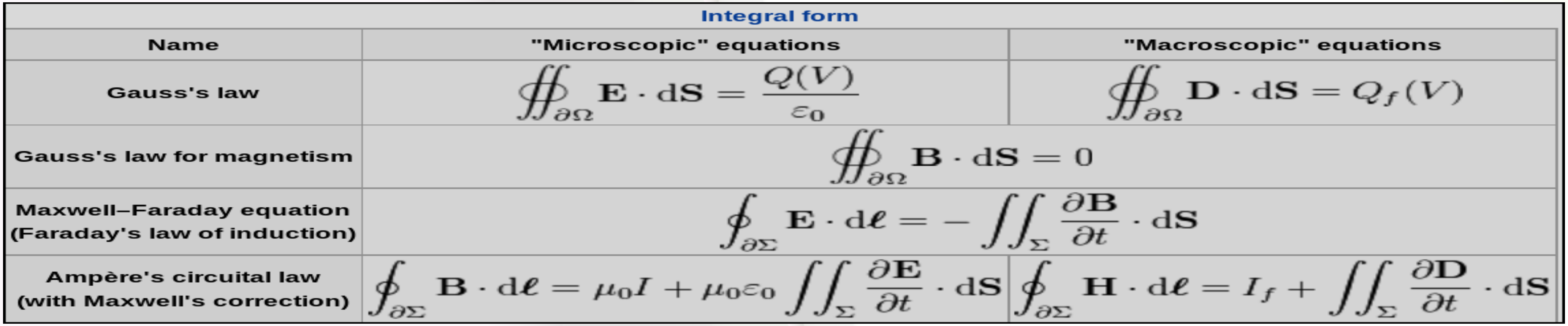
Physics Review – *ψ* Function Fun

- Uncertainty principle deals with product of *momentum* and position, **not** velocity. Photon's known velocity is not a problem.
- Electromagnetic waves have **nothing** to do with wave-particle duality. Rather, Maxwell's equations *facilitate* and indeed ***require*** wavelike propagation of the field.
- 1D wave: $-\partial_t^2 u + c^2 \Delta u = 0$ (Δ is the Laplacian, ∇^2)
  - Admits fully general solution $F(x - ct) + G(x + ct)$
- Adding energy in the direction of propagation doesn't increase velocity, but reduces wavelength
  - *cref* relativity's dilation in the direction of motion



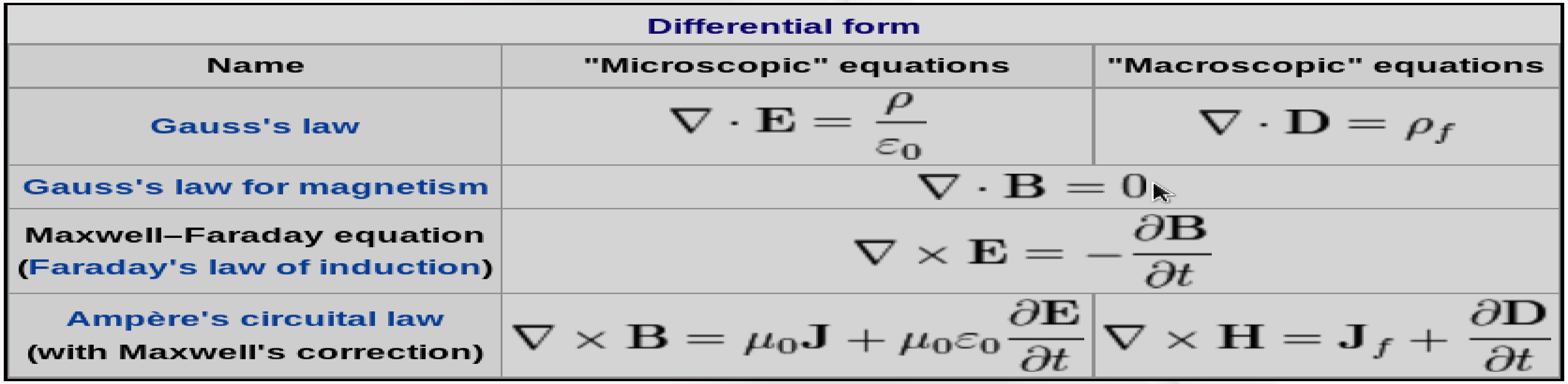
Physics Review – Electromagnetics

“How many ways can we write Maxwell's Equations?”



Integral form

Name	"Microscopic" equations	"Macroscopic" equations
Gauss's law	$\oiint_{\partial\Omega} \mathbf{E}\cdot \mathrm{d}\mathbf{S} = \frac{Q(V)}{\varepsilon_0}$	$\oiint_{\partial\Omega} \mathbf{D}\cdot \mathrm{d}\mathbf{S} = Q_f(V)$
Gauss's law for magnetism	$\oiint_{\partial\Omega} \mathbf{B}\cdot \mathrm{d}\mathbf{S} = 0$	
Maxwell–Faraday equation (Faraday's law of induction)	$\oint_{\partial\Sigma} \mathbf{E}\cdot \mathrm{d}\boldsymbol{\ell} = -\iint_{\Sigma} \frac{\partial \mathbf{B}}{\partial t}\cdot \mathrm{d}\mathbf{S}$	
Ampère's circuital law (with Maxwell's correction)	$\oint_{\partial\Sigma} \mathbf{B}\cdot \mathrm{d}\boldsymbol{\ell} = \mu_0 I + \mu_0\varepsilon_0 \iint_{\Sigma} \frac{\partial \mathbf{E}}{\partial t}\cdot \mathrm{d}\mathbf{S}$	$\oint_{\partial\Sigma} \mathbf{H}\cdot \mathrm{d}\boldsymbol{\ell} = I_f + \iint_{\Sigma} \frac{\partial \mathbf{D}}{\partial t}\cdot \mathrm{d}\mathbf{S}$



Differential form

Name	"Microscopic" equations	"Macroscopic" equations
Gauss's law	$\nabla\cdot\mathbf{E} = \frac{\rho}{\varepsilon_0}$	$\nabla\cdot\mathbf{D} = \rho_f$
Gauss's law for magnetism	$\nabla\cdot\mathbf{B} = 0$	
Maxwell–Faraday equation (Faraday's law of induction)	$\nabla\times\mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$	
Ampère's circuital law (with Maxwell's correction)	$\nabla\times\mathbf{B} = \mu_0\mathbf{J} + \mu_0\varepsilon_0\frac{\partial \mathbf{E}}{\partial t}$	$\nabla\times\mathbf{H} = \mathbf{J}_f + \frac{\partial \mathbf{D}}{\partial t}$

The electric field of one charge (Feynman 1950 (published 1963)):

$$\boldsymbol{E} = \frac{-q}{4\pi\epsilon_0}\left[\frac{\boldsymbol{e}_{r'}}{r'^2} + \frac{r'}{c}\frac{d}{dt}\left(\frac{\boldsymbol{e}_{r'}}{r'^2}\right) + \frac{1}{c^2}\frac{d^2}{dt^2}\boldsymbol{e}_{r'}\right]$$

The electromagnetic wave equations (assuming flat background):

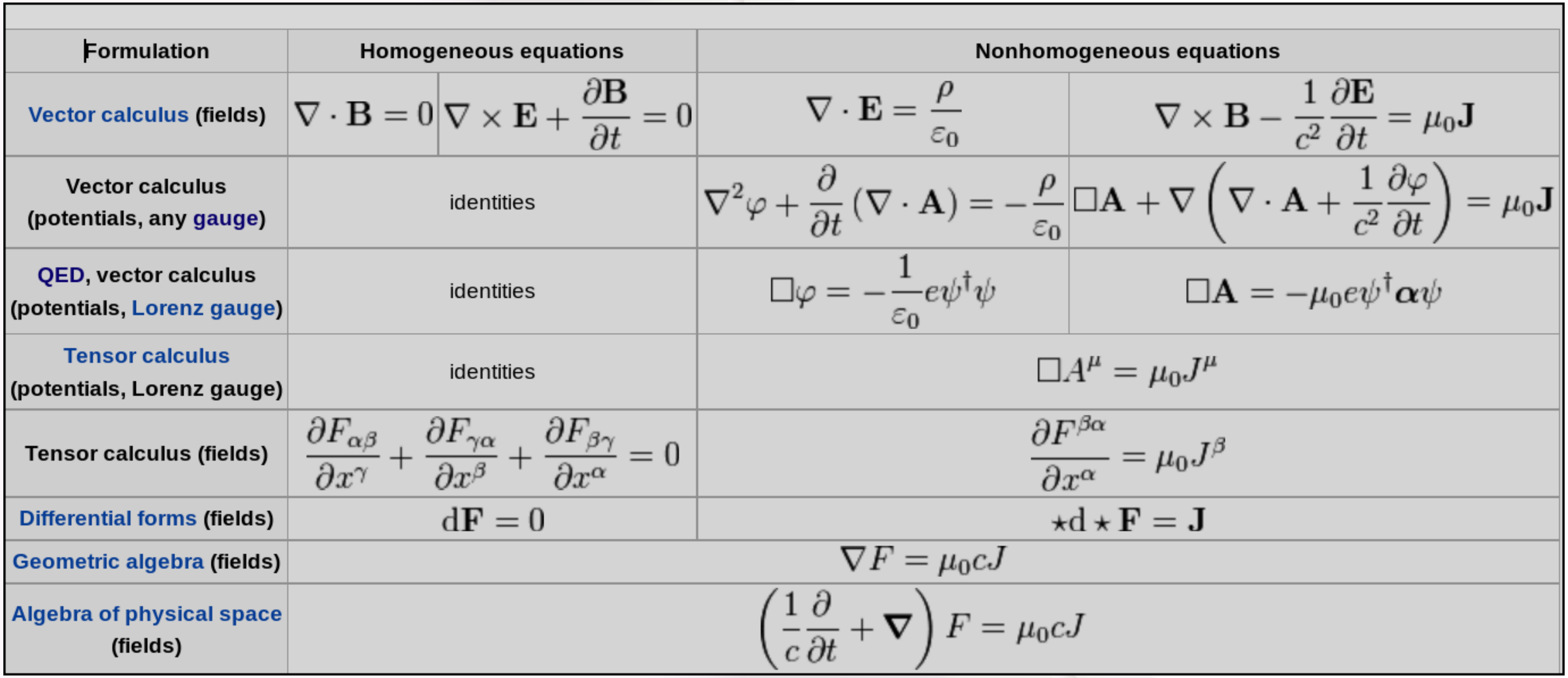
$$\left(\nabla^2 - \mu\varepsilon\frac{\partial^2}{\partial t^2}\right)\boldsymbol{E} = 0$$

$$\left(\nabla^2 - \mu\varepsilon\frac{\partial^2}{\partial t^2}\right)\boldsymbol{B} = 0$$

$$c = \frac{1}{\sqrt{\mu\varepsilon}}$$

Too many ways

(This doesn't cover changes of units ala cgs, free space variants, etc)



Formulation	Homogeneous equations		Nonhomogeneous equations	
Vector calculus (fields)	$\nabla \cdot \mathbf{B} = 0$	$\nabla \times \mathbf{E} + \frac{\partial \mathbf{B}}{\partial t} = 0$	$\nabla \cdot \mathbf{E} = \frac{\rho}{\varepsilon_0}$	$\nabla \times \mathbf{B} - \frac{1}{c^2}\frac{\partial \mathbf{E}}{\partial t} = \mu_0 \mathbf{J}$
Vector calculus (potentials, any gauge)	identities		$\nabla^2 \varphi + \frac{\partial}{\partial t}(\nabla \cdot \mathbf{A}) = -\frac{\rho}{\varepsilon_0}$	$\Box \mathbf{A} + \nabla\left(\nabla \cdot \mathbf{A} + \frac{1}{c^2}\frac{\partial \varphi}{\partial t}\right) = \mu_0 \mathbf{J}$
QED, vector calculus (potentials, Lorenz gauge)	identities		$\Box \varphi = -\frac{1}{\varepsilon_0} e \psi^\dagger \psi$	$\Box \mathbf{A} = -\mu_0 e \psi^\dagger \boldsymbol{\alpha} \psi$
Tensor calculus (potentials, Lorenz gauge)	identities		$\Box A^\mu = \mu_0 J^\mu$	
Tensor calculus (fields)	$\frac{\partial F_{\alpha\beta}}{\partial x^\gamma} + \frac{\partial F_{\gamma\alpha}}{\partial x^\beta} + \frac{\partial F_{\beta\gamma}}{\partial x^\alpha} = 0$		$\frac{\partial F^{\beta\alpha}}{\partial x^\alpha} = \mu_0 J^\beta$	
Differential forms (fields)	$\mathrm{d}\mathbf{F} = 0$		$\star \mathrm{d} \star \mathbf{F} = \mathbf{J}$	
Geometric algebra (fields)	$\nabla F = \mu_0 c J$			
Algebra of physical space (fields)	$\left(\frac{1}{c}\frac{\partial}{\partial t} + \boldsymbol{\nabla}\right) F = \mu_0 c J$			

$\Box$ is the **d'Alembertian** operator

$$\frac{1}{c^2}\frac{\partial^2}{\partial} t^2 - \nabla^2$$

ohgodwhatthehellisthat

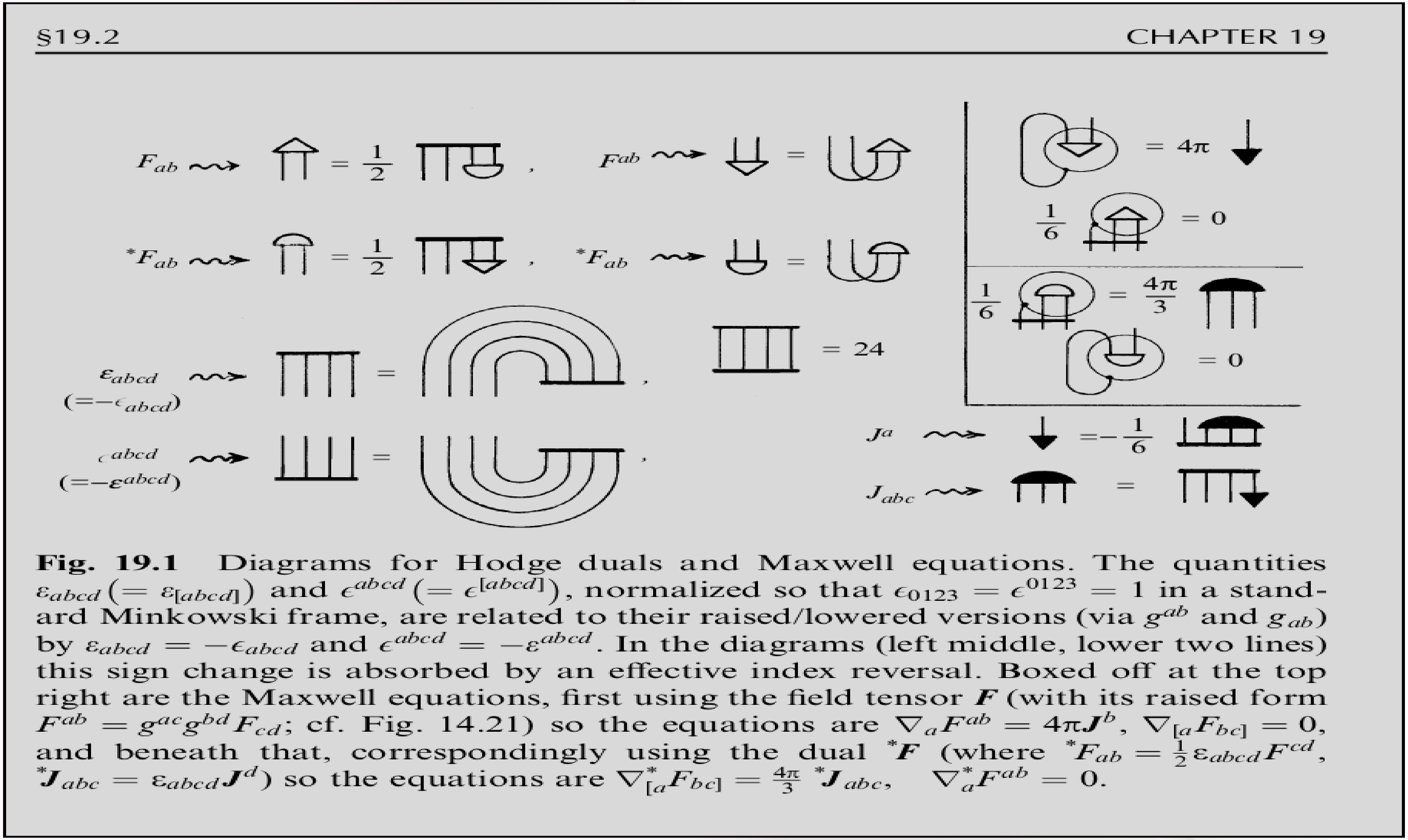
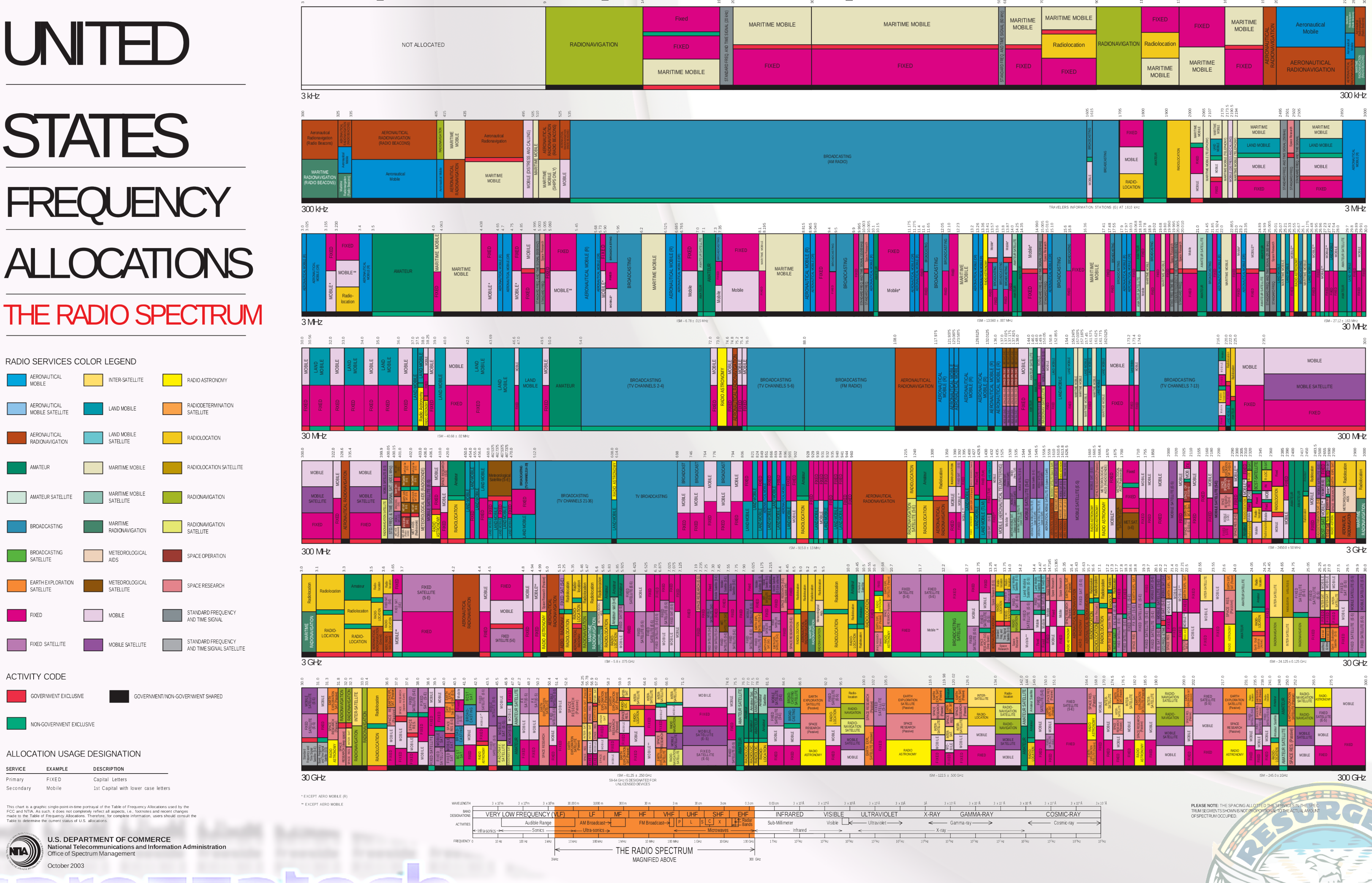


Fig. 19.1 Diagrams for Hodge duals and Maxwell equations. The quantities $\varepsilon_{abcd} (= \varepsilon_{[abcd]})$ and $\epsilon^{abcd} (= \epsilon^{[abcd]})$, normalized so that $\epsilon_{0123} = \epsilon^{0123} = 1$ in a standard Minkowski frame, are related to their raised/lowered versions (via g^{ab} and g_{ab}) by $\varepsilon_{abcd} = -\epsilon_{abcd}$ and $\epsilon^{abcd} = -\varepsilon^{abcd}$. In the diagrams (left middle, lower two lines) this sign change is absorbed by an effective index reversal. Boxed off at the top right are the Maxwell equations, first using the field tensor $\boldsymbol{F}$ (with its raised form $F^{ab} = g^{ac}g^{bd}F_{cd}$; cf. Fig. 14.21) so the equations are $\nabla_a F^{ab} = 4\pi \boldsymbol{J}^b$, $\nabla_{[a}F_{bc]} = 0$, and beneath that, correspondingly using the dual ${}^*\boldsymbol{F}$ (where ${}^*F_{ab} = \frac{1}{2}\varepsilon_{abcd}F^{cd}$, ${}^*\boldsymbol{J}_{abc} = \varepsilon_{abcd}\boldsymbol{J}^d$) so the equations are $\nabla^*_{[a}F_{bc]} = \frac{4\pi}{3}\,{}^*\boldsymbol{J}_{abc}$, $\nabla^*_a F^{ab} = 0$.

I have never understood anything about **Fig 19.1**, nor has anyone even been willing to attempt to explain it. I assume this is because they also no clue what, if anything, is being described. I check often for errata involving printers or seizures.

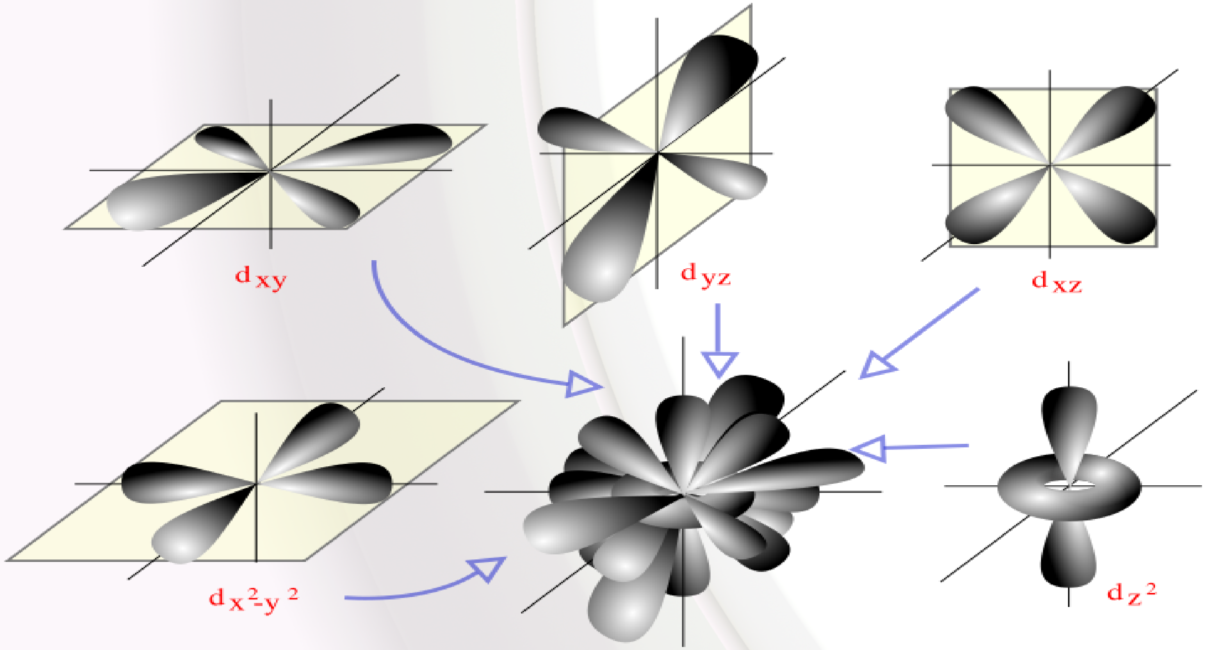
The (Low-ν) US Spectrum

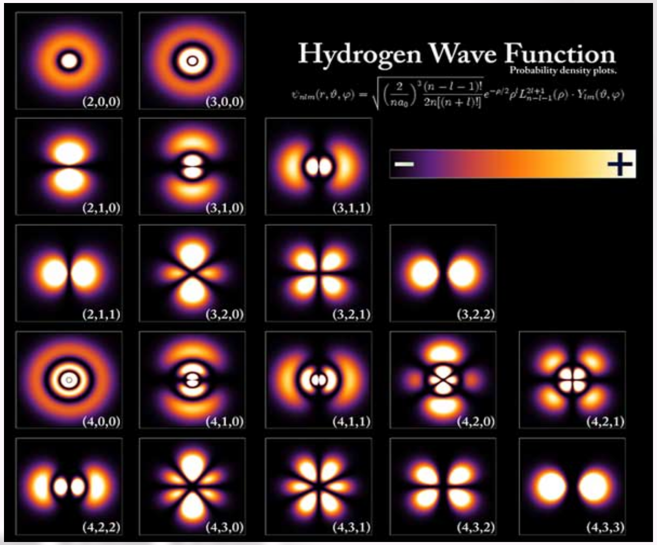


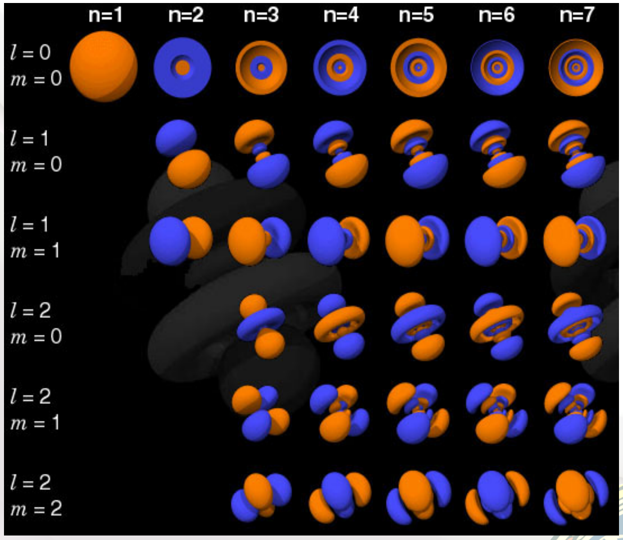
Physics Review – Electrons

- Stable charge-carrying fundamental lepton
- Rest mass: $9\text{x}10^{-31}$ kg ($1836m_e = m_p$), charge -e
- Not typically found unbound (β^- decay)
- Double-slit experiment confirmed for e^- by Clauss Jönsson in 1961
- Spin ½, thus fermion (Pauli exclusion applies)
- Spontaneous emission – electron drops energy levels
- From electrons' spin+charge emerge molecules, and the periodic table, and chemistry...

Physics Review – Electron Orbitals







Information Theory Review

- Norton issues space of messages X over channel C
- Natasha receives space of messages Y
- *p*(y|x) is fixed for channel; want to maximize “mutual info” as *signaled* in pulsed {light, V, I...} and *measured* in bits
- Amplitude response function *A(f)*: ratio of output to input tone of a frequency *f*
- Bandwidth W of a channel: frequencies passed through
- W can handle up to 2W pulses / sec (Nyquist's Theorem)

Information Theory Review

- 2^1 states are the minimum we can differentiate
- Multilevel transmission sends from among 2^m
- Noise begins to drown out signal divisions

  Medium SNR (dB): signal / noise amplitudes
- Shannon Channel Capacity maximum:

  $C = W \log_2(1 + SNR)$ bps
- C for telco at ideal 40dB SNR: 45.2kbps
  - 33.6kbps modems until V.90

Information Theory Review

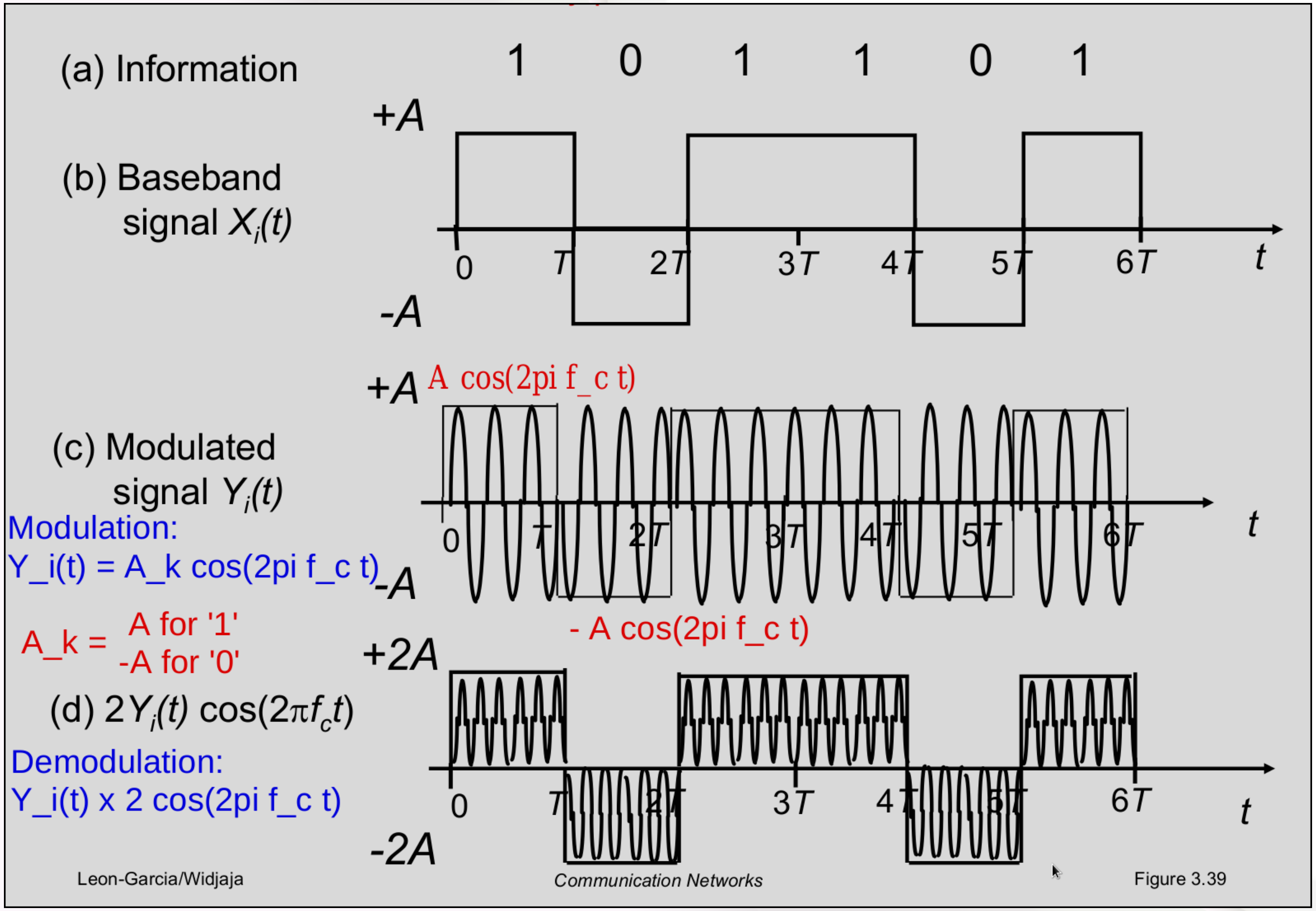
- Sinusoidal signal $x(t) = cos(2\pi ft)$ at f Hz
- Channel output $y(t)$:

  $A(f)\ cos(2\pi ft + \varphi(f)) = A(f)\ cos(2\pi f(t - \tau(f)))$
- NRZ coding on A volts: 0 for 0, A for 1
- Polar NRZ: -A/2 for 0, A/2 for 1
- Bipolar: for kth 1 value, $(-1)^k/2$ for 1

Shootout at the Line Coding Corral

- Polar NRZ average power: $A^2/4 < A^2/2$ (NRZ)
- Bipolar average frequency: Gaussian 1/2T
  - Vs pNRZ exponential falloff from low frequencies
  - Use differential bipolar to avoid systematic flip
- Manchester uses two pulses per bit to self-clock
- ASK/PSK/FSK/QAM
- $X_i(t)$ baseband is modulated by *(±)Acos(2πft)*
- Demodulated by, say, *2cos(2πft)*

And there we go.


(a) Information
1
0
1
1
0
1
(b) Baseband signal $X_i(t)$
+A
-A
0
T
2T
3T
4T
5T
6T
t
(c) Modulated signal $Y_i(t)$
+A
-A
0
T
2T
3T
4T
5T
6T
t
(d) $2Y_i(t)\cos(2\pi f_c t)$
+2A
-2A
0
T
2T
3T
4T
5T
6T
t

A cos(2pi f_c t)

- A cos(2pi f_c t)

Modulation:
Y_i(t) = A_k cos(2pi f_c t)

A_k = A for '1'
-A for '0'

Demodulation:
Y_i(t) x 2 cos(2pi f_c t)

Leon-Garcia/Widjaja

Communication Networks

Figure 3.39

Part 2: Insertion

(A Game of Chess)

Perimeters are played out

- Workstation and laptop firewalling is the norm
- Exposed services can rarely be escalated beyond theft of emails / credit cards
- VPNs using RSA SecureID / SafeNet eToken
  - RSA is currently replacing all SecureID tokens...
- I don't know anything about web apps, sorry.

Browser security still a joke

- This morning:

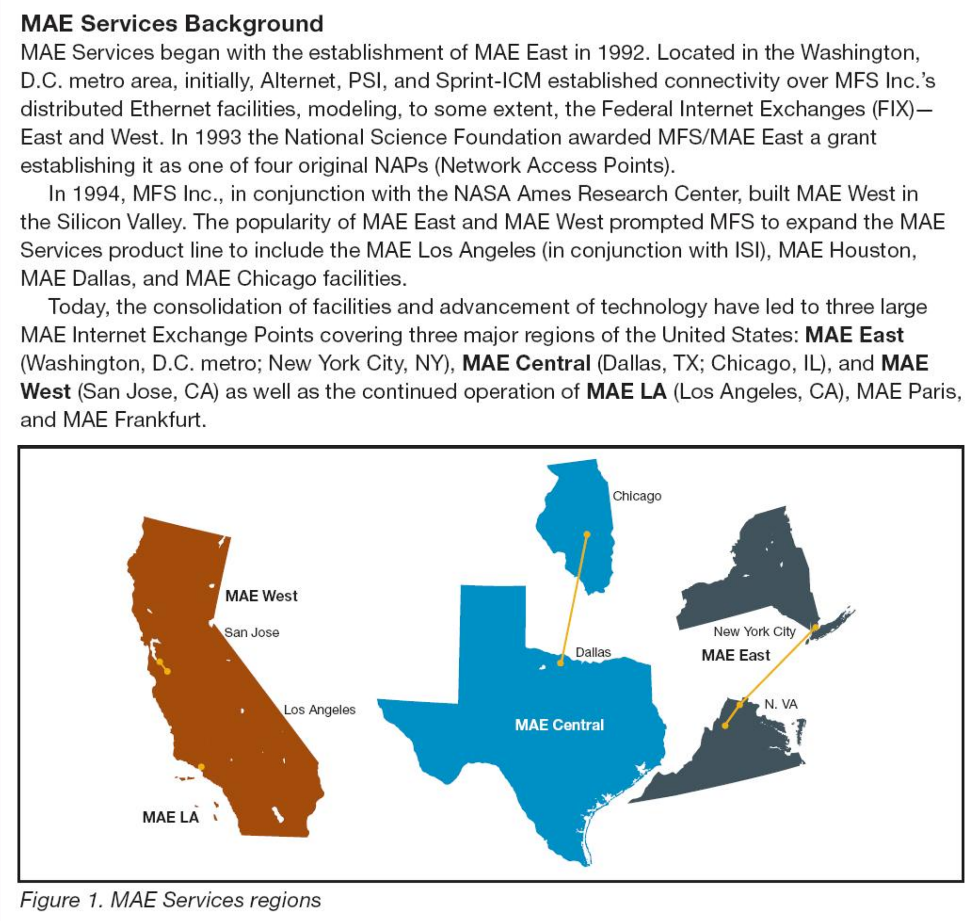
```
  “iceweasel (10.0.6esr-1) unstable; urgency=high

  * New upstream release.
  * Fixes for mfsa2012-{42-49,51-56}, also known as
    CVE-2012-1948, CVE-2012-1950, CVE-2012-1951, CVE-2012-1954,
    CVE-2012-1953, CVE-2012-1952, CVE-2012-1966, CVE-2012-1955,
    CVE-2012-1957, CVE-2012-1958, CVE-2012-1959, CVE-2012-1961,
    CVE-2012-1962, CVE-2012-1963, CVE-2012-1964, CVE-2012-1965,
    CVE-2012-1967.

 -- Mike Hommey <glandium@debian.org>  Tue, 17 Jul 2012 10:55:36 +0200
```

- If you can get them to come to a web page, you own the machine.

Whip 'em and drive 'em

- How to drive someone to a webpage? Can we widen the browser attack vector?
- Web client at layer 4 requires services from underlying layers
- Each can be attacked, **assuming suitable network position** on attacker's part

Lucky souls enjoy great vantage



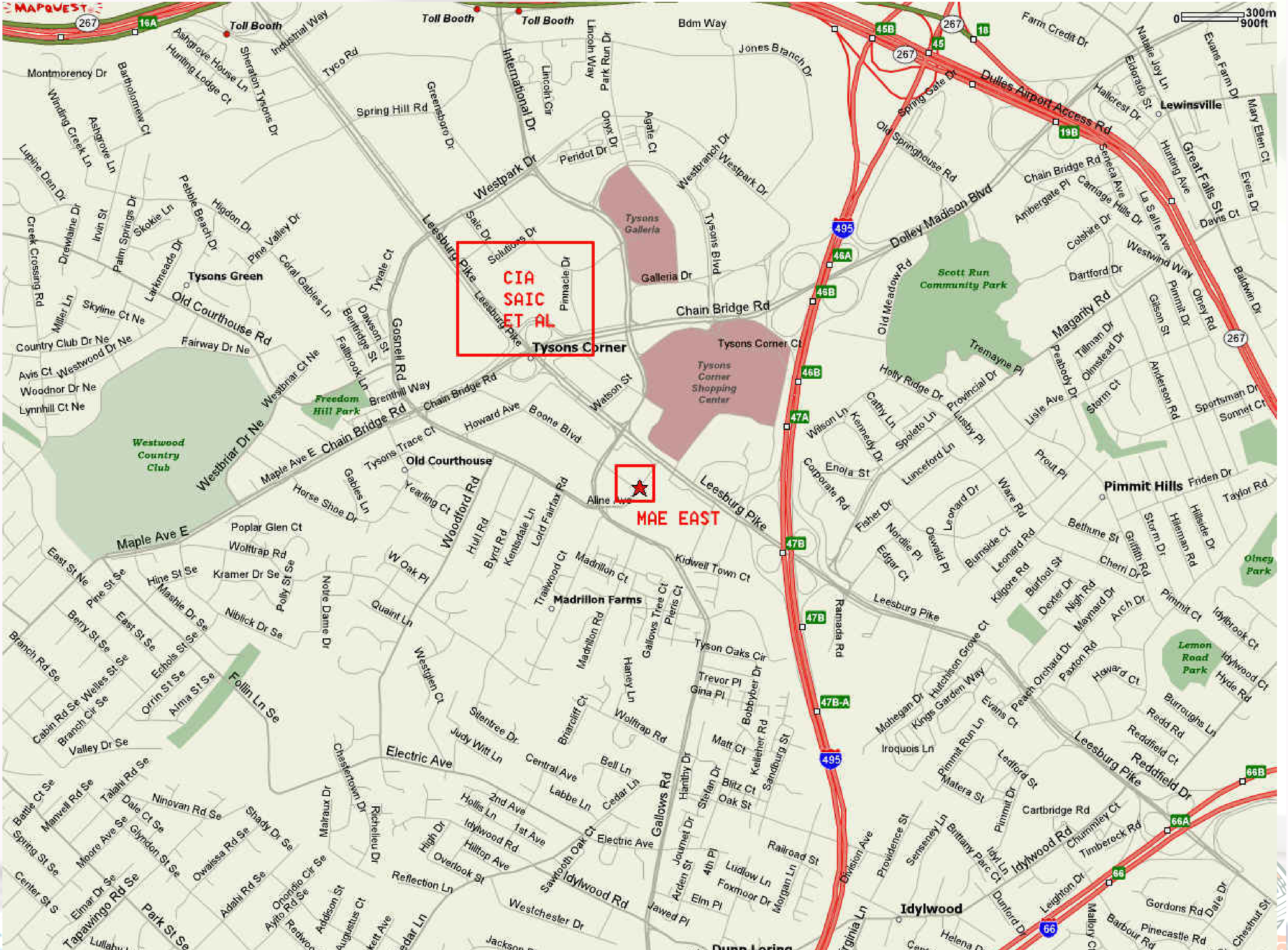
MAE Services Background

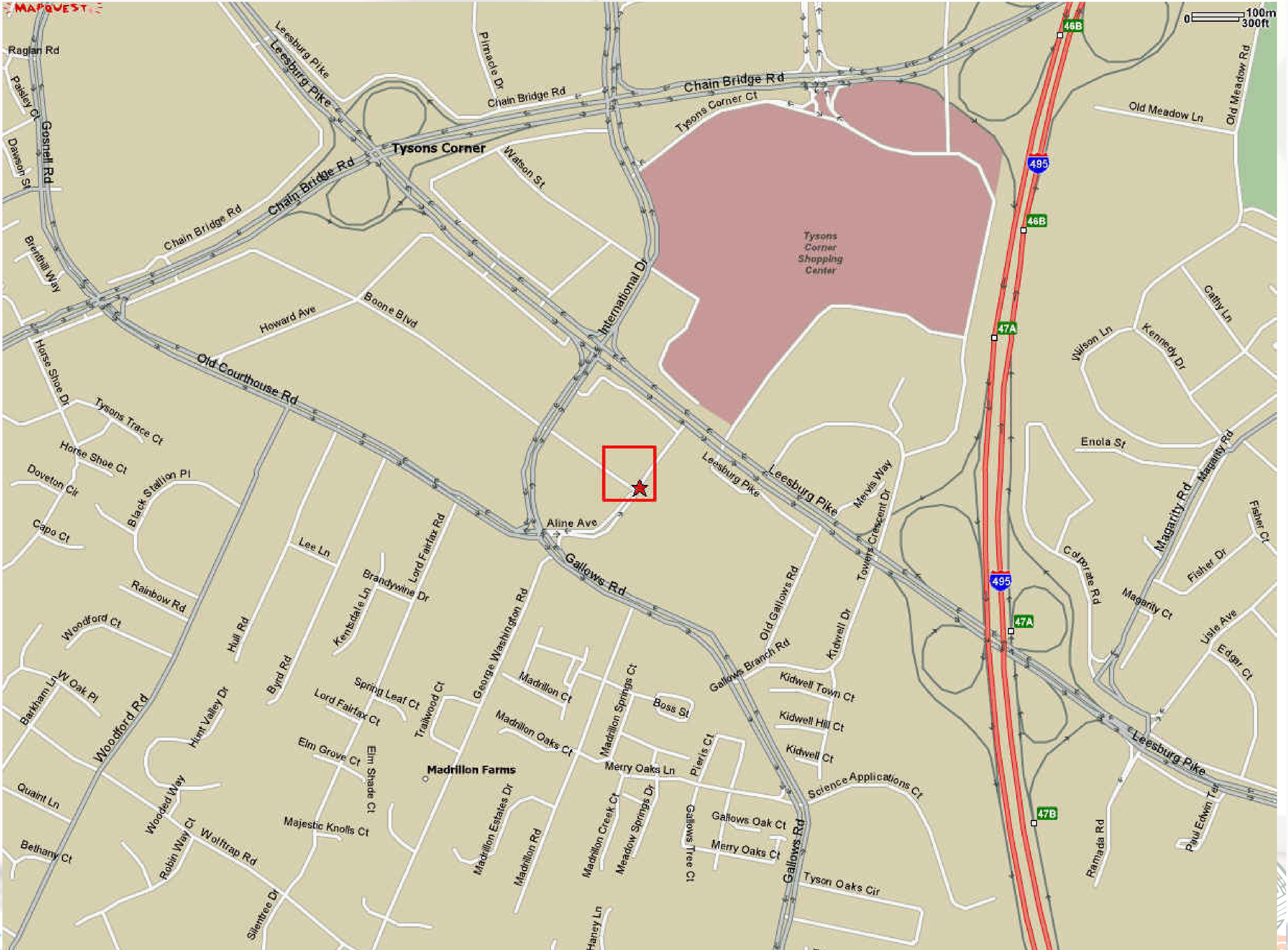
MAE Services began with the establishment of MAE East in 1992. Located in the Washington, D.C. metro area, initially, Alternet, PSI, and Sprint-ICM established connectivity over MFS Inc.'s distributed Ethernet facilities, modeling, to some extent, the Federal Internet Exchanges (FIX)—East and West. In 1993 the National Science Foundation awarded MFS/MAE East a grant establishing it as one of four original NAPs (Network Access Points).

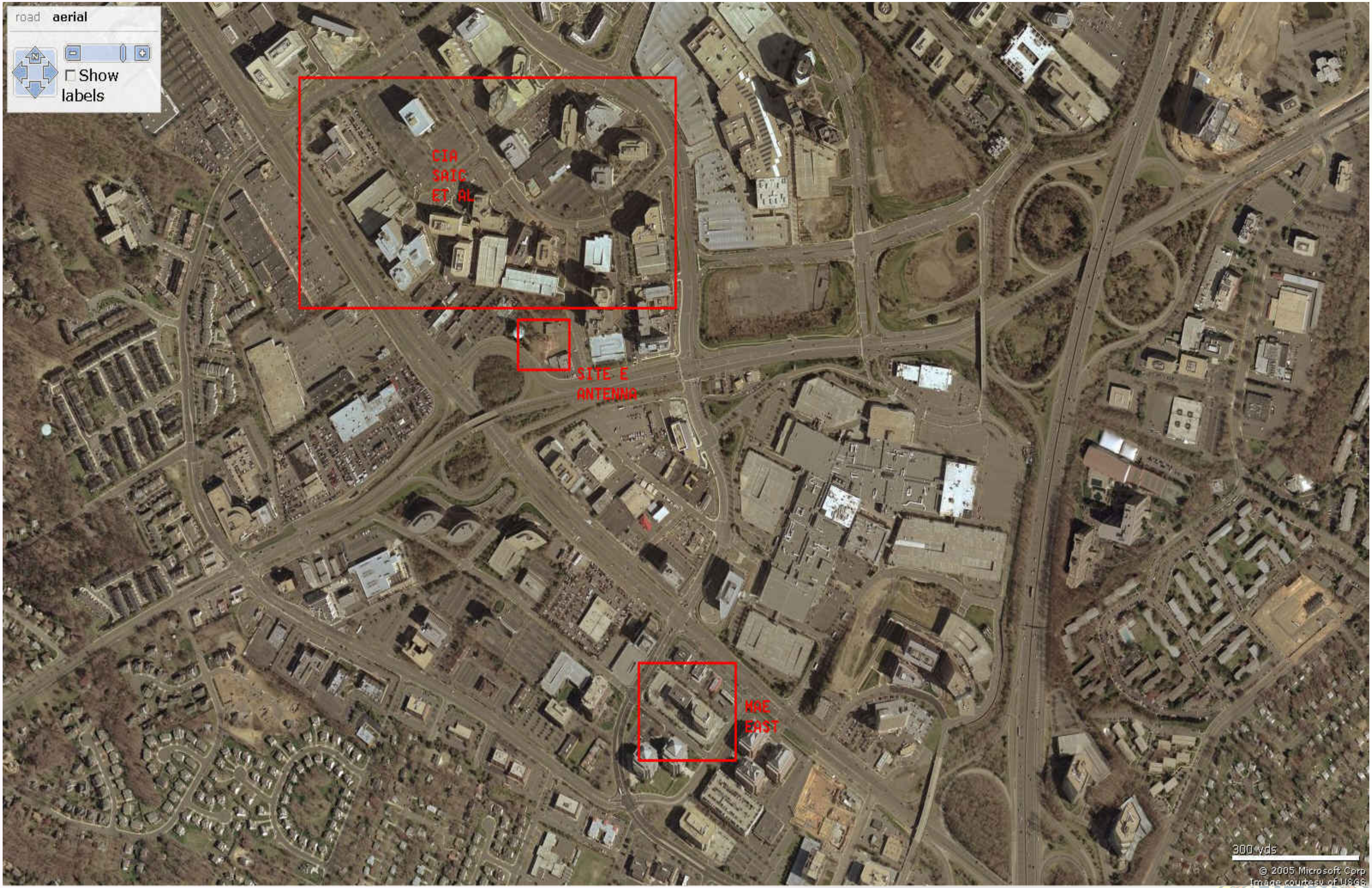
In 1994, MFS Inc., in conjunction with the NASA Ames Research Center, built MAE West in the Silicon Valley. The popularity of MAE East and MAE West prompted MFS to expand the MAE Services product line to include the MAE Los Angeles (in conjunction with ISI), MAE Houston, MAE Dallas, and MAE Chicago facilities.

Today, the consolidation of facilities and advancement of technology have led to three large MAE Internet Exchange Points covering three major regions of the United States: **MAE East** (Washington, D.C. metro; New York City, NY), **MAE Central** (Dallas, TX; Chicago, IL), and **MAE West** (San Jose, CA) as well as the continued operation of **MAE LA** (Los Angeles, CA), MAE Paris, and MAE Frankfurt.

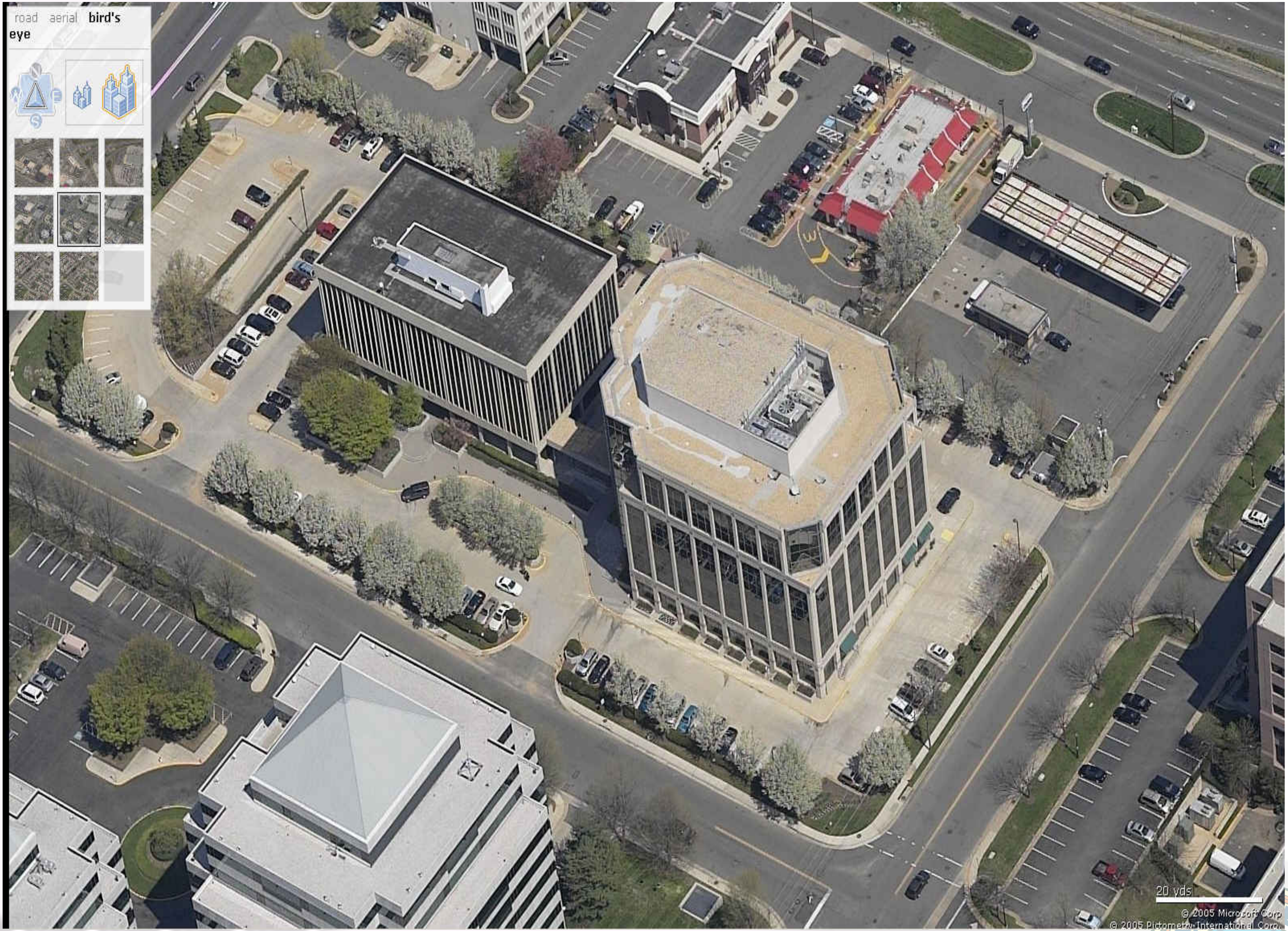
Figure 1. MAE Services regions

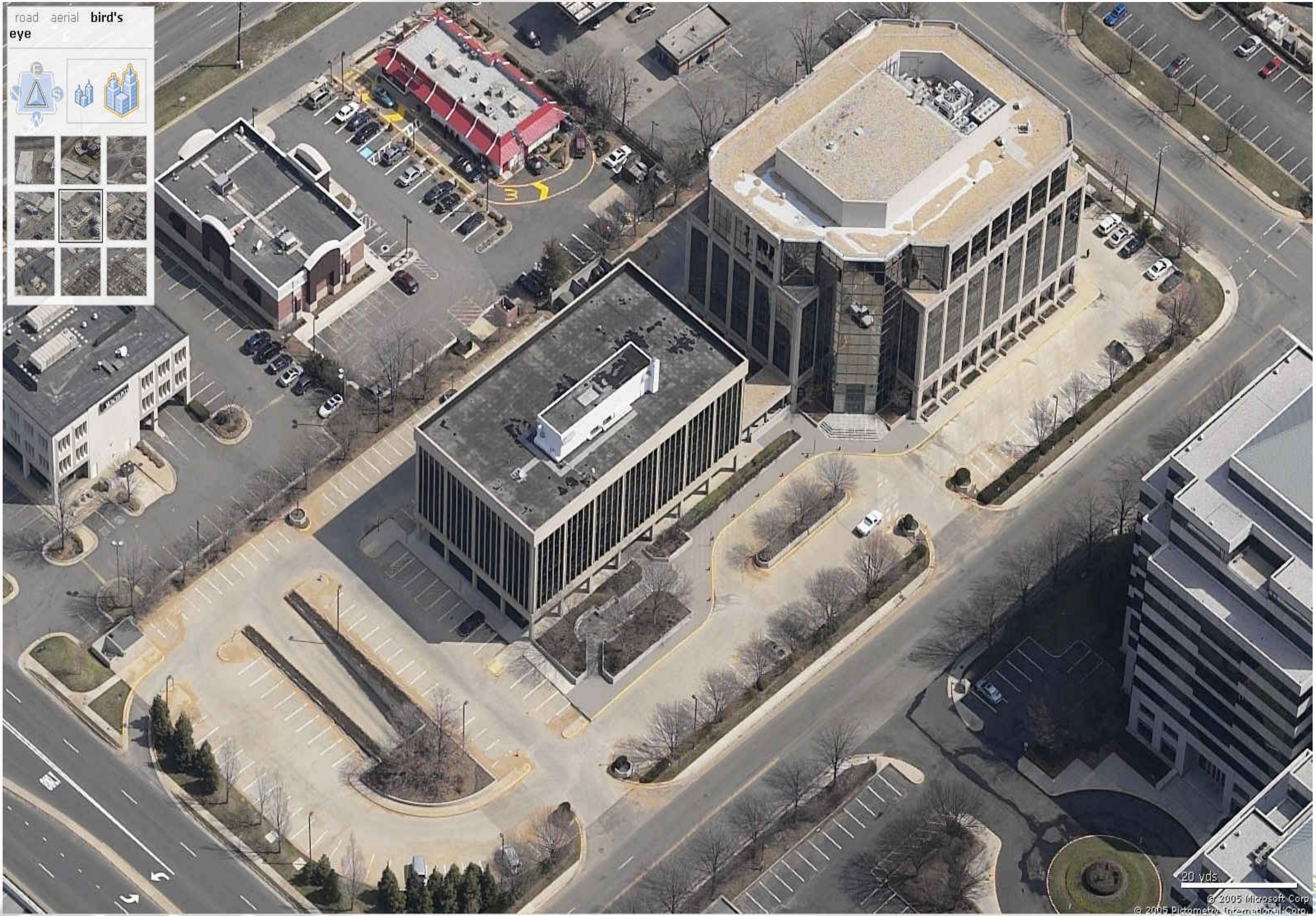

CIA
SAIC
ET AL
MAE EAST
MAPQUEST
0
300m
900ft
Tysons Corner
Tysons Galleria
Tysons Corner Shopping Center
Tysons Green
Old Courthouse
Madrillon Farms
Lewinsville
Pimmit Hills
Idylwood
Dunn Loring
Westwood Country Club
Freedom Hill Park
Scott Run Community Park
Lemon Road Park
Olney Park
Toll Booth
Toll Booth
Toll Booth
Dulles Airport Access Rd
Leesburg Pike
Chain Bridge Rd
Dolley Madison Blvd
Old Courthouse Rd
Maple Ave E
Westpark Dr
International Dr
Gosnell Rd
Woodford Rd
Gallows Rd
Electric Ave
Idylwood Rd
Magarity Rd
Great Falls St
Galleria Dr
Tysons Blvd
Solutions Dr
Saic Dr
Pinnacle Dr
Westbranch Dr
Jones Branch Dr
Spring Hill Rd
Tyco Rd
Industrial Way
Greensboro Dr
Westbriar Dr Ne
Boone Blvd
Howard Ave
Watson St
Aline Ave
Kidwell Town Ct
Tyson Oaks Cir
Wolftrap Rd
Madrillon Rd
Old Meadow Rd
Route 267
495
66
16A
45B
45
18
19B
46A
46B
47A
47B
47B-A
66A
66B
86

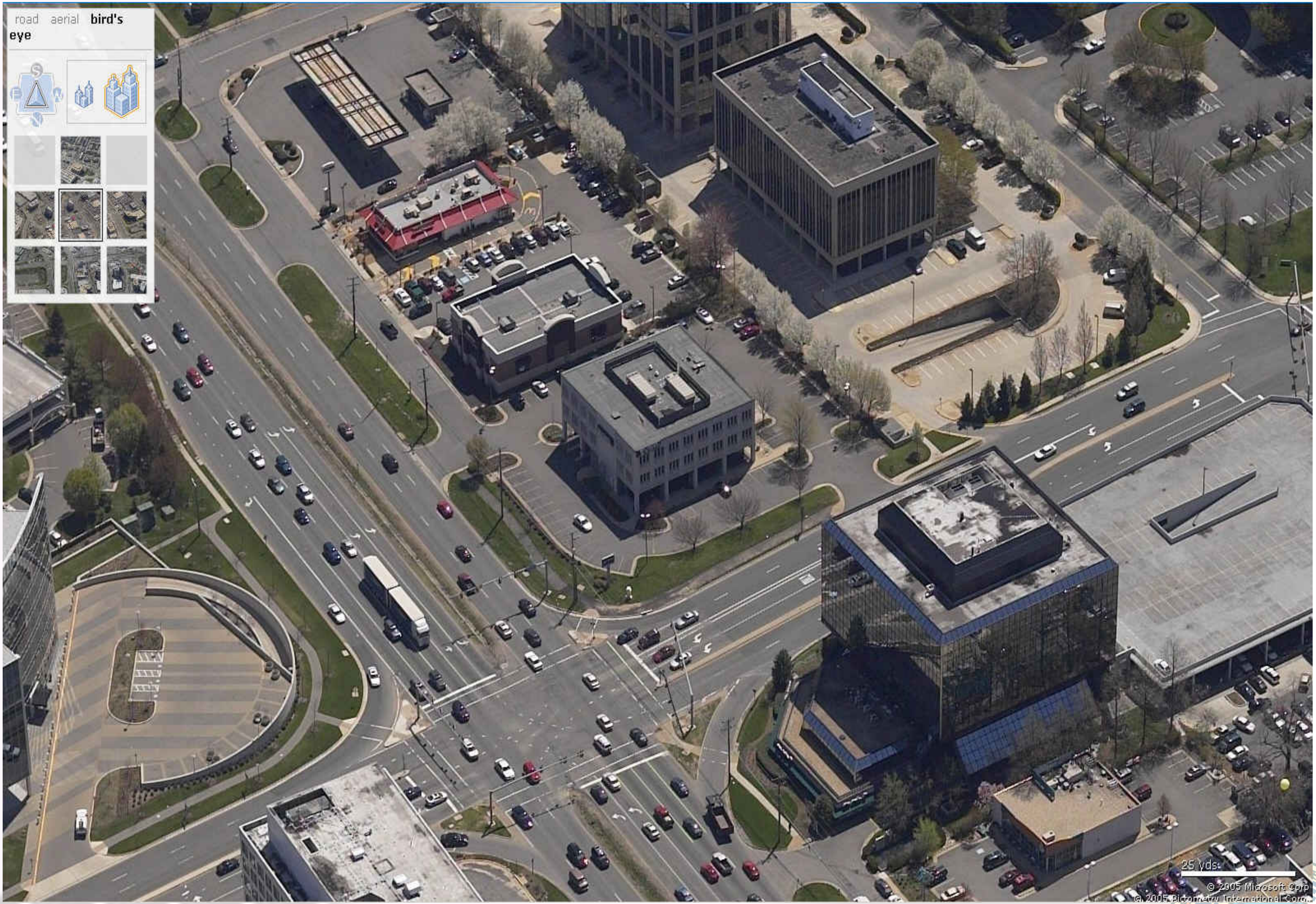

MAPQUEST
0
100m
300ft
Raglan Rd
Paisley Ct
Gosnell Rd
Dawson St
Leesburg Pike
Leesburg Pike
Pinnacle Dr
Chain Bridge Rd
Chain Bridge Rd
Tysons Corner Ct
46B
Old Meadow Ln
Old Meadow Rd
Tysons Corner
Watson St
Chain Bridge Rd
Chain Bridge Rd
495
46B
Brentthill Way
Tysons Corner Shopping Center
International Dr
Boone Blvd
Howard Ave
47A
Cathy Ln
Wilson Ln
Kennedy Dr
Horse Shoe Dr
Old Courthouse Rd
Tysons Trace Ct
Enola St
Magarity Rd
Horse Shoe Ct
Black Stallion Pl
Leesburg Pike
Leesburg Pike
Mervis Way
Doveton Cir
Magarity Rd
Fisher Ct
Aline Ave
Towers Crescent Dr
Capo Ct
Lee Ln
Lord Fairfax Rd
Gallows Rd
Corporate Rd
Fisher Dr
Rainbow Rd
Brandywine Dr
George Washington Rd
Old Gallows Rd
495
Magarity Ct
Kensdale Ln
Lisle Ave
Woodford Ct
Hull Rd
47A
Kidwell Dr
Edgar Ct
Gallows Branch Rd
W Oak Pl
Barkham Ln
Byrd Rd
Madrillon Ct
Kidwell Town Ct
Spring Leaf Ct
Trailwood Ct
Madrillon Springs Ct
Boss St
Woodford Rd
Hunt Valley Dr
Lord Fairfax Ct
Kidwell Hill Ct
Madrillon Oaks Ct
Leesburg Pike
Elm Grove Ct
Kidwell Ct
Pieris Ct
Elm Shade Ct
Madrillon Farms
Merry Oaks Ln
Science Applications Ct
Quaint Ln
Wooded Way
Madrillon Estates Dr
Madrillon Rd
Majestic Knolls Ct
Madrillon Creek Ct
Meadow Springs Dr
Gallows Tree Ct
Gallows Oak Ct
47B
Paul Edwin Ter
Robin Way Ct
Wolftrap Rd
Merry Oaks Ct
Gallows Rd
Ramada Rd
Bethany Ct
Tyson Oaks Cir
Silentree Dr
Haney Ln

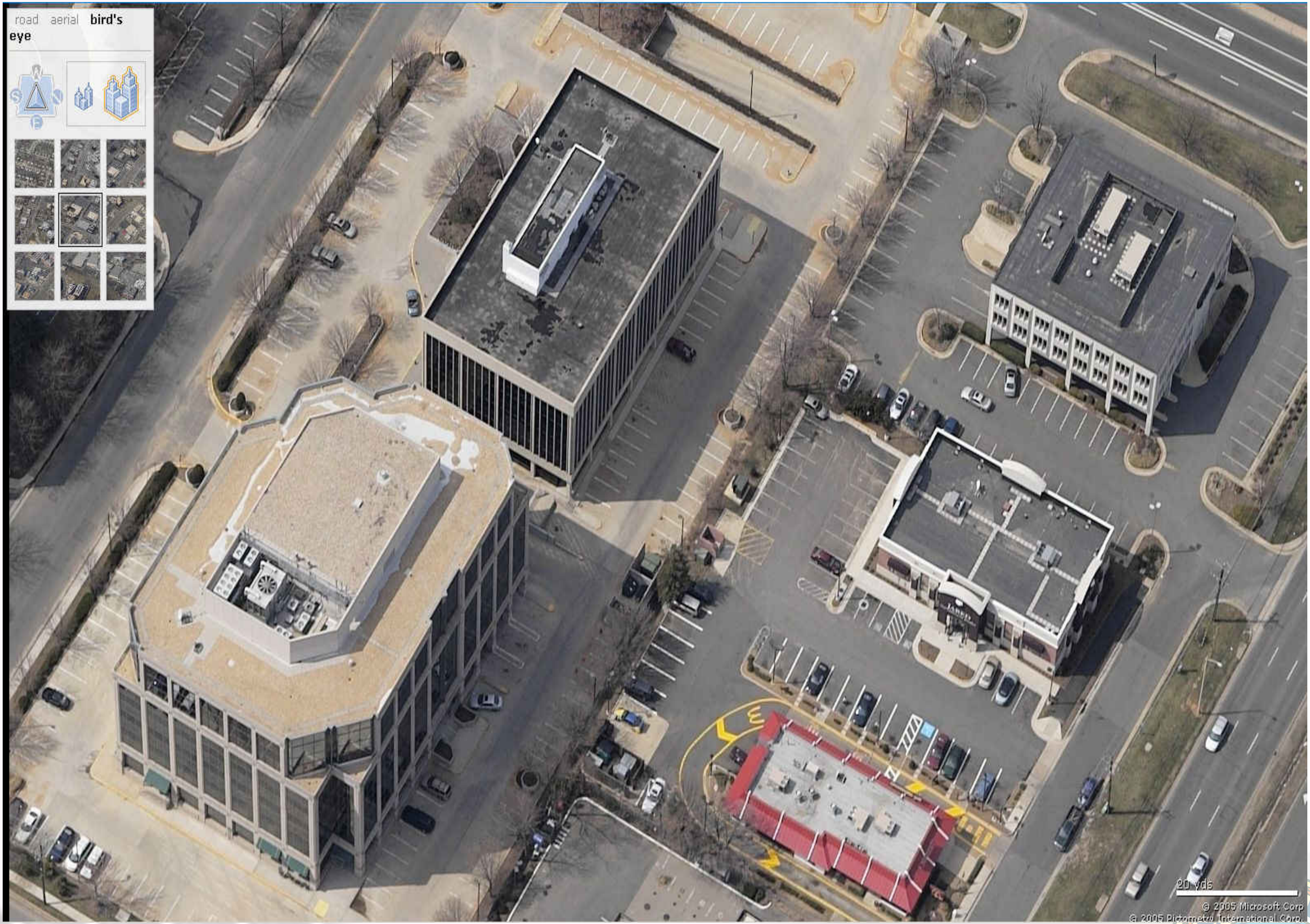


© 2005 Microsoft Corp
Image courtesy of USGS


road
aerial
bird's eye
N
W
E
S
20 yds
© 2005 Microsoft Corp
© 2005 Pictometry International Corp.


road aerial bird's eye
20 yds
© 2005 Microsoft Corp
© 2005 Pictometry International Corp.


road
aerial
bird's eye
S
E
W
N
25 yds
© 2005 Microsoft Corp
© 2005 Pictometry International Corp.

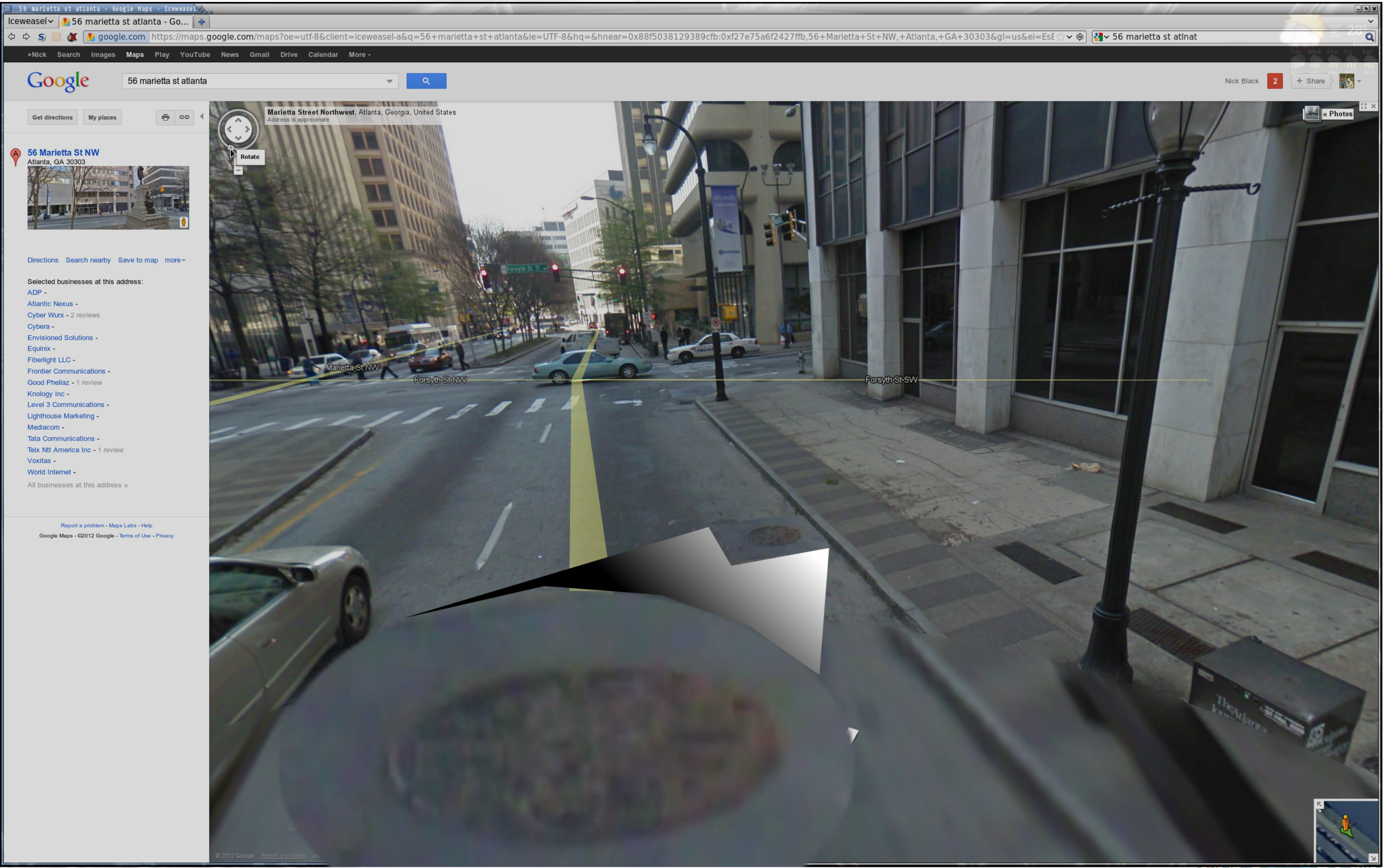


© 2005 Microsoft Corp
© 2005 Pictometry International Corp.

EXERCISE:

Where can a Molotov cocktail be
most devastatingly thrown
in the Atlanta area?

Mmmmm, smells like incapacitation of the Southeast


56 marietta st atlanta - Google Maps - Iceweasel
Iceweasel
56 marietta st atlanta - Go...
google.com https://maps.google.com/maps?oe=utf-8&client=iceweasel-a&q=56+marietta+st+atlanta&ie=UTF-8&hq=&hnear=0x88f5038129389cfb:0xf27e75a6f2427ffb,56+Marietta+St+NW,+Atlanta,+GA+30303&gl=us&ei=EsE
56 marietta st atlnat
+Nick
Search
Images
Maps
Play
YouTube
News
Gmail
Drive
Calendar
More
Google
56 marietta st atlanta
Nick Black
2
+ Share
Get directions
My places
Rotate
« Photos
Forsyth St
Marietta St NW
Forsyth St NW
Forsyth St SW
©2012 Google
Report a problem

Marietta Street Northwest, Atlanta, Georgia, United States
Address is approximate

56 Marietta St NW
Atlanta, GA 30303

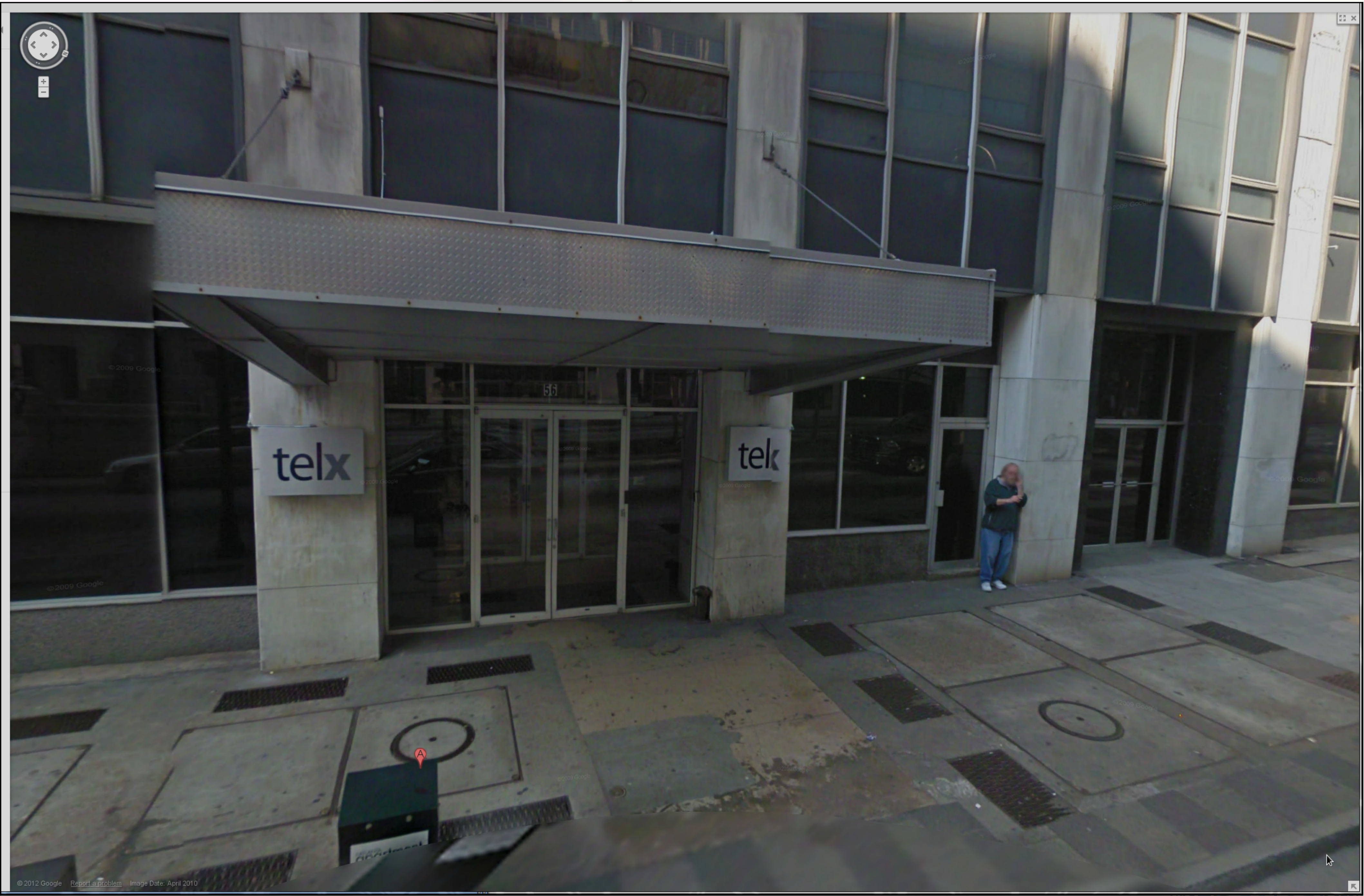
Directions Search nearby Save to map more

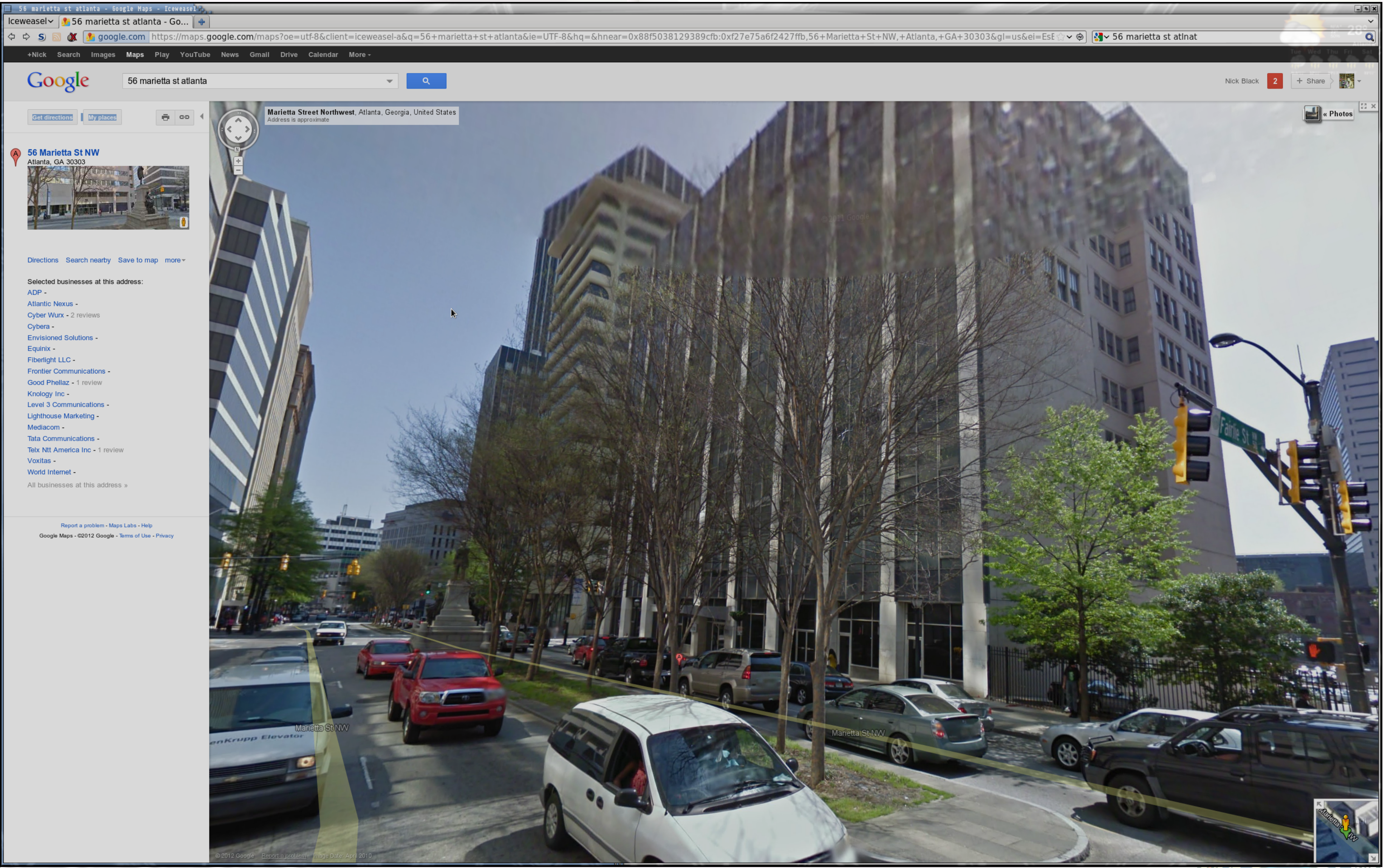
Selected businesses at this address:

- ADP -
- Atlantic Nexus -
- Cyber Wurx - 2 reviews
- Cybera -
- Envisioned Solutions -
- Equinix -
- Fiberlight LLC -
- Frontier Communications -
- Good Phellaz - 1 review
- Knology Inc -
- Level 3 Communications -
- Lighthouse Marketing -
- Mediacom -
- Tata Communications -
- Telx Ntt America Inc - 1 review
- Voxitas -
- World Internet -

All businesses at this address »

Report a problem - Maps Labs - Help
Google Maps - ©2012 Google - Terms of Use - Privacy


56
telx
telx
© 2012 Google
Report a problem
Image Date: April 2010


56 marietta st atlanta - Google Maps - Iceweasel
Iceweasel
56 marietta st atlanta - Go...
google.com
https://maps.google.com/maps?oe=utf-8&client=iceweasel-a&q=56+marietta+st+atlanta&ie=UTF-8&hq=&hnear=0x88f5038129389cfb:0xf27e75a6f2427ffb,56+Marietta+St+NW,+Atlanta,+GA+30303&gl=us&ei=EsE
56 marietta st atlnat
+Nick
Search
Images
Maps
Play
YouTube
News
Gmail
Drive
Calendar
More
Google
56 marietta st atlanta
Nick Black
2
+ Share
Get directions
My places
Marietta Street Northwest, Atlanta, Georgia, United States
Address is approximate
« Photos
Marietta St NW
Marietta St NW
Fairlie St
©2012 Google · Report a problem · Image Date: April 2010

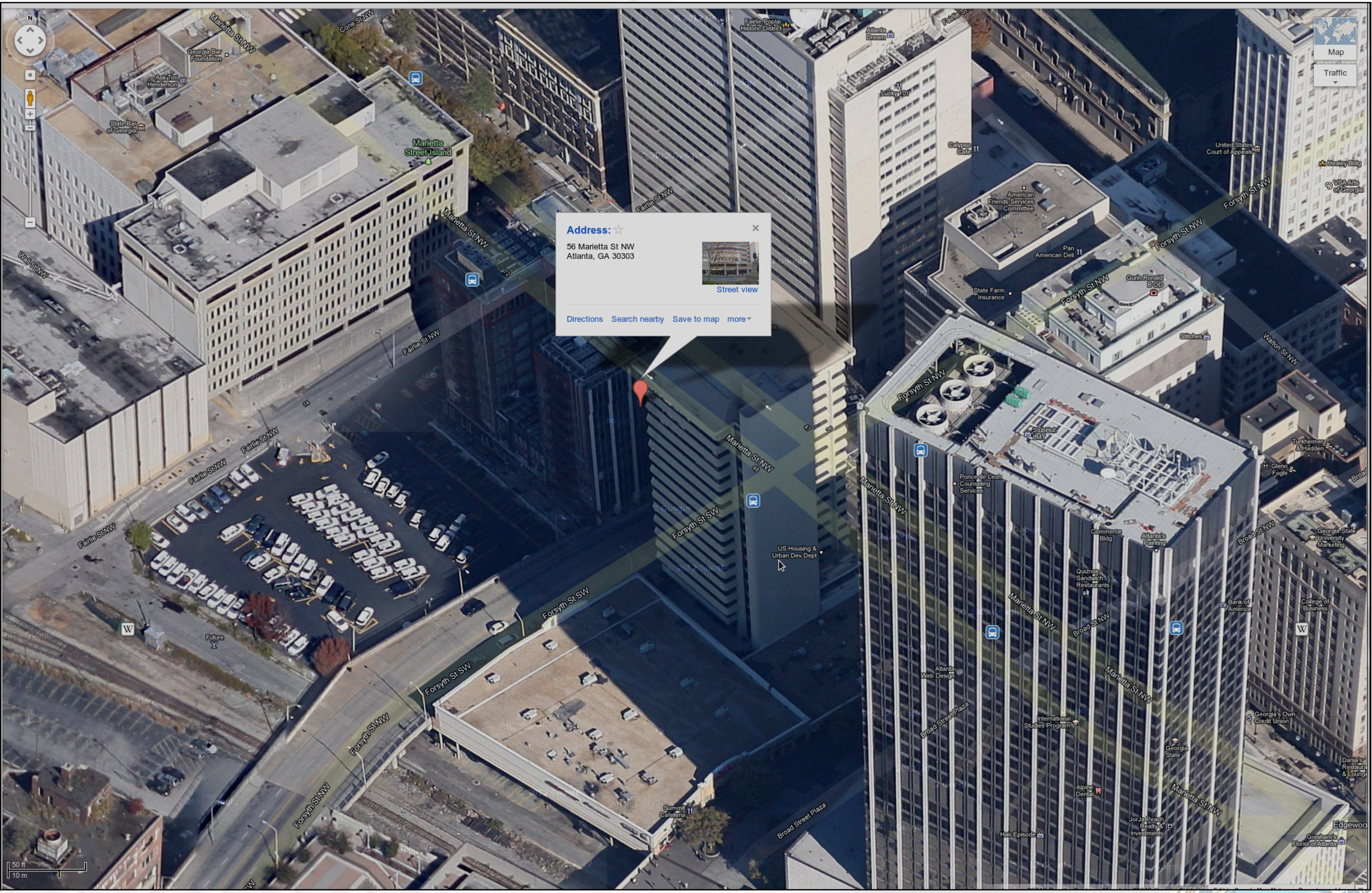
56 Marietta St NW
Atlanta, GA 30303

Directions Search nearby Save to map more

Selected businesses at this address:

ADP -
Atlantic Nexus -
Cyber Wurx - 2 reviews
Cybera -
Envisioned Solutions -
Equinix -
Fiberlight LLC -
Frontier Communications -
Good Phellaz - 1 review
Knology Inc -
Level 3 Communications -
Lighthouse Marketing -
Mediacom -
Tata Communications -
Telx Ntt America Inc - 1 review
Voxitas -
World Internet -
All businesses at this address »

Report a problem - Maps Labs - Help
Google Maps - ©2012 Google - Terms of Use - Privacy



Address: ☆

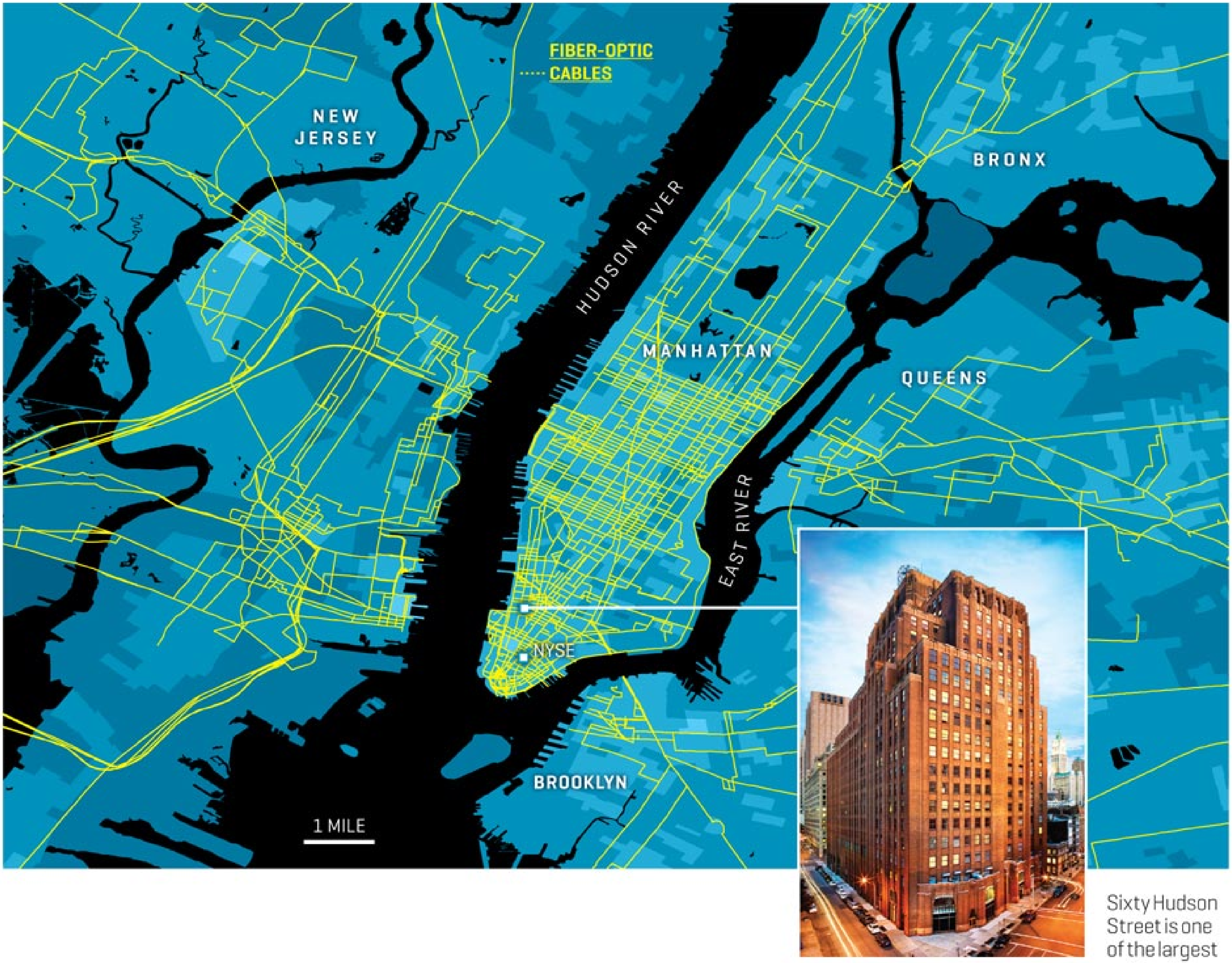
56 Marietta St NW
Atlanta, GA 30303

Street view

Directions Search nearby Save to map more

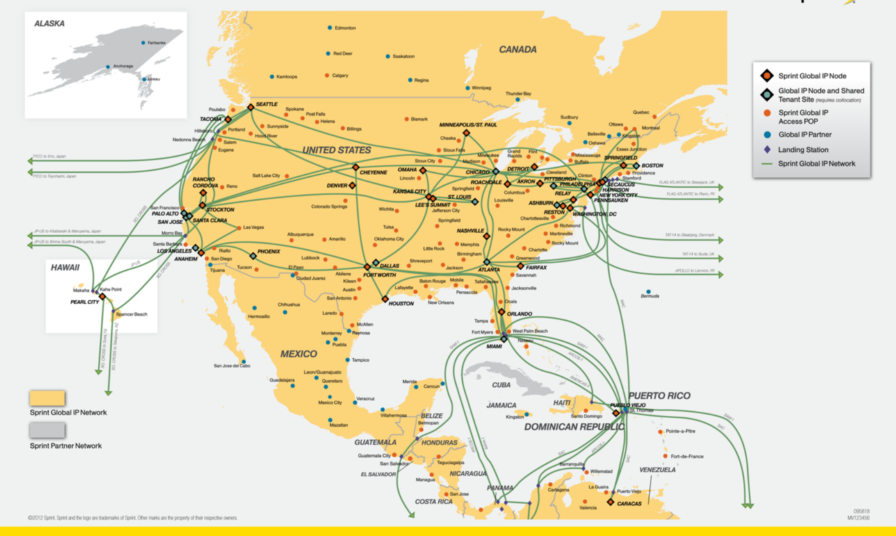
AVERAGE INTERNET SPEEDS (MAXIMUM ADVERTISED)

0 5 6 7 8 9 MEGABYTES PER SECOND

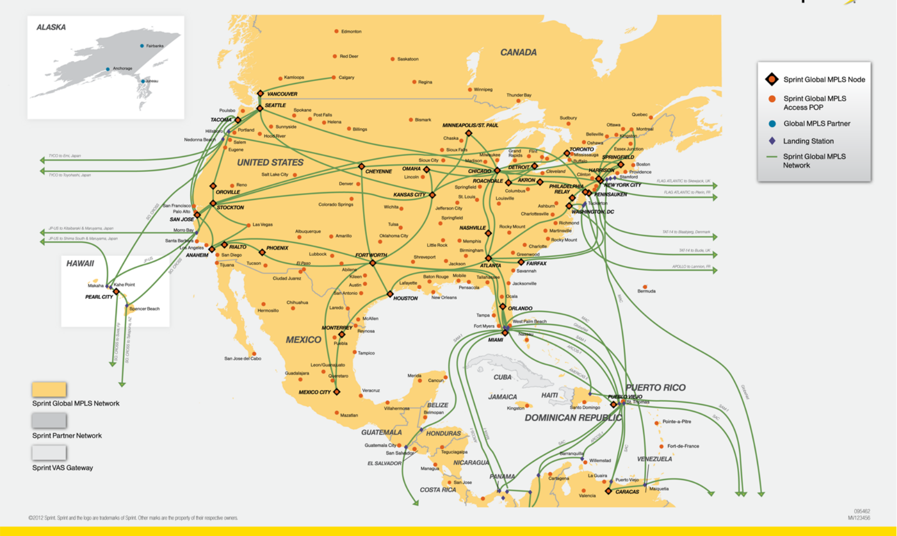


Sixty Hudson Street is one of the largest points of Internet traffic in the U.S.

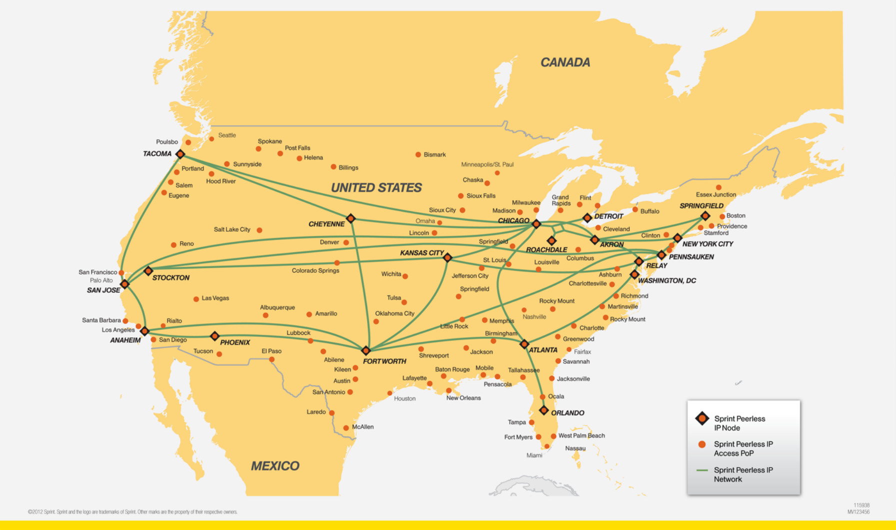
Sprint Global IP Map | North America



Sprint Global MPLS Map | North America

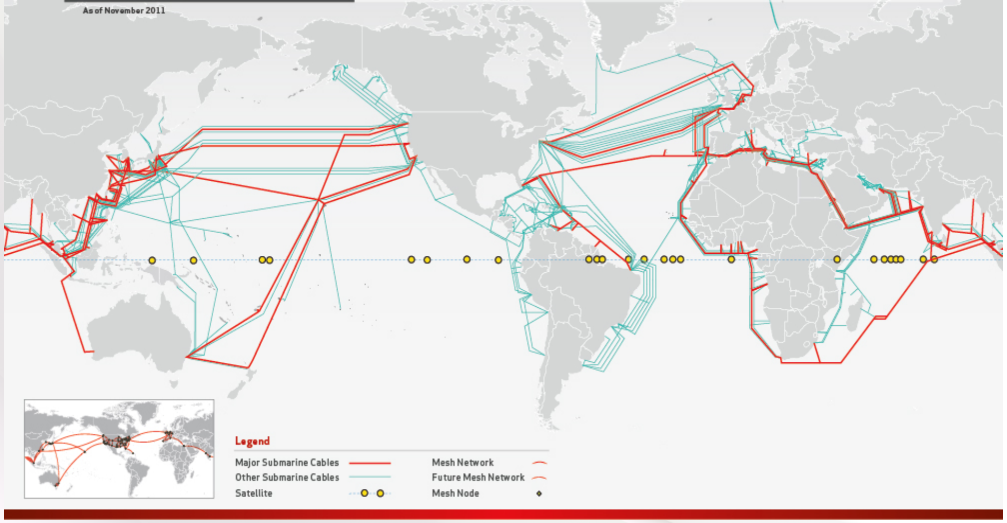


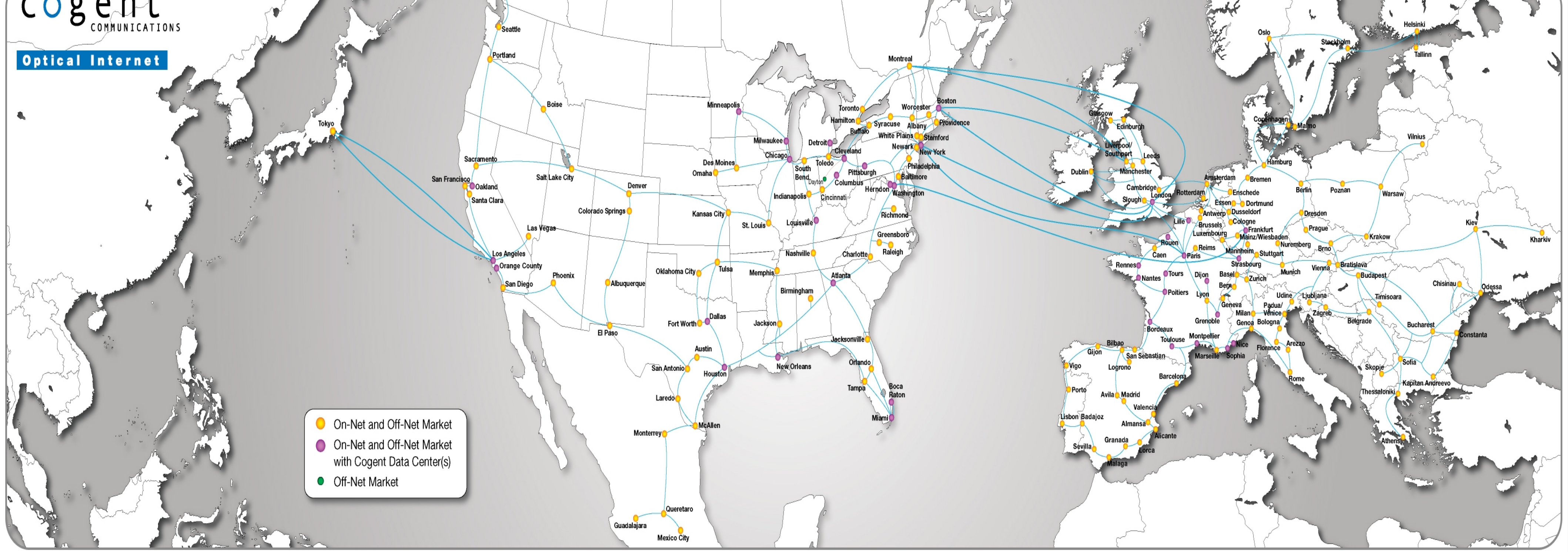
Sprint Peerless IP Network Map | North America

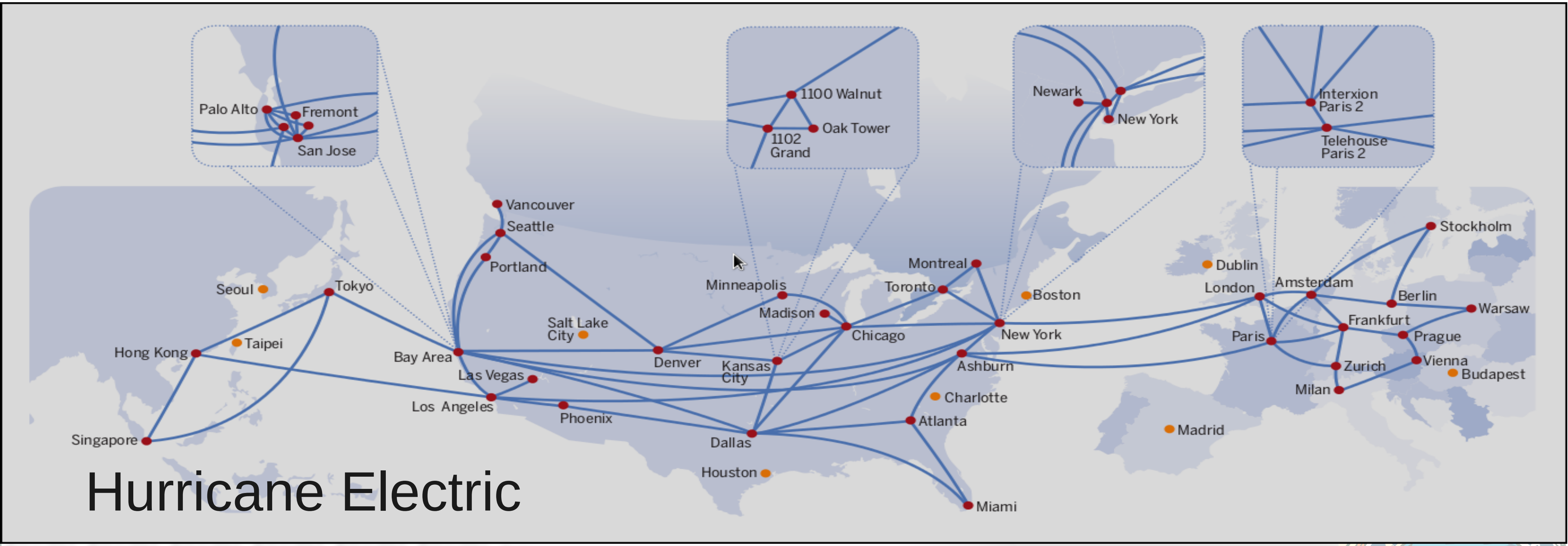


THE VERIZON GLOBAL NETWORK

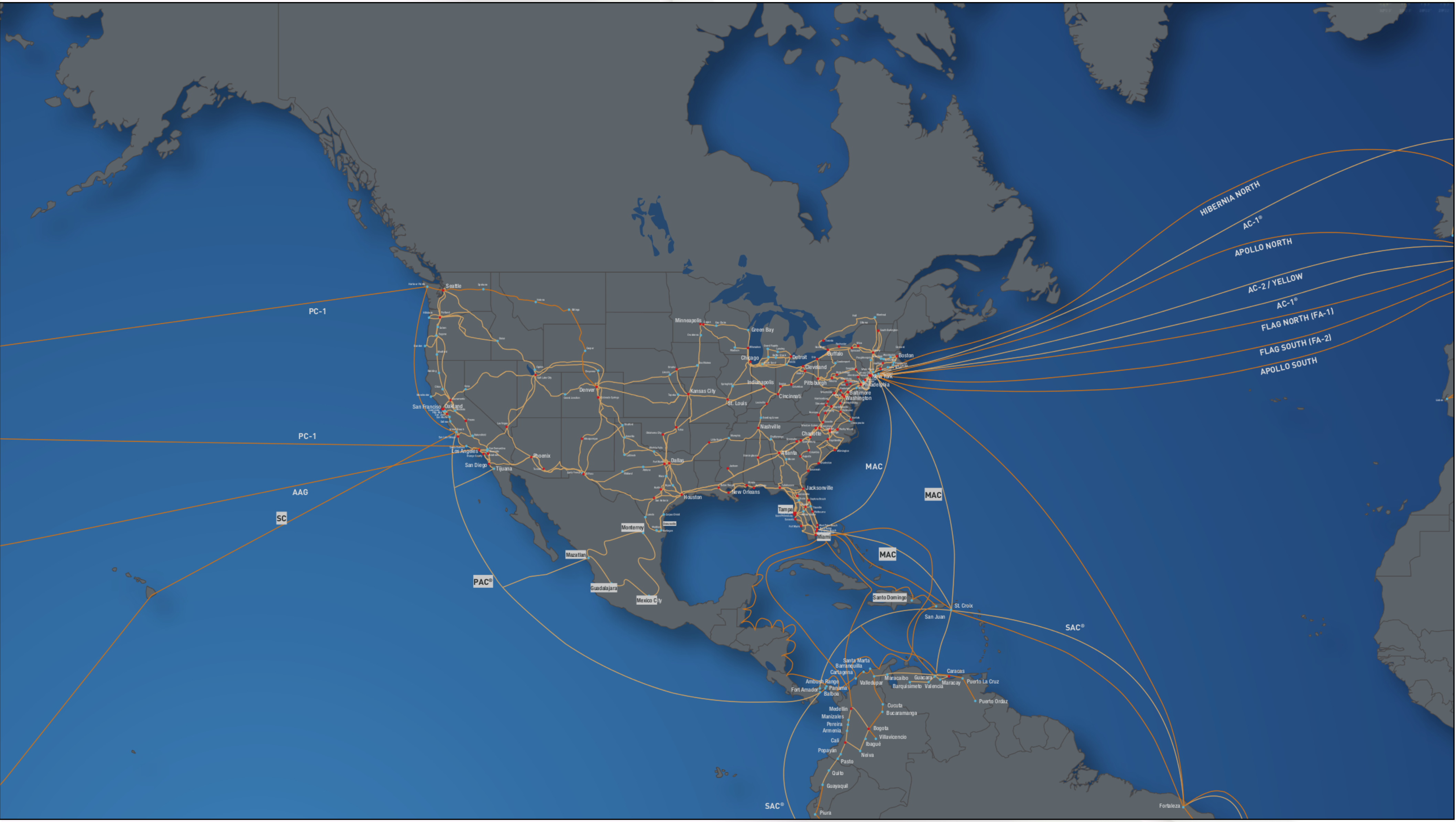
As of November 2011





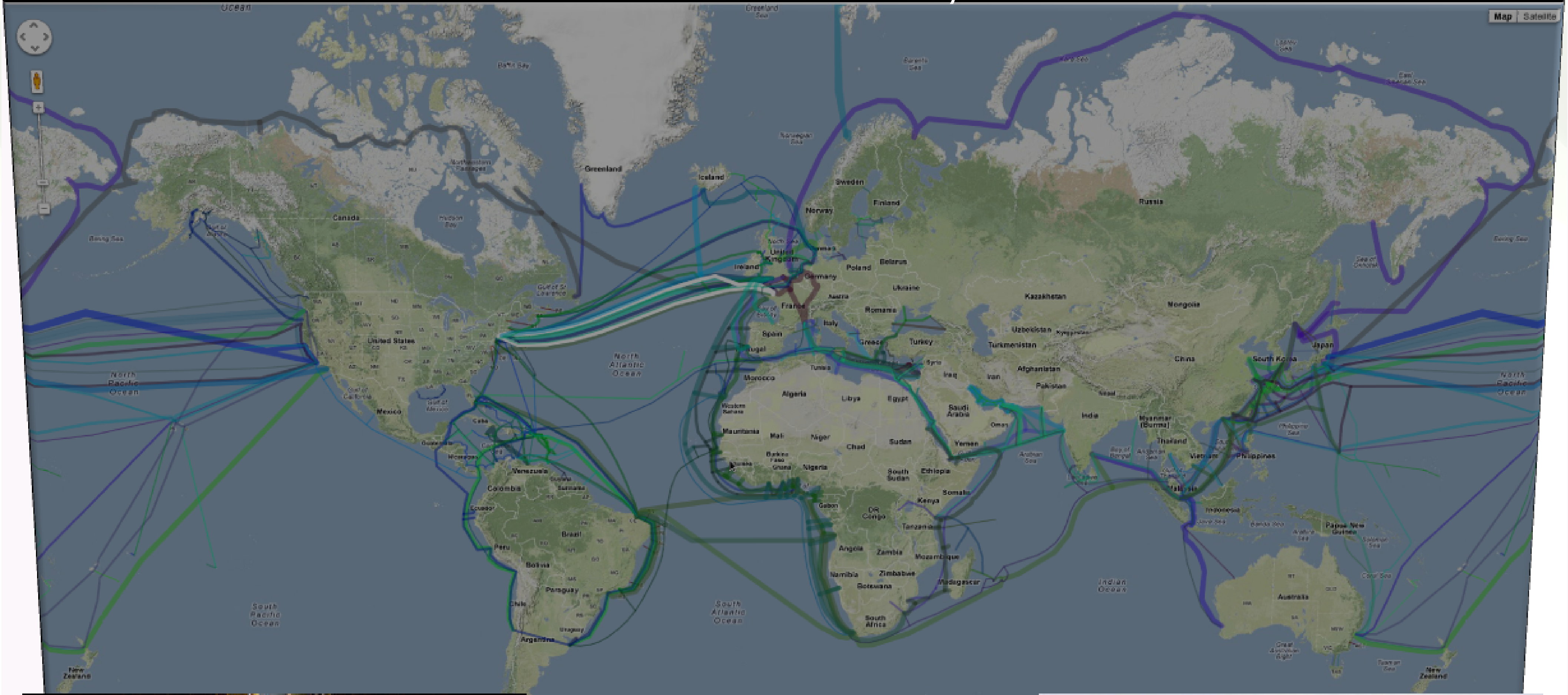


Hurricane Electric



Level 3 Communications

Global undersea transit, June 2012



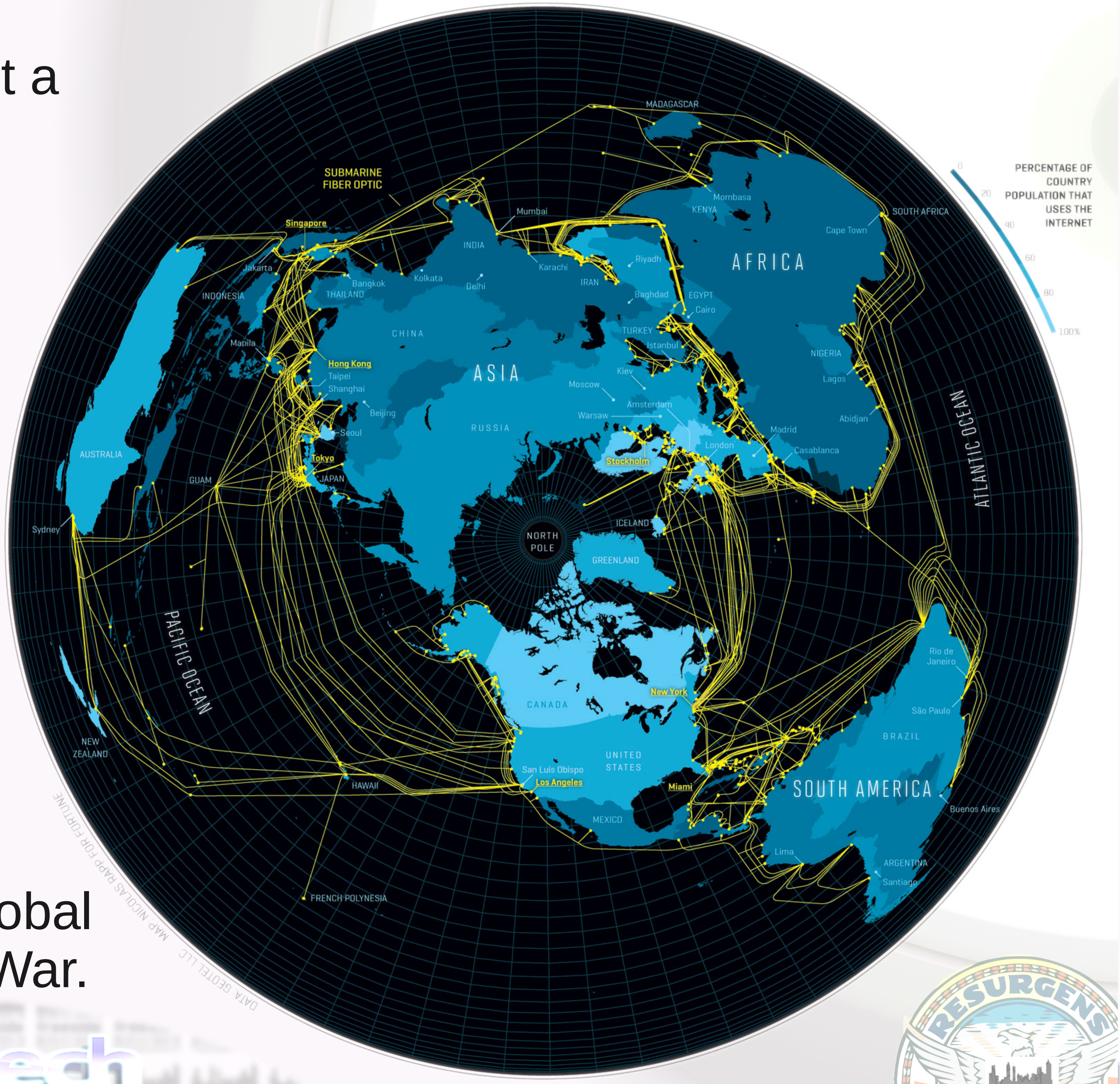
☑ Active Cables
☑ Future Cables

ACE (21 Landings, 14000km, 5.12Tbps)
(Click to see details on right)

PHOTO: JEAN CLAUDE MOSCHETTI/REA

PHOTO: AFP/GETTY IMAGES

What about a nice game of chess?



Maybe later.
Let's play Global Information War.

Le Attack Physique

- Drop a USB key. Hey, it worked for Stuxnet.
- Trojanized input drivers on USB passthroughs
- Felton frozen memory attack on blockcrypt
- Router upgrades
- Ethernet taps

Wireless with everyone they've had wireless with

- Machine logs into VPN from Starbucks using two-factor auth
- Your VPN's strength is, at that Starbucks, as strong as that machine's securty
- Getting pwned is a lifelong disease

Internal threat is tremendous

- Physical access to a box → ownership of box
  - So it always has been.
  - Pervasive code signing beginning to change this
  - Encrypted filesystems help against theft/loss
  - Bring-your-own initiatives work against policy
- Ownership of a box with network access → access to network

Part 3: Seizure

(The Fire Sermon)

Viehböck went hard in the paint

- Reaper attack on WPS will kill you if you let it
- Update firmware
- Verify WPS disabled!

- Personal experimentation: access recovered on **9** of 13 readily accessible networks.

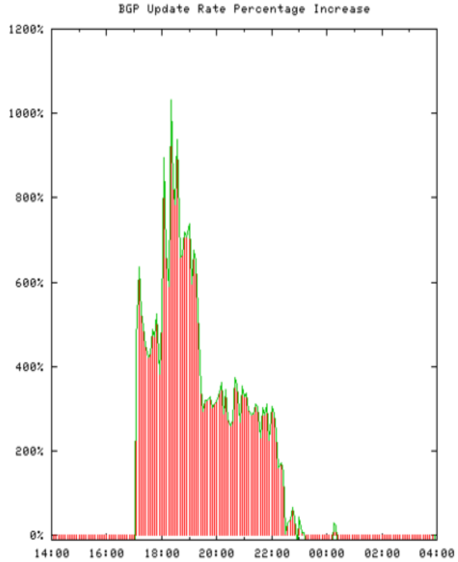
- It's a real shame that this was allowed to happen

LOL you're not using WPA2+CCMP?

(or *way* better yet, 802.1X)?

Old friends, old problems

- Fundamental issues remain fundamental:
  - DHCP jacking
  - DHCP6 jacking :)
  - ARP poisoning
  - Attacks on BGP
    - Pakistan shutting down YouTube LOL
  - Kaminsky's accelerated DNS redirections



Great moments in infrastructure fail

- Stuxnet, ahhhh Stuxnet
  - TIME's Man of the Year 2011
- Roto-rooter 2011-08-15
- “PdoS” 2008 EUSecWest
- Cisco IOS XR 2009-08-19
- 2005 Cisco / Juniper single packet DoSs
- Witty Worm 2004-03-19
- Warhol [Staniford, Paxson, Weaver 2002]
- 1988-11-02: never forget
- Teardrop / PoD / Black fax / CGA fires / Blotto box :)

IPv6

- Worse than ARP, augmented by...
- Router Solicitation, Router response
- 128 bits: everyone in their own little garden
- Analysis tools aren't ready
- Enumeration is easier
- Broadcast goes away...kinda

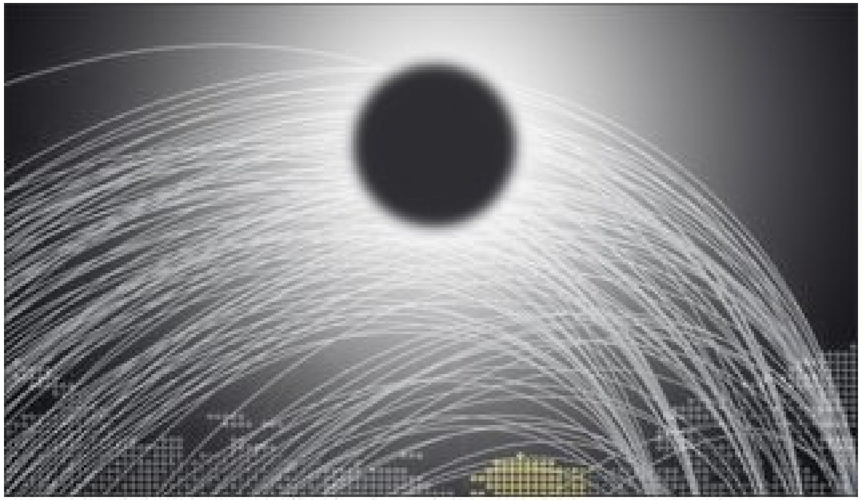
HTTPS is broken

- Check your CA trust store.
- You need about, like, 4 of those.
- Are you notified when a cert changes?
- Are you pulling largely useless CRLs?
- Are your applications properly using SSL?
- Audit! Generate certs valid save non-matching CN, etc...the results **will** surprise you.
- CertPatrol plugin is pretty acceptable.

Part 4: Denial of Service

(Death by Water)

Spray the area

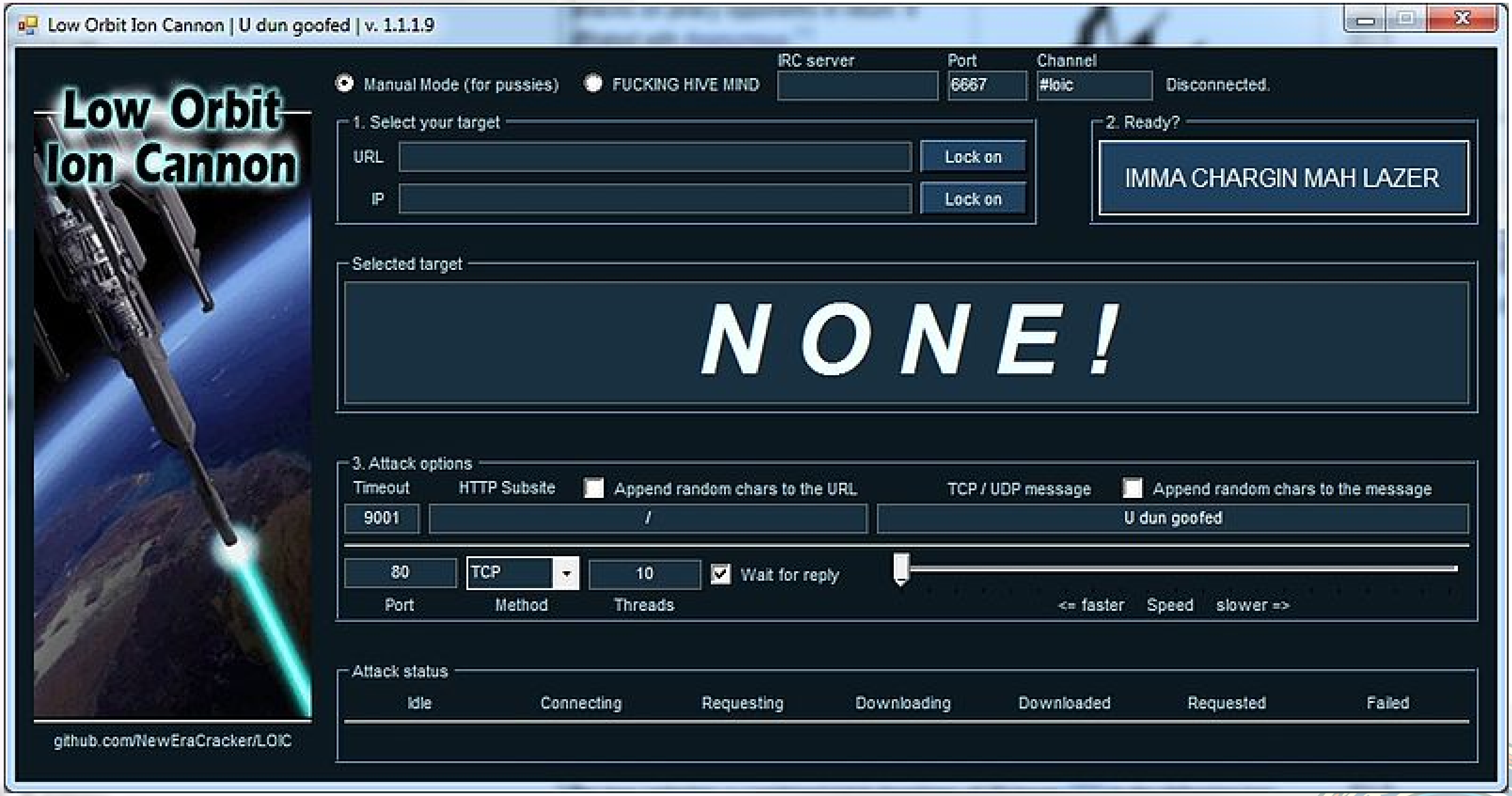


In this THREAT LEVEL simulation, Chinese DDoS packets are seen blotting out the sun, plunging the Earth into a perpetual "botnet winter."

- Metasploit beacon frame fuzzer
- Metasploit beacon SSID emulator
- Metasploit fake AP beacon flood
- Good ol' disassociation and deauthentication
- Reactive jammer
- Reservation based (RTS)
- Power-saving (TIM)
- Expand wireless congestion windows via arbitrary scrambling
  - Sense DATA, wait for SIFS, jam channel (or CTS+DIFS, or RTS+SIFS)
- Expand wireless NAV busy period via +RTS/DATA duration value
- [Gummadi et al 2007] narrow-band jamming (time recovery / PLCP processing)
- MAC flooding on wireless, wired
  - Some switches still fall back to broadcast mode

DdoS for fun and profit, mainly profit

- LOIC
- Stacheldraht
- yawn



Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.9

● Manual Mode (for pussies) ○ FUCKING HIVE MIND

IRC server:

Port: 6667

Channel: #loic

Disconnected.

1. Select your target

URL:

IP:

Selected target: NONE!

3. Attack options

Timeout: 9001

HTTP Subsite: /

□ Append random chars to the URL

TCP / UDP message: U dun goofed

□ Append random chars to the message

Port: 80

Method: TCP

Threads: 10

☑ Wait for reply

Wireless jammers? We've got that.

Any color you like, so long as it jams.

Part 5: Rome Falls – Tetelestai

(What the Thunder Said)

Georgia began their campaign for a national title in college football with a disheartening loss to the nation of Russia over the weekend, according to international observers and correspondents on the ground.

Using a powerful ground game and a dominating aerial assault, the Russians broke through the vaunted Georgia line "with the ease of a hot knife through butter," according to Major General Vassily Pretsky at a press conference in Moscow on Sunday night. “We have neutralized the their offensive front with tanks and missiles, and eliminated any threat through the air with a concentrated assault on their defenses. There was little challenge in the matter for us."

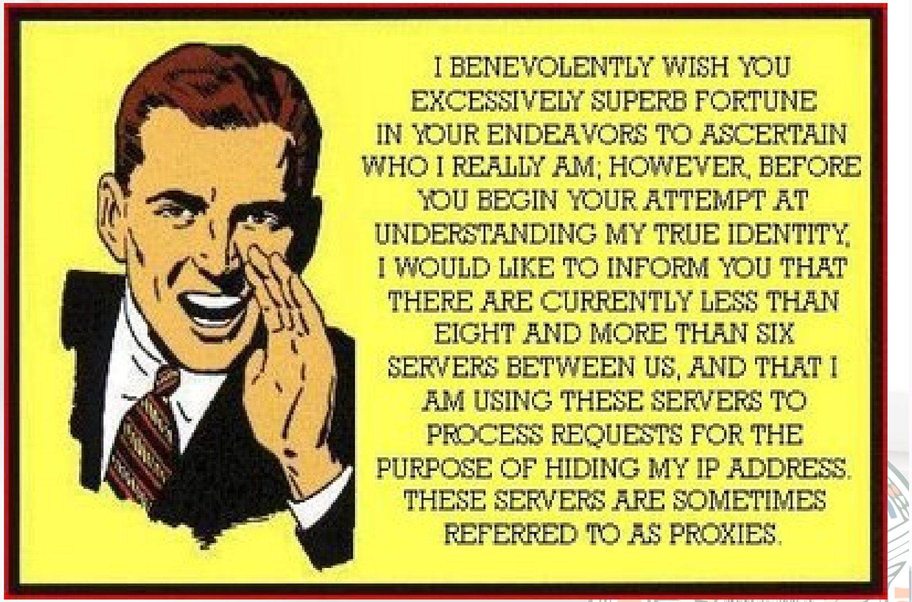
"Surrender, Bulldogs of Georgia, before we run out of the mercy we have displayed thus far."

“Georgia Begins Season with Humiliating Loss”, 2008-08-11

What's one to do?

- **Disable connection to arbitrary wireless networks!**
- Pervasive VPN to **your trusted server**
- Audit certificate verification stack
- DNSSEC within one's AS
- WPA2+CCMP, preferably 802.1X
- Ensure NX bit support is enabled, duh
- Much more intensive outbound monitoring
- Reality auditing

No panacea, as you well know


I BENEVOLENTLY WISH YOU EXCESSIVELY SUPERB FORTUNE IN YOUR ENDEAVORS TO ASCERTAIN WHO I REALLY AM; HOWEVER, BEFORE YOU BEGIN YOUR ATTEMPT AT UNDERSTANDING MY TRUE IDENTITY, I WOULD LIKE TO INFORM YOU THAT THERE ARE CURRENTLY LESS THAN EIGHT AND MORE THAN SIX SERVERS BETWEEN US, AND THAT I AM USING THESE SERVERS TO PROCESS REQUESTS FOR THE PURPOSE OF HIDING MY IP ADDRESS. THESE SERVERS ARE SOMETIMES REFERRED TO AS PROXIES.

Browsers: sucking since Navigator 3.04

- I've been saying this since 2003 or so:

  run your browser in a VM!

- The browser exploit gravy train runs thick and syrupy and inexorably and unceasingly.
- This problem is not going to be fixed soon.
- No excuses with modern virtualization support
- Even then, use NoScript and CertPatrol
- Probably best to reset image each time
  - No good unless cloud sync is disabled

What about the n00bs?

- Pervasive code signing (iOS, UEFI+Win8)
- Drastically reduce default shipped CA stores

It's dangerous out there, folks.

Snoopy says, "Constant Vigilance!"

Thanks; you've been fantastic! Vive le Atlantaside libre!