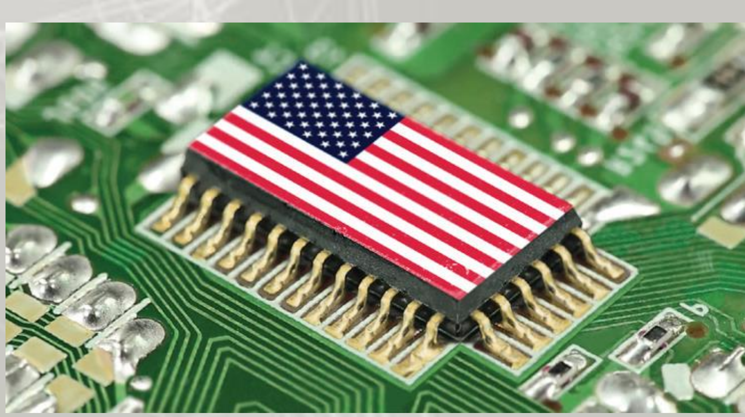
Any opinions, findings, and conclusions or recommendations expressed in this presentation are those of the author and do not necessarily reflect the views of the US Air Force, Department of Defense or the USAF Cyber College.

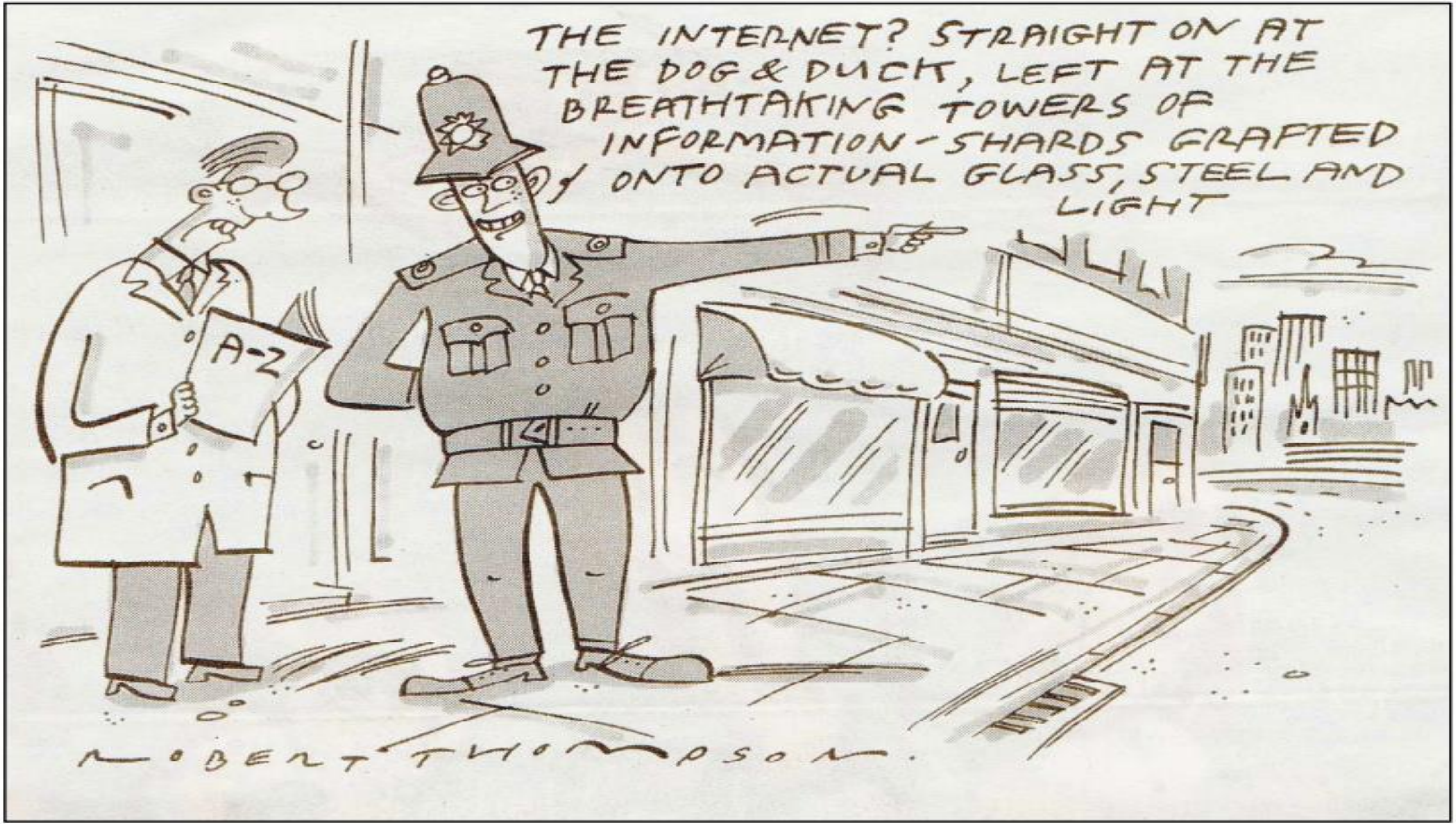
Chinese POP & Subsea Cable Overview

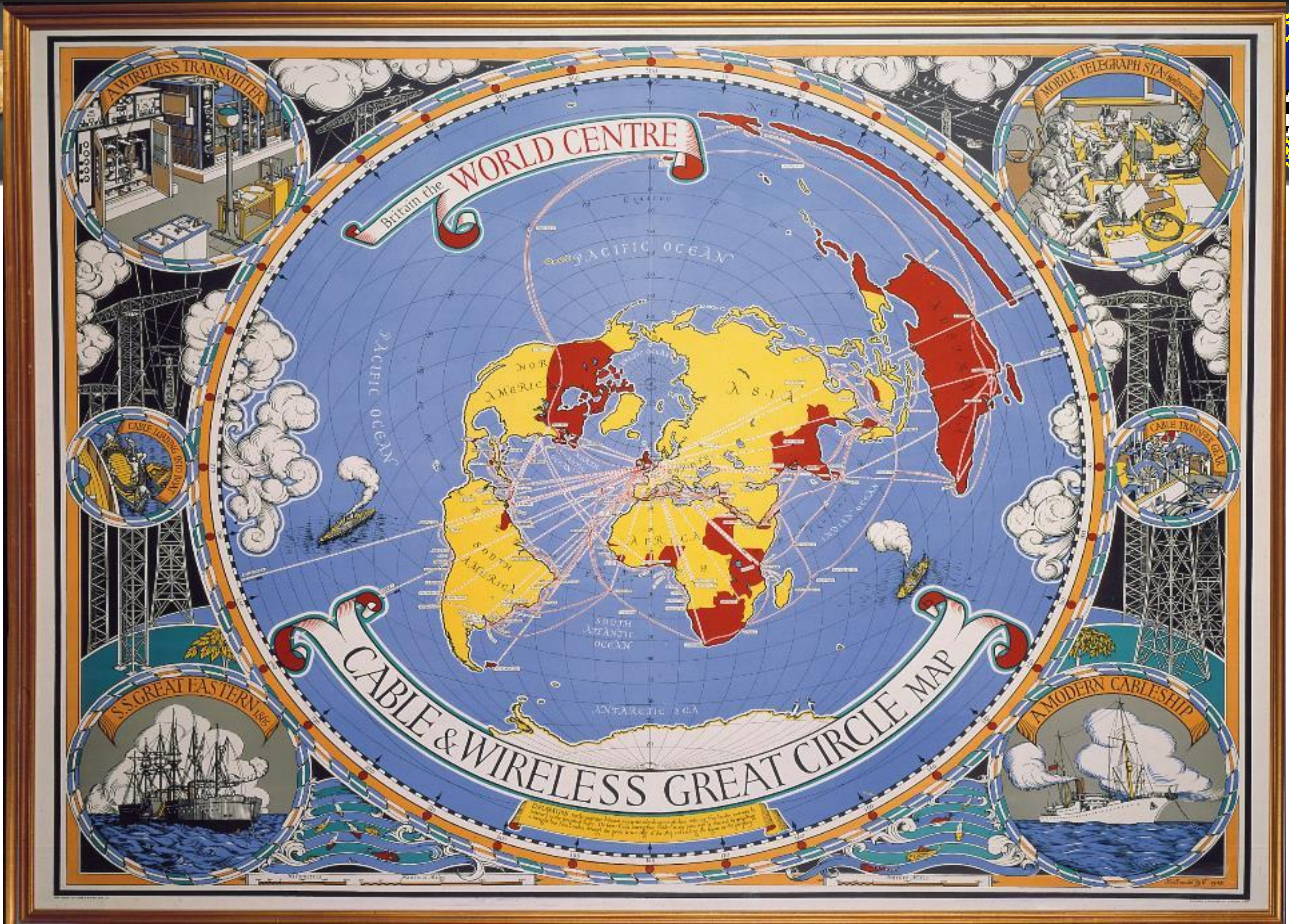
Dr. Michael L. Thomas
Professor of Cyberwarfare Studies
U.S. Air Force Cyber College
Maxwell AFB, Montgomery, Alabama

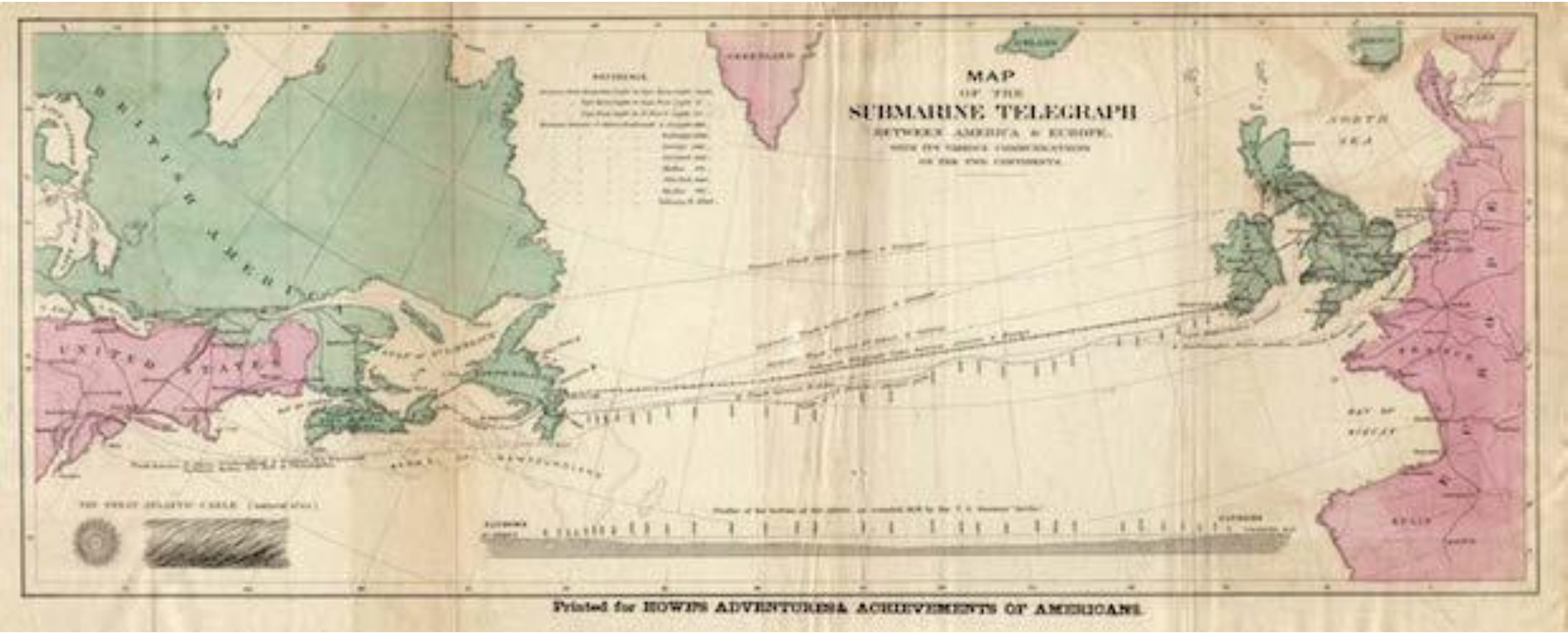


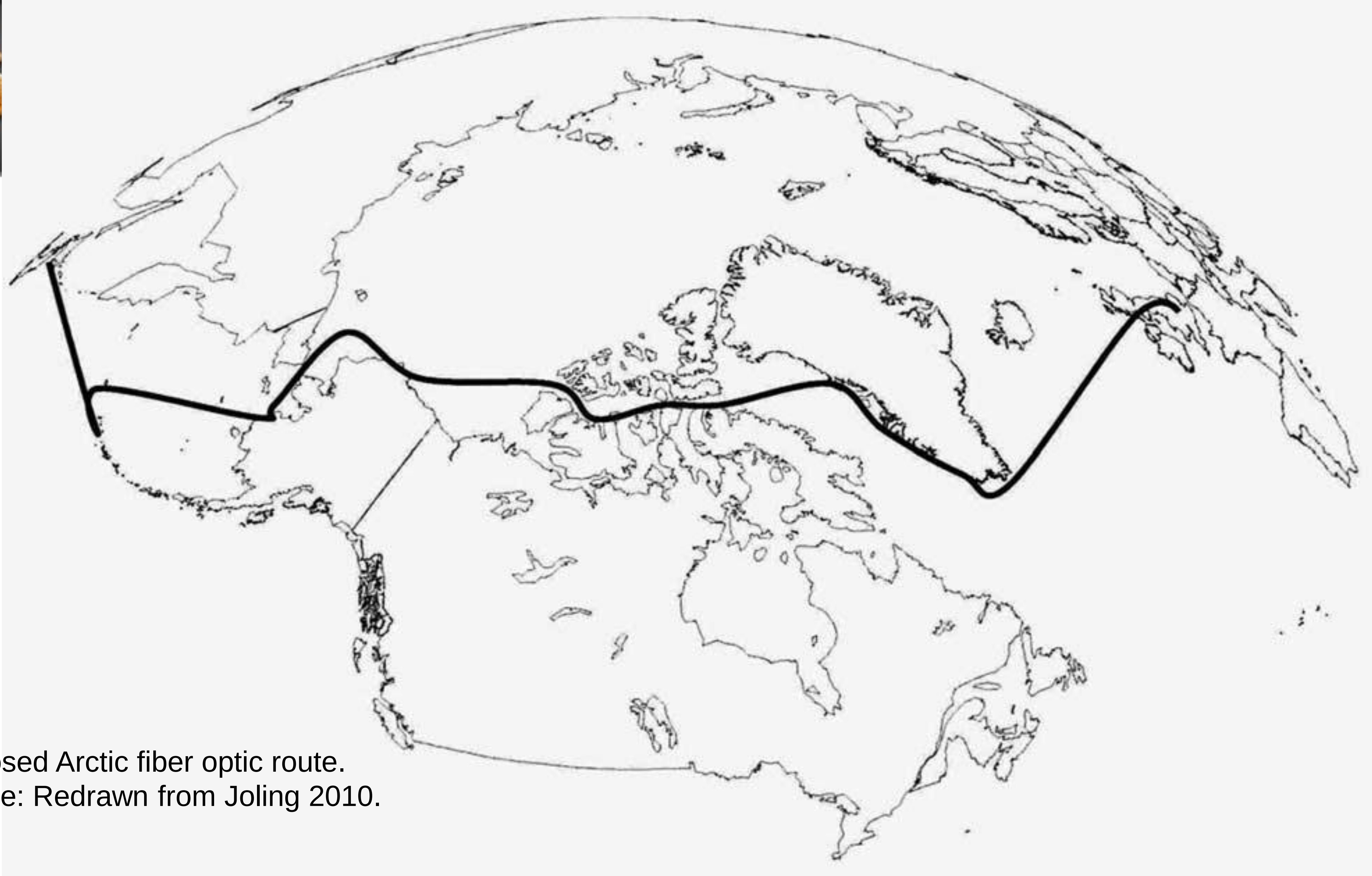
Agenda

- A Little History
- Geopolitics
- Economics of Subsea Cables
- Owners of Subsea Projects
- Future Views
- Chinese Points of Presence in North America

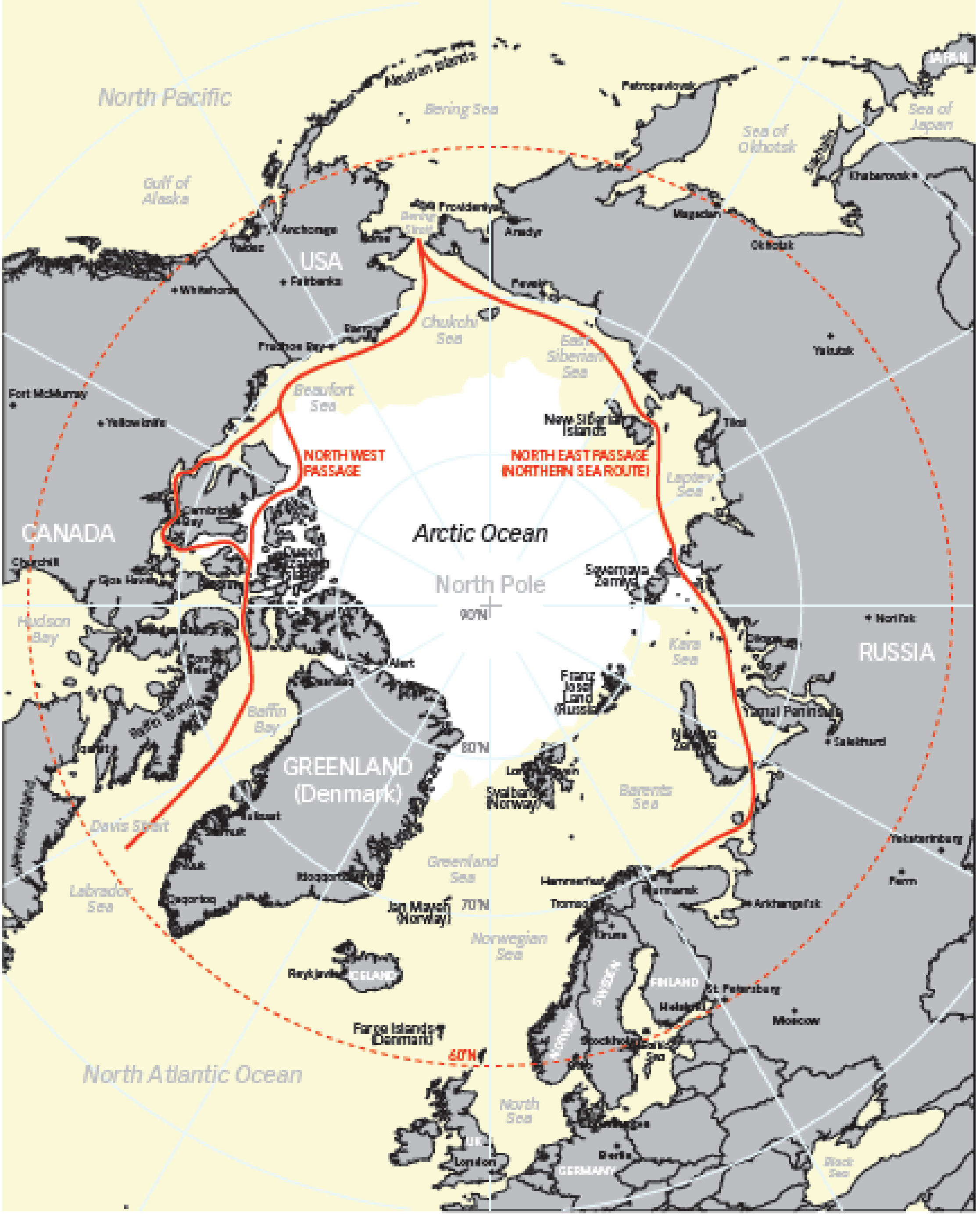

THE INTERNET? STRAIGHT ON AT THE DOG & DUCK, LEFT AT THE BREATHTAKING TOWERS OF INFORMATION-SHARDS GRAFTED ONTO ACTUAL GLASS, STEEL AND LIGHT
A-Z
ROBERT THOMPSON.


A WIRELESS TRANSMITTER
Britain the WORLD CENTRE
MOBILE TELEGRAPH STA.
CABLE LOADING INTO SHIP
CABLE TRANSFER GEAR
PACIFIC OCEAN
PACIFIC OCEAN
NEW ZEALAND
NORTH AMERICA
ASIA
AUSTRALIA
AFRICA
SOUTH AMERICA
INDIAN OCEAN
SOUTH ATLANTIC OCEAN
ANTARCTIC SEA
S.S. GREAT EASTERN 1865
A MODERN CABLESHIP
CABLE & WIRELESS GREAT CIRCLE MAP


MAP
OF THE
SUBMARINE TELEGRAPH
BETWEEN AMERICA & EUROPE,
WITH ITS VARIOUS COMMUNICATIONS
ON THE TWO CONTINENTS
BRITISH AMERICA
UNITED STATES
GREENLAND
ICELAND
NORTH SEA
FRANCE
SPAIN
BAY OF BISCAY
BANKS OF NEWFOUNDLAND
THE GREAT ATLANTIC CABLE (natural size)
Printed for HOWE'S ADVENTURES & ACHIEVEMENTS OF AMERICANS.

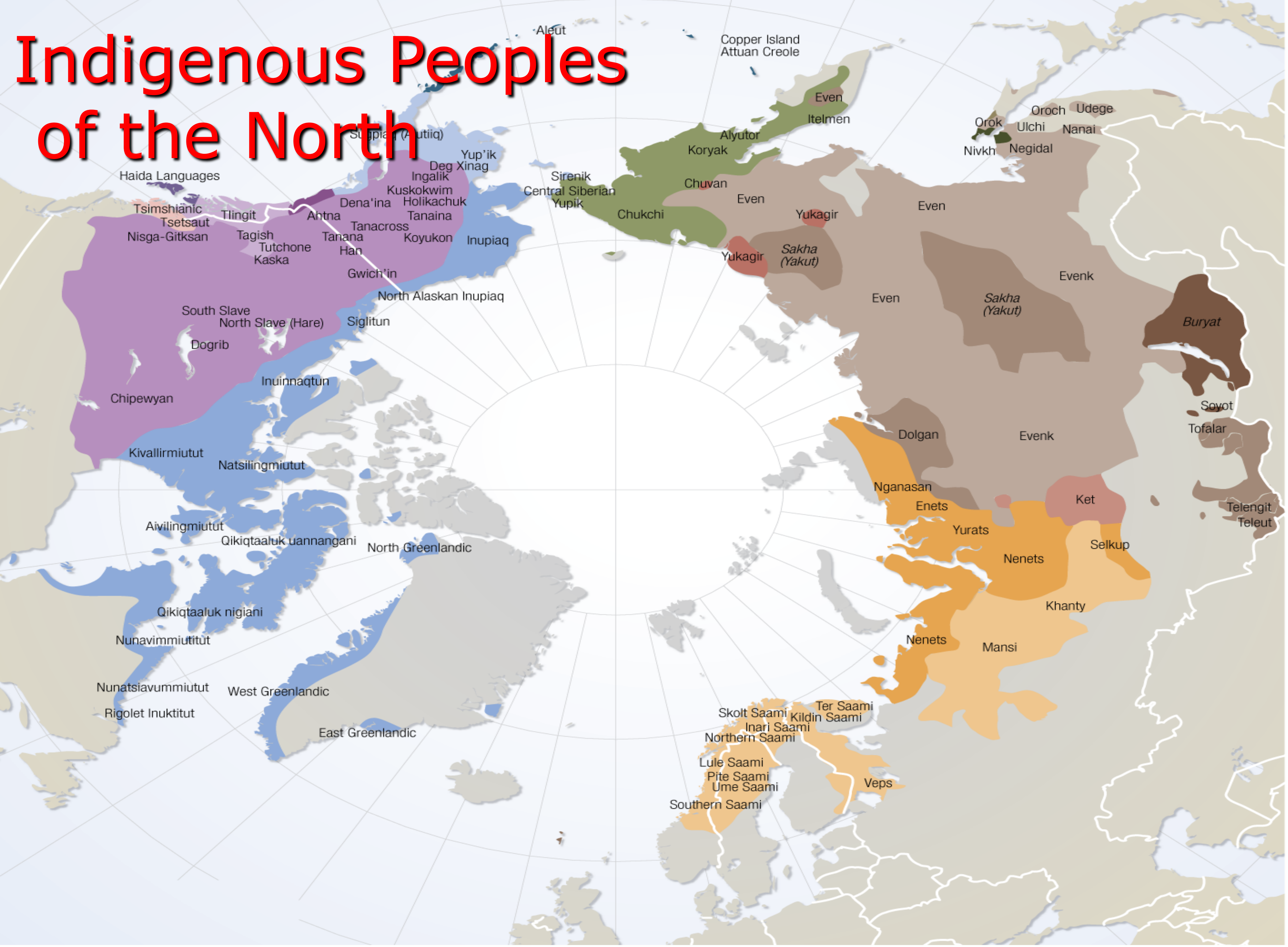


Proposed Arctic fiber optic route.
Source: Redrawn from Joling 2010.



source: Adapted from CIA: The World Factbook, https://www.cia.gov/library/publications/the-world-factbook/maps/refmap_arctic.html

Indigenous Peoples of the North



Na'Dene family

- ■ Athabaskan branch
- ■ Eyak branch
- ■ Tlingit branch
- ■ Haida branch

Indo-European family

- ■ Germanic branch

Eskimo-Aleut family

- ■ Inuit group of Eskimo branch
- ■ Yupik group of Eskimo branch
- ■ Aleut group

Uralic-Yukagiran family

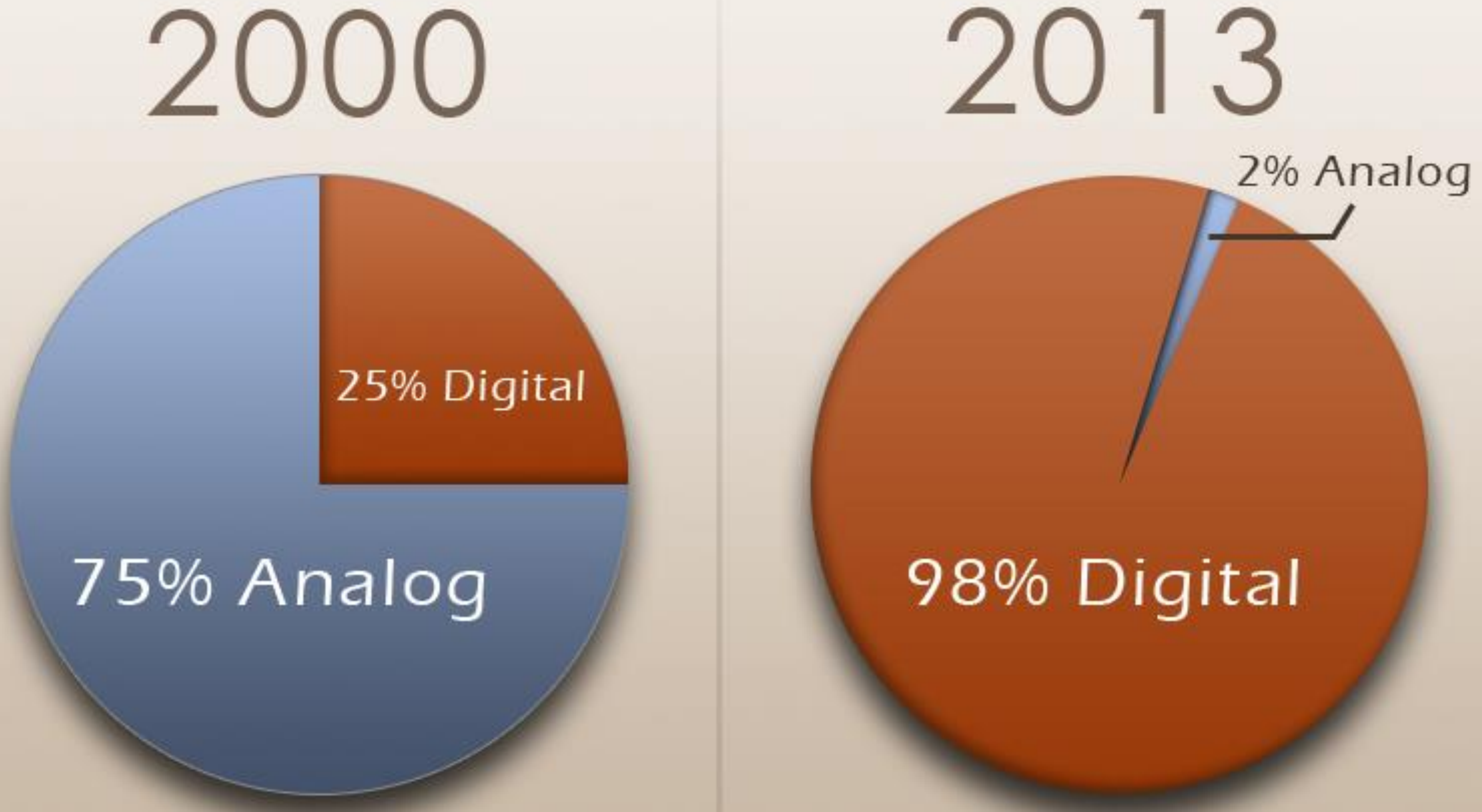
- ■ Finno-Ugric branch
- ■ Samodic branch
- ■ Yukagiran branch

Altaic family

- ■ Turkic branch
- ■ Mongolic branch
- ■ Tunguso-Manchurian branch

- ■ **Chukotko-Kamchatkan family**
- ■ **Ket** (isolated language)
- ■ **Nivkh** (isolated language)
- ■ **Tsimshianic** (isolated language)

Information Overflow

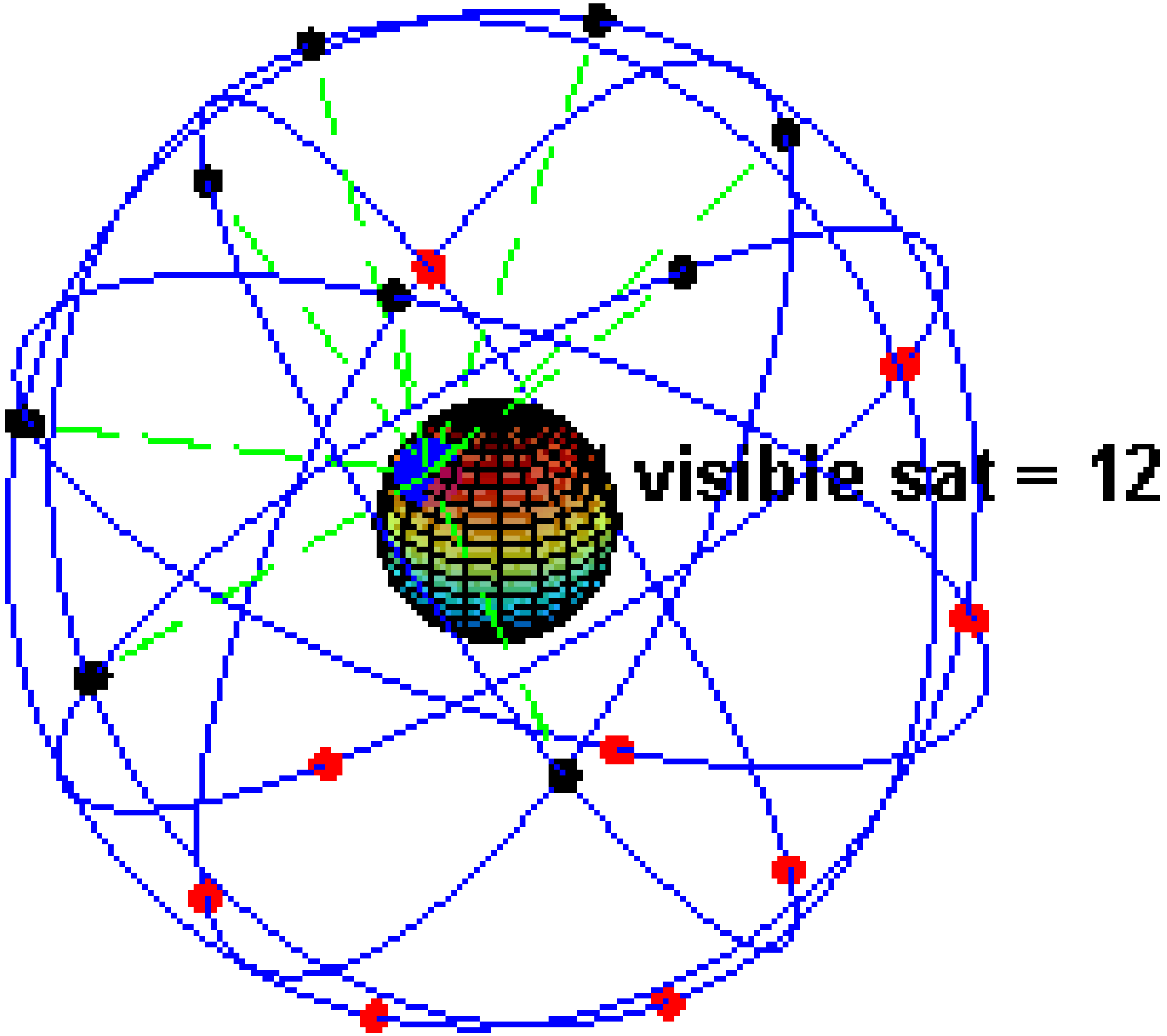


*90% of all digital data has been created in the last three years

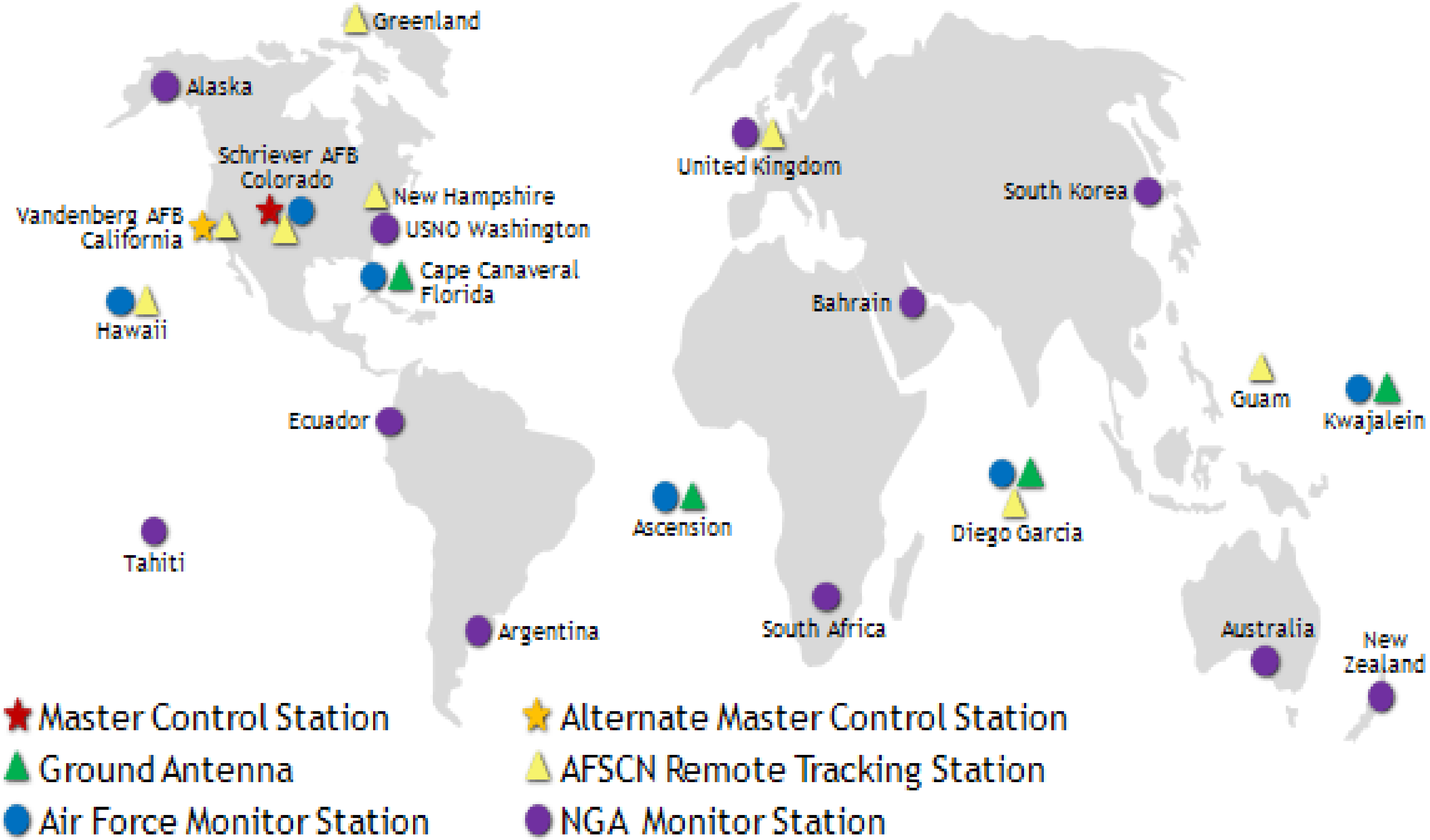
Source: SINTEF 2013

ICT Infrastructure Increase

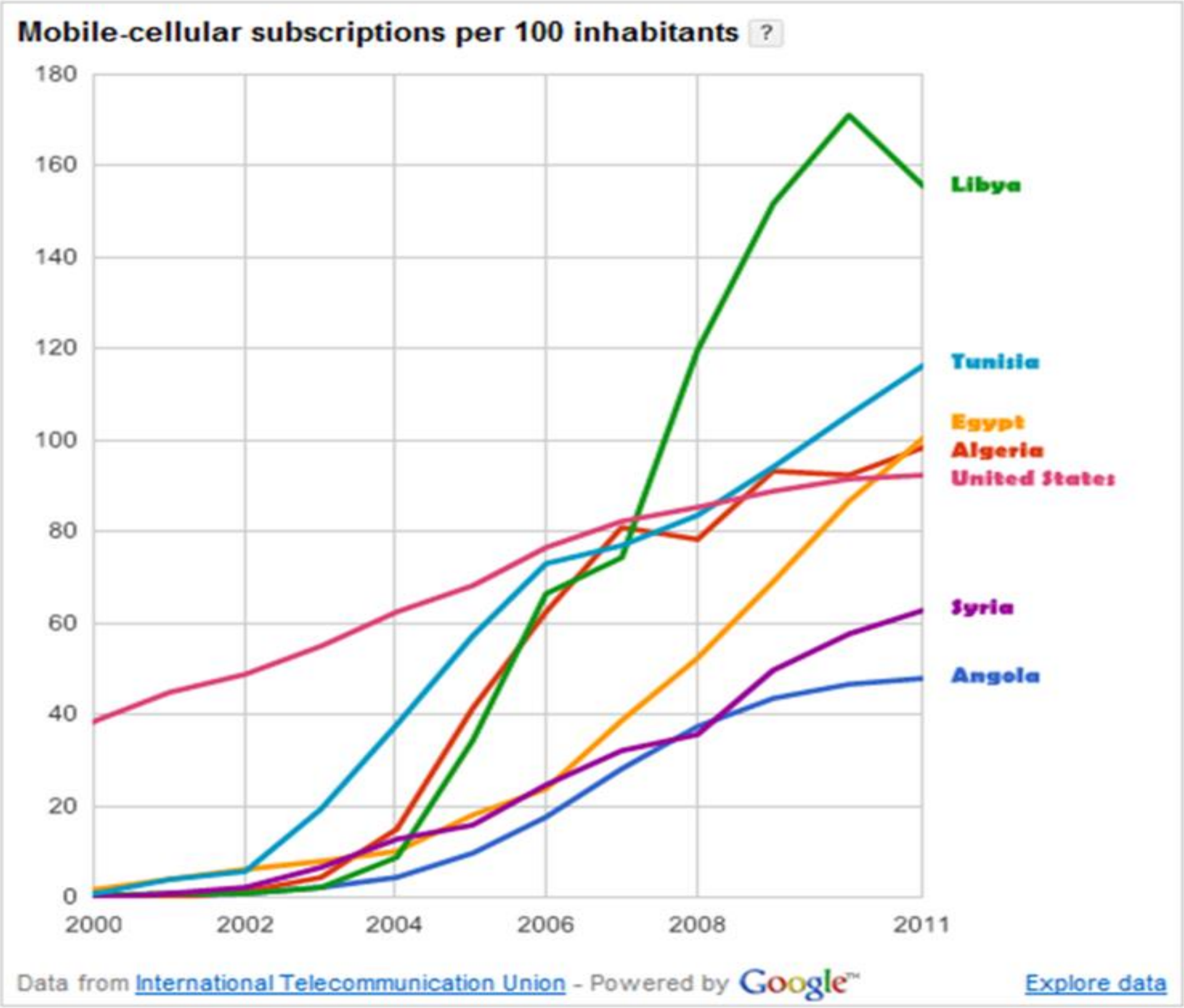
GPS Constellation 24X7 Location Capability



Locations of GPS Ground Stations



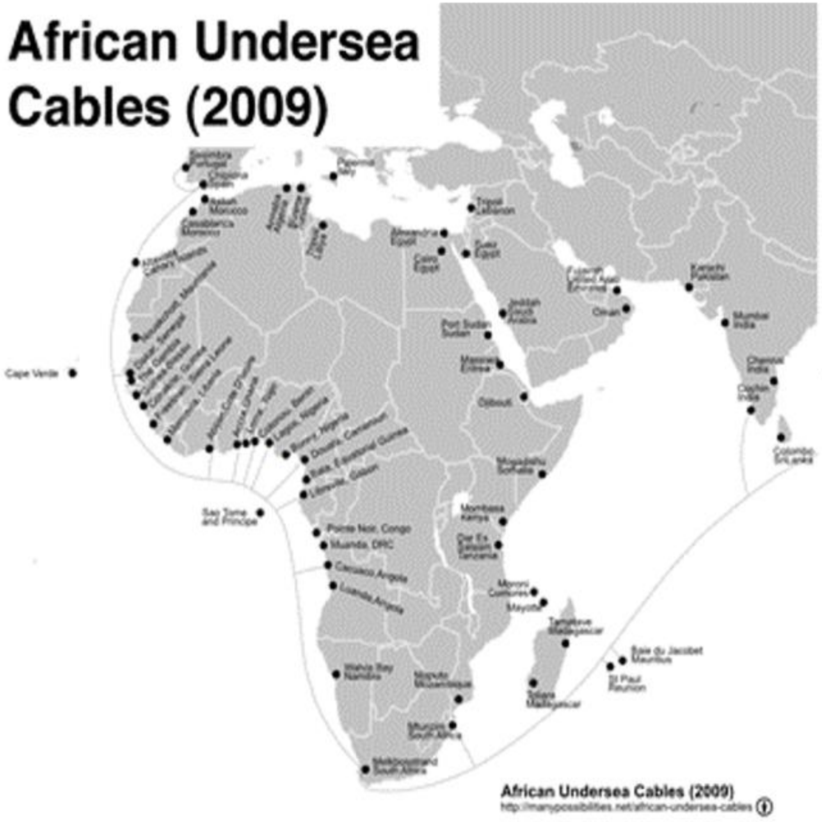
ICT Infrastructure Increase II



Mobile-cellular subscriptions per 100 inhabitants ?

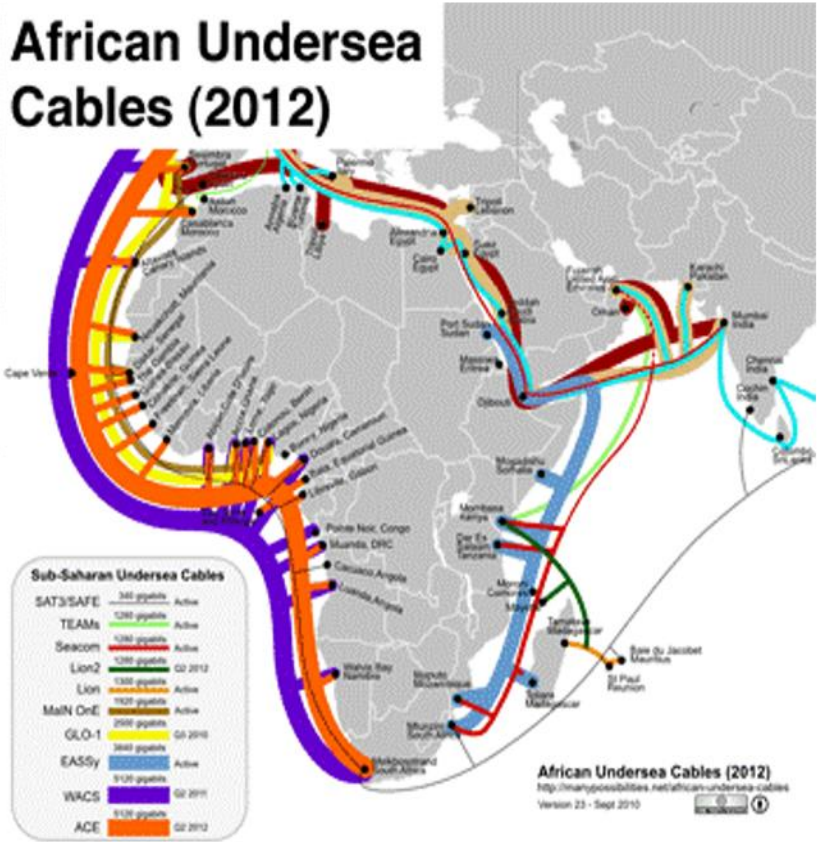
Data from International Telecommunication Union - Powered by Google™ Explore data

ICT Infrastructure Increase III



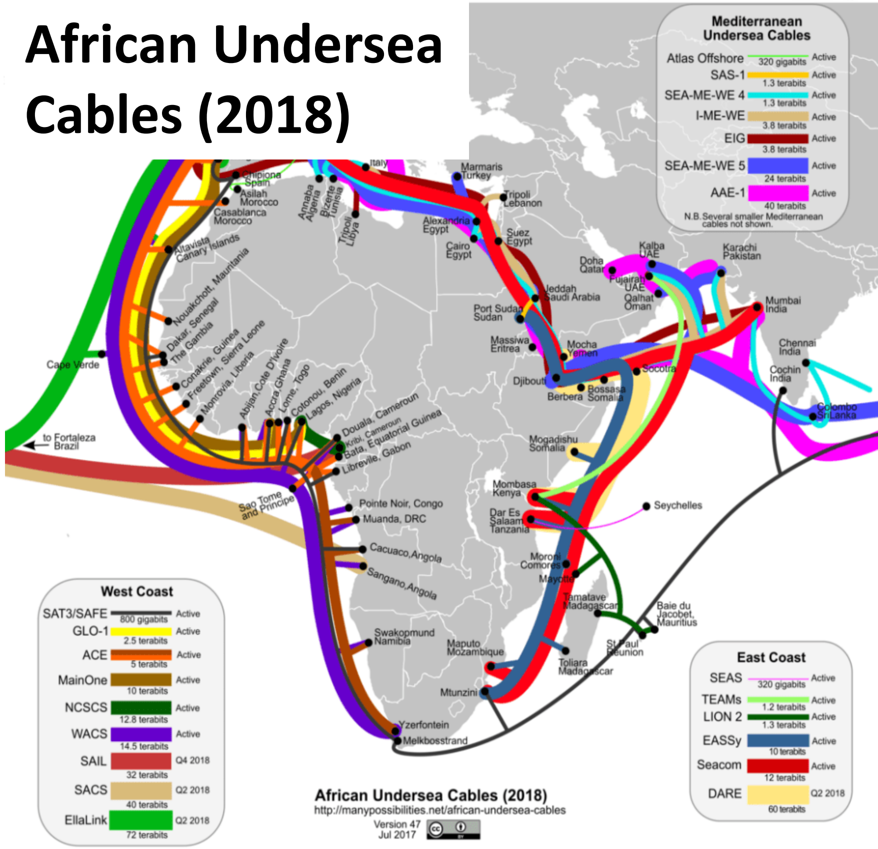
African Undersea Cables (2009)

African Undersea Cables (2009)
http://manypossibilities.net/african-undersea-cables



African Undersea Cables (2012)

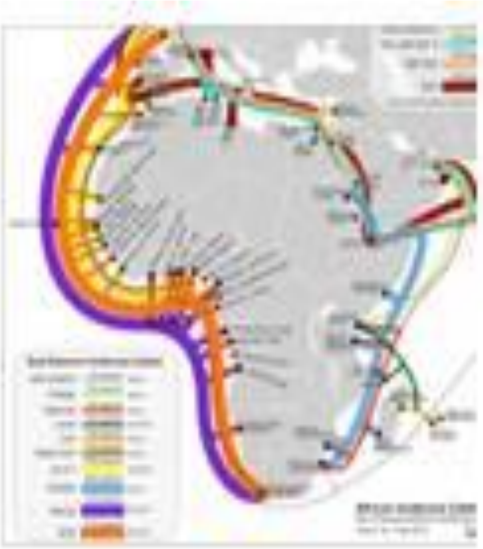
Sub-Saharan Undersea Cables
SAT3/SAFE 340 gigabits Active
TEAMs 1280 gigabits Active
Seacom 1280 gigabits Active
Lion2 1280 gigabits Q2 2012
Lion 1300 gigabits Active
MaIN OnE 1920 gigabits Active
GLO-1 2500 gigabits Q3 2010
EASSy 3840 gigabits Active
WACS 5120 gigabits Q2 2011
ACE 5120 gigabits Q2 2012
Cape Verde
African Undersea Cables (2012)
http://manypossibilities.net/african-undersea-cables
Version 23 - Sept 2010



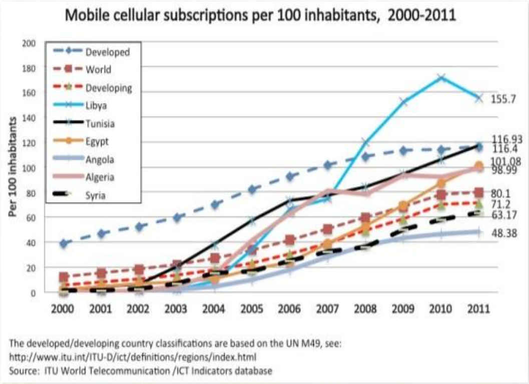
African Undersea Cables (2018)

Total > Sum of the Parts

+



+



Mobile cellular subscriptions per 100 inhabitants, 2000-2011

The developed/developing country classifications are based on the UN M49, see:
http://www.itu.int/ITU-D/ict/definitions/regions/index.html
Source: ITU World Telecommunication /ICT Indicators database

= ?

= Exponential increases in connectivity, information flow and location data

Basics

- Satellites provide between 1-7% of total internet traffic capacity
- Subsea Cables provide >90% capacity
  - For the US, 36 cables carry 95% of all international voice and video
  - Subsea Cables are “the Cloud”
  - Datacenters are worldwide
- Cable routes fall along historic shipping and traffic lanes

History in Warfare

- Subsea Cables have provided telecom traffic for over 100 years
- Spanish American War – US cut cables linking Spain to colonies
- 1st offensive action by UK Navy in WWI was similar to cut off Germany
- WWII, subsea operators in Porthcurno installed flame throwers on beaches at landing points
- *Ergo – to pretend they will not be a target in a future confict is naïve’.*

Annual Accidents

- Cables are vulnerable.
- < 1500 meters buried in yard deep trenches & armored in a steel sheeth
- Most common accident caused by shipping
- Deeper than 1500 meters – laying bare on the sea floor
- On average there are 200 cable faults per year
- Since the US is not part of UNCLOS, willful destruction of cable – 2yrs & $5000 fine.
- Physical infrastructure is critical. Not enough to think of only software hacks.

Where is the data?

- City of LA has deal with Google – all data MUST be stored in lower 48.
  - Most customers cannot strike that type of bargain.
  - Most accidents take 1-2 weeks to repair.
- Most court will not allow companies to collect damages due to loss of access.
  - Issue – loss of access.
  - Issue – loss of data.
- *Breach of cables is a cybersecurity issue.*

Architecture

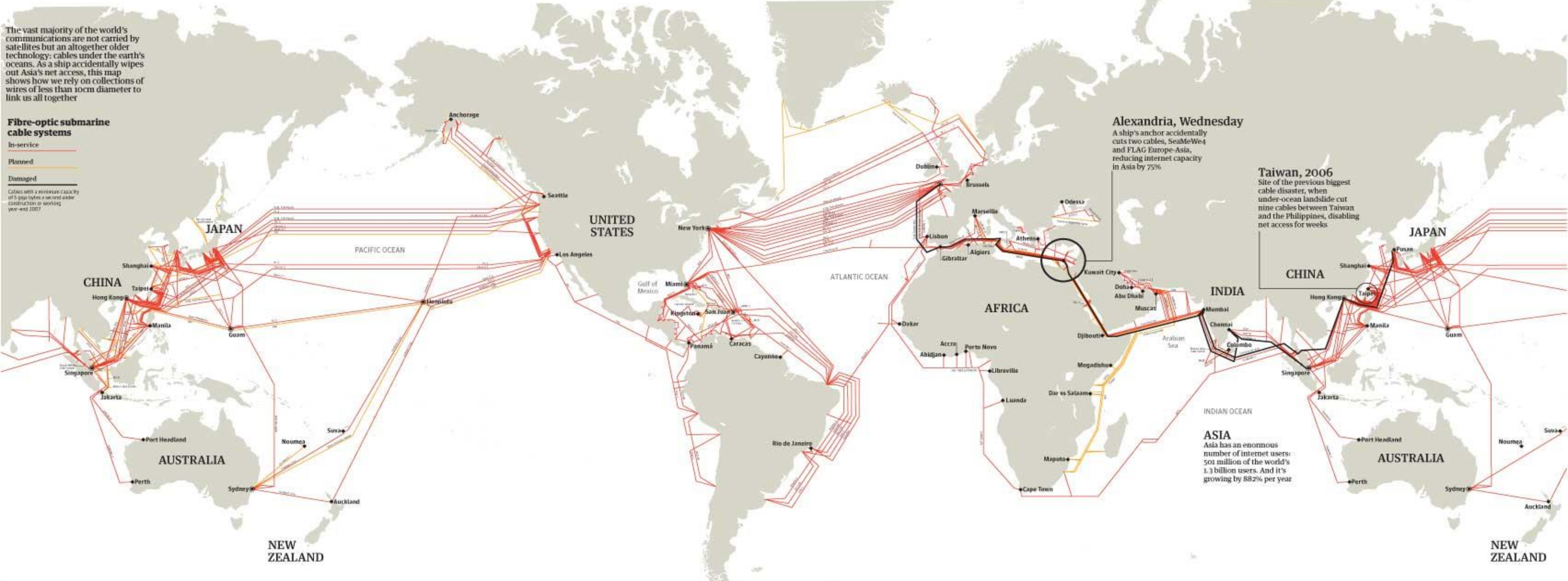
- Redundancy is not efficient
- It is resilient.
- Inefficiency creates resiliency.
- Architecture like a Hydra….
- Complicates the “targeting solution”.
  - Security is increased not by patrols but by resiliency.

Other Factors

- Marginal Profits
- Conflated at traditional landing points
- We are on third generation of subsea cable technology
- Fishermen and shipping companies have to be informed
- Most infrastructure getting long in the tooth.
- Moving data to the cloud entails dependence on undersea links

The internet's undersea world

The vast majority of the world's communications are not carried by satellites but an altogether older technology: cables under the earth's oceans. As a ship accidentally wipes out Asia's net access, this map shows how we rely on collections of wires of less than 10cm diameter to link us all together



Fibre-optic submarine cable systems

In-service

Planned

Damaged

Cables with a minimum capacity of 5 giga bytes a second under construction or working year-end 2007

Alexandria, Wednesday

A ship's anchor accidentally cuts two cables, SeaMeWe4 and FLAG Europe-Asia, reducing internet capacity in Asia by 75%

Taiwan, 2006

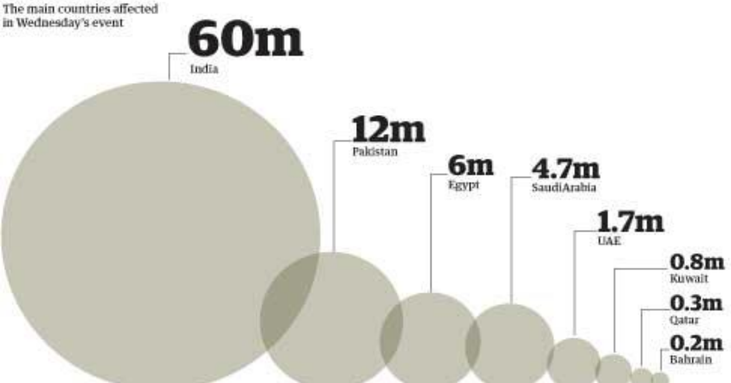
Site of the previous biggest cable disaster, when under-ocean landslide cut nine cables between Taiwan and the Philippines, disabling net access for weeks

ASIA

Asia has an enormous number of internet users: 501 million of the world's 1.3 billion users. And it's growing by 882% per year

Internet users affected by the Alexandria accident

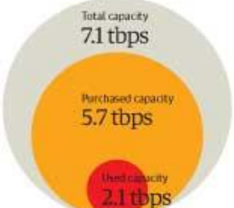
The main countries affected in Wednesday's event



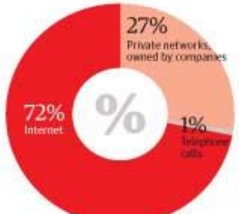
World cable capacity

Submarine cable operators light (turn on) capacity on their systems to sell bandwidth to other carriers. Carriers buy extra capacity, mainly to hold in reserve. On the trans-Atlantic route 80% of the bandwidth is purchased, but only 29% is used

Capacity in terabytes a second



What makes up "used capacity"?



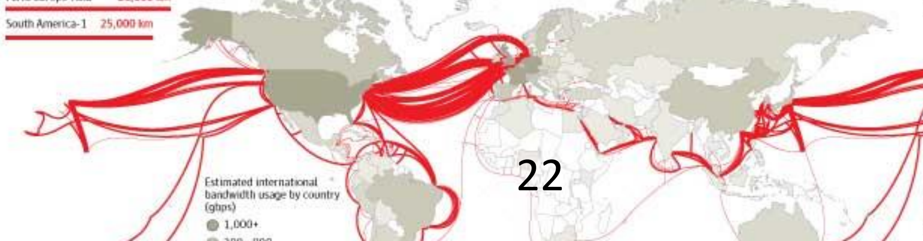
The longest submarine cables

The SeaMeWe-3 system from Norden in Germany to Keoje, South Korea connects 32 different countries with 39 landing points

SeaMeWe-3	39,000 km
Southern Cross	30,500 km
China-US	30,476 km
FLAG Europe-Asia	28,000 km
South America-1	25,000 km

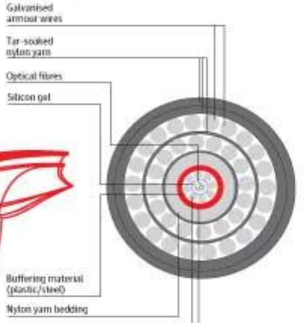
The world's cables in bandwidth

The first intercontinental telephony submarine cable system, TAT-1, connected North America to Europe in 1958 and had an initial capacity of 640,000 bytes per second. Since then, total trans-Atlantic cable capacity has soared to over 7 trillion bps

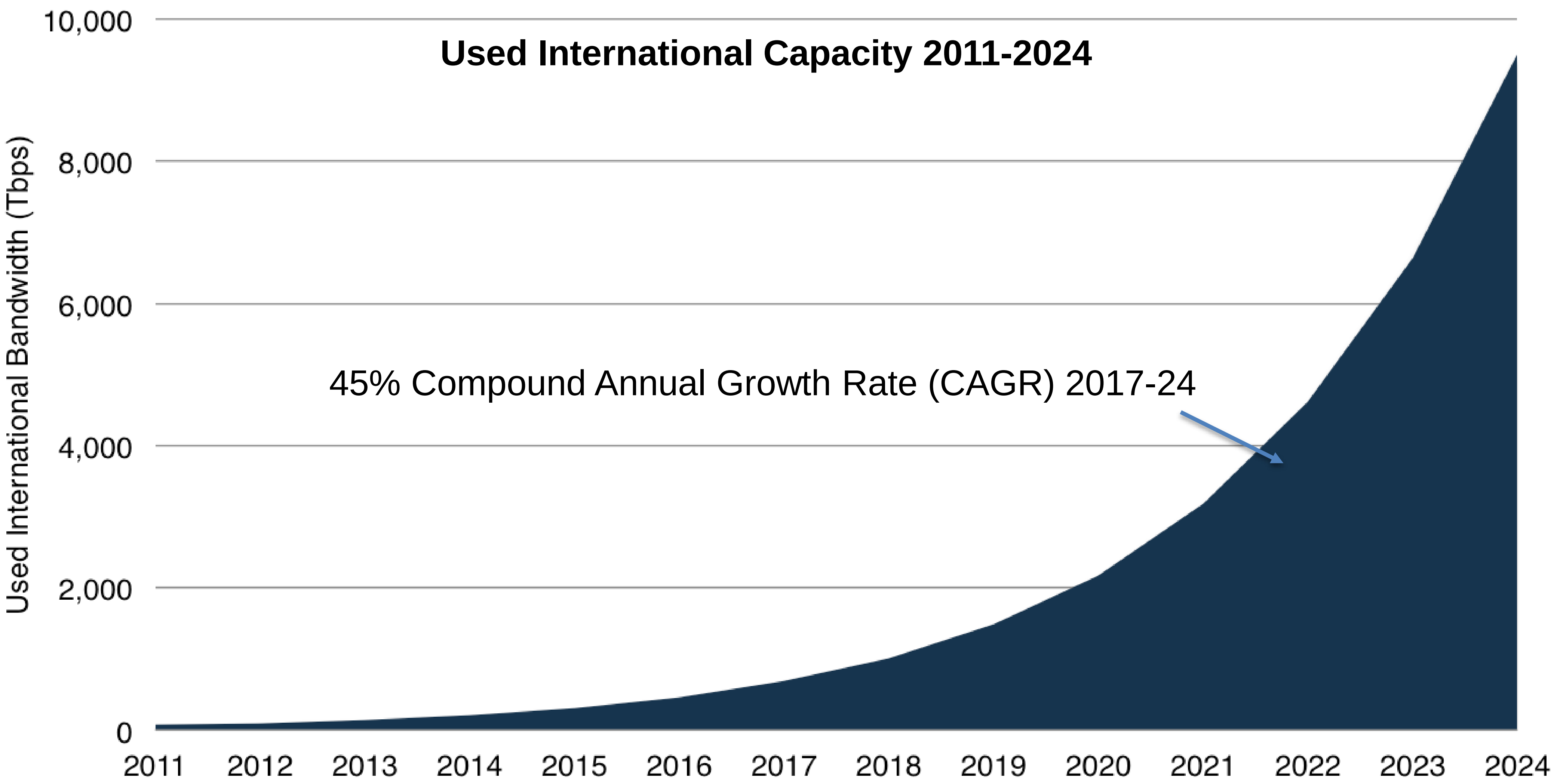


Cross-section of a cable

Cables of this strength are typically 69 mm in diameter and weigh over 10,000 kilograms a kilometer. In deeper waters, lighter and less insulated cables are used



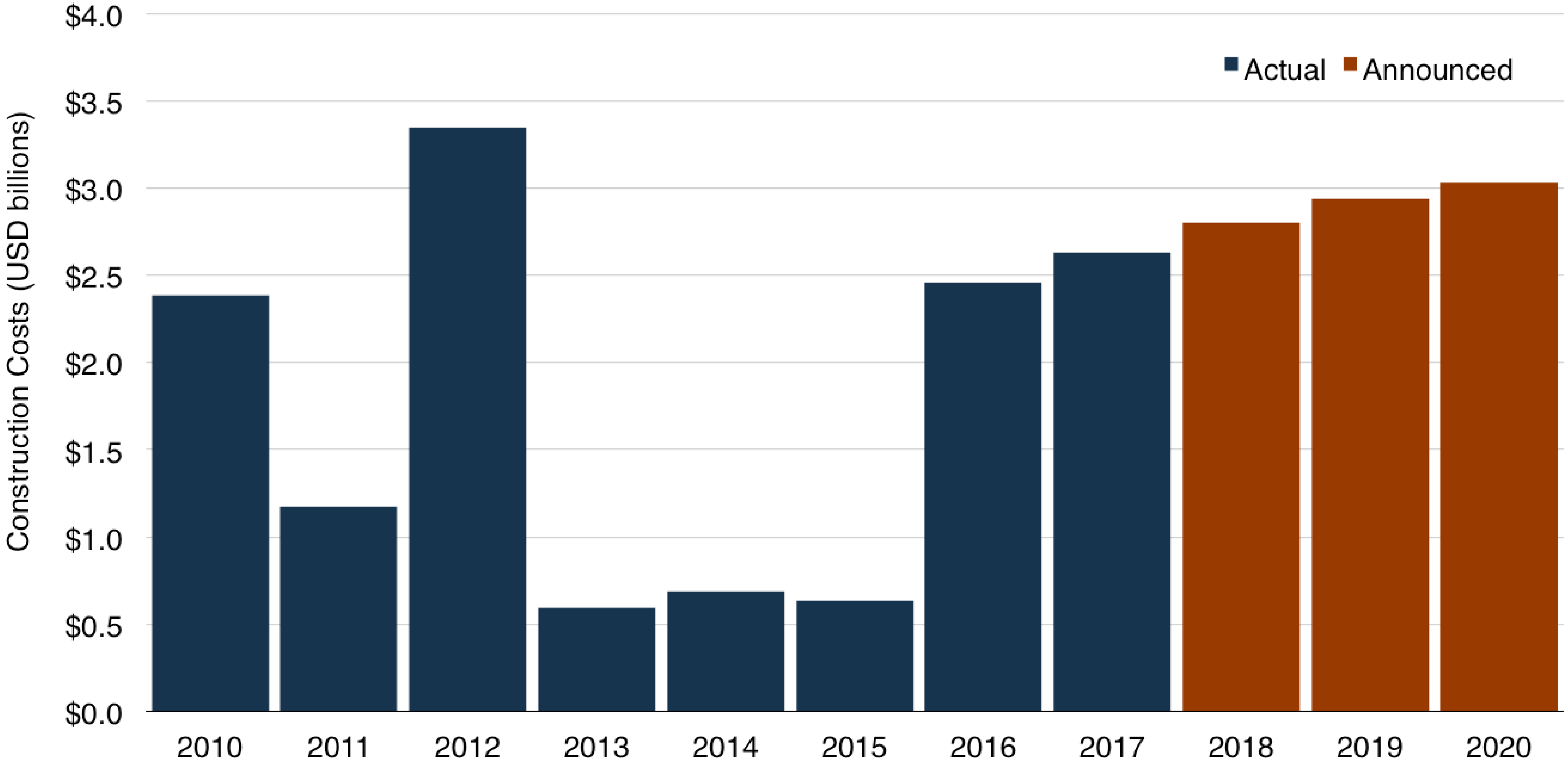
Compounding Growth Leading to Massive Volumes



https://www.telegeography.com/

Large Investment in New Cables Underway

Investment in New Submarine Cable Systems by Request For Service (RFS) Year, 2010-2020



https://www.telegeography.com/

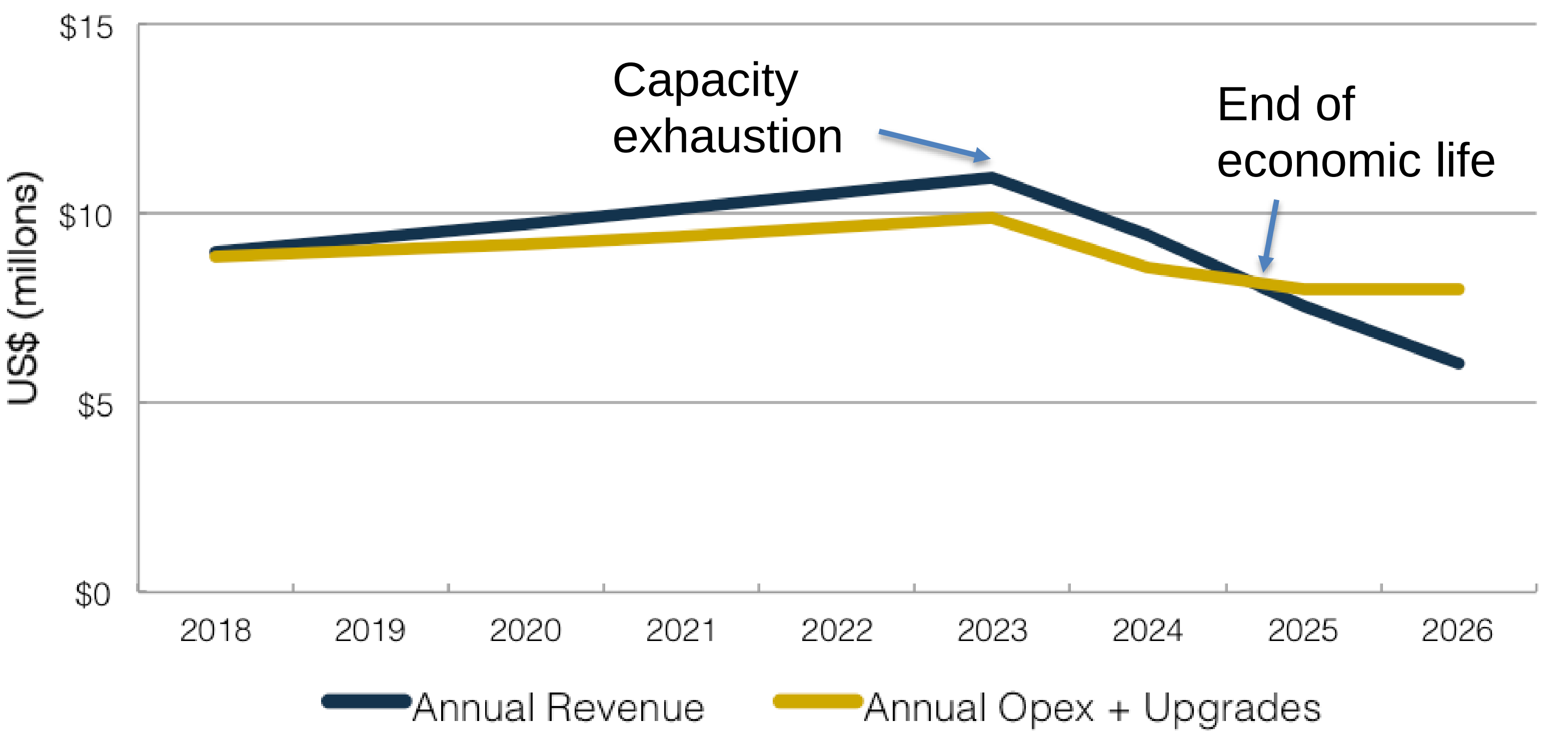
How is a Submarine Cable Retired?

- Cables' minimum *design* life is 25 years, but what matters is *economic* life
- Economic life of a cable depends on a system's revenues exceeding costs
- Cables must continually add capacity to offset the negative effect of lower capacity prices on revenues
- At some point, annual costs exceed revenues, once this threshold is reached…

What does economic life look like?

- Model Assumptions:
- Construction costs recovered/written off
- Opex - $8m/year
- Upgrade cost - $75k/100G, declining 10% annually
- Prices - $15k/month/100G, declining 20% annually
- Sales - 100% 100G leases
- Demand - 5 Tbps sold in 2018, rising 30% annually

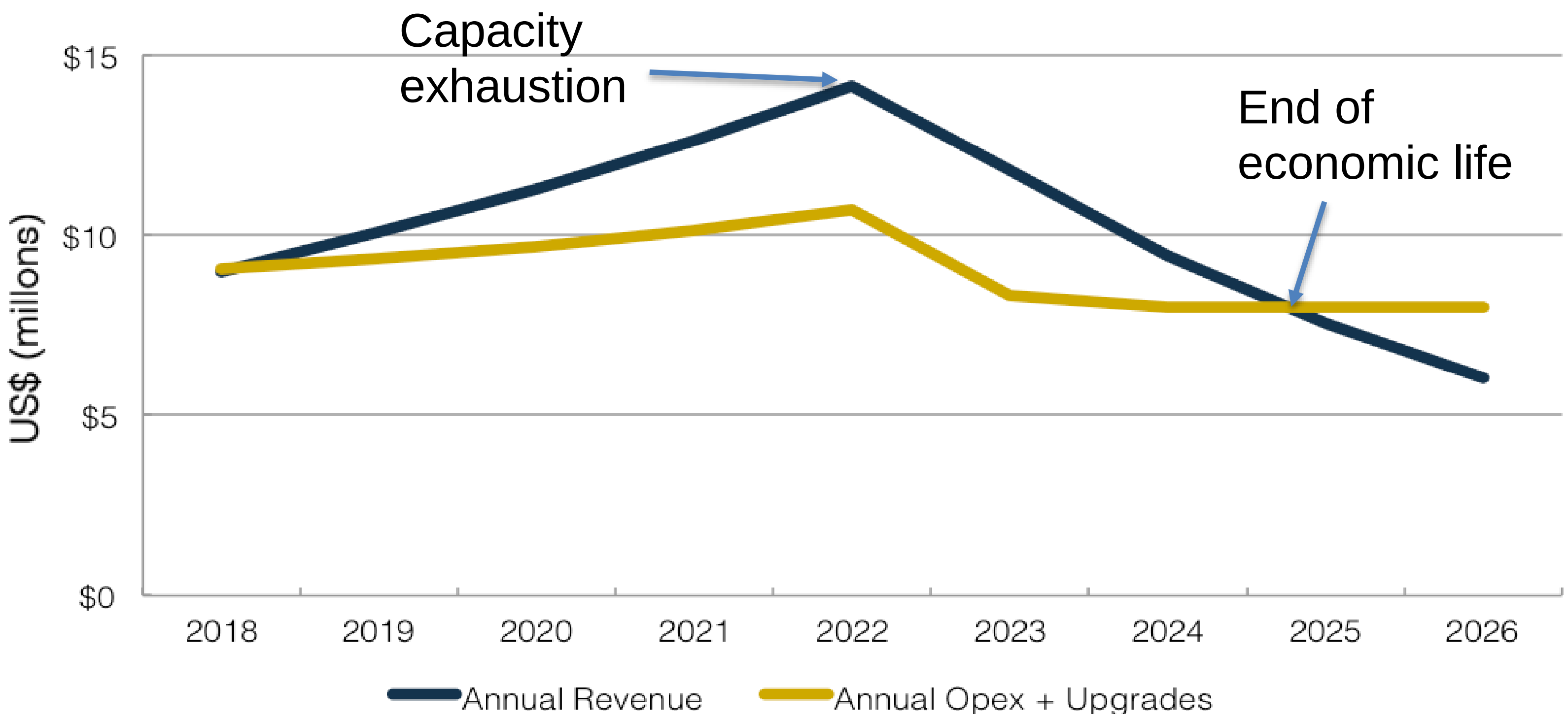
Hypothetical “Old” 20 Tbps Cable



What does economic life look like?

- Model Assumptions:
- Construction costs recovered/written off
- Opex - $8m/year
- Upgrade cost - $75k/100G, declining 10% annually
- Prices - $15k/month/100G, declining 20% annually
- Sales - 100% 100G leases
- Demand - 5 Tbps sold in 2018, rising 40% annually

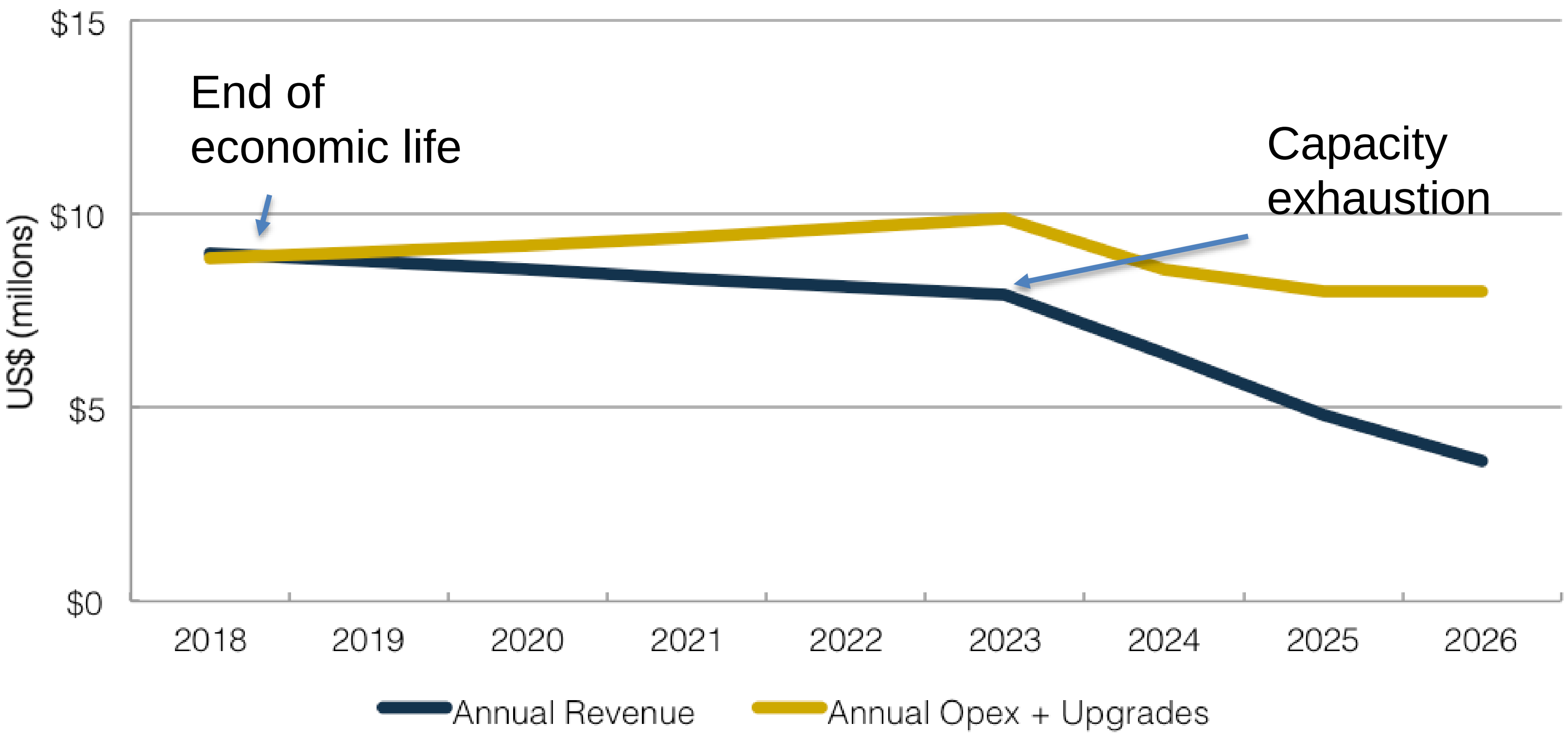
Hypothetical "Old" 20 Tbps Cable



What does economic life look like?

- Model Assumptions:
- Construction costs recovered/written off
- Opex - $8m/year
- Upgrade cost - $75k/100G, declining 10% annually
- Prices - $15k/month/100G, declining 25% annually
- Sales - 100% 100G leases
- Demand - 5 Tbps sold in 2018, rising 30% annually

Hypothetical “Old” 20 Tbps Cable



End of economic life

Capacity exhaustion

Factors Influencing Economic Life

- Price erosion – more rapid erosion will move up the end of economic life
- Demand – large differences in volumes and pace of growth lead to far different economic lifespans across regions/routes
- Upgrade costs – unit upgrade costs are often higher on older cables compared to newer systems
- Increased competition – new high capacity cables can reduce an older cable's market share, slower sales growth shortens economic life
- Faults – increases in repairs as cables age, which would boost costs and hasten end of life
- Capacity exhaustion – running out of capacity does *not* mean immediate end of economic life, but does start the countdown to retirement

Cable retirement challenges

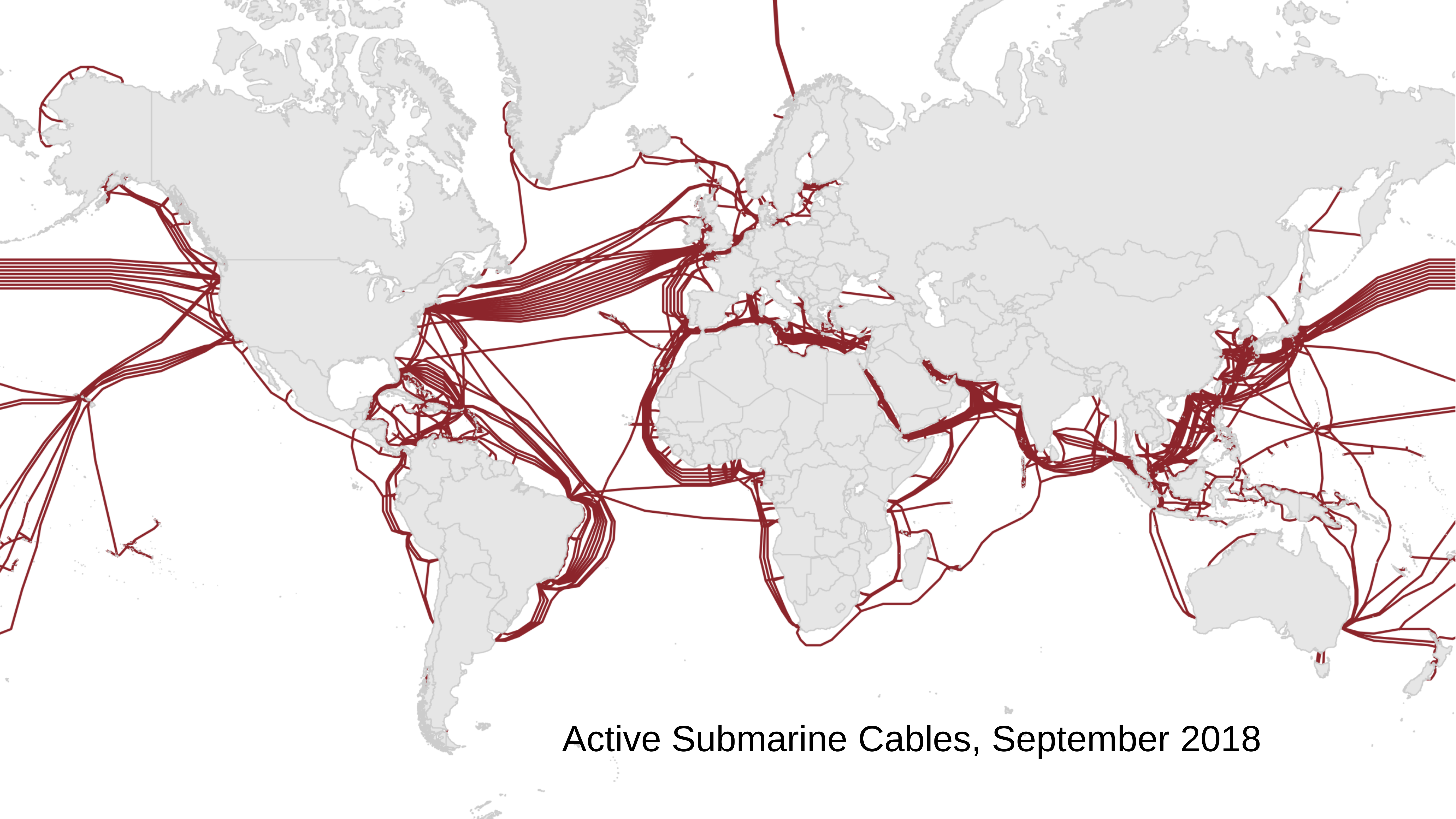
- Consortia have differing requirements for voting for retirement: unanimous decision? majority?
  - Members with favorable backhaul agreements may be reluctant to vote for retirements
  - Members from countries with a limited number of cables may be less inclined to vote for retirement
- Customers with existing IRUs may need to be compensated
- Hidden retirement costs – some governments require portions of cables to be recovered once they are decommissioned

Cable Retirement Phases

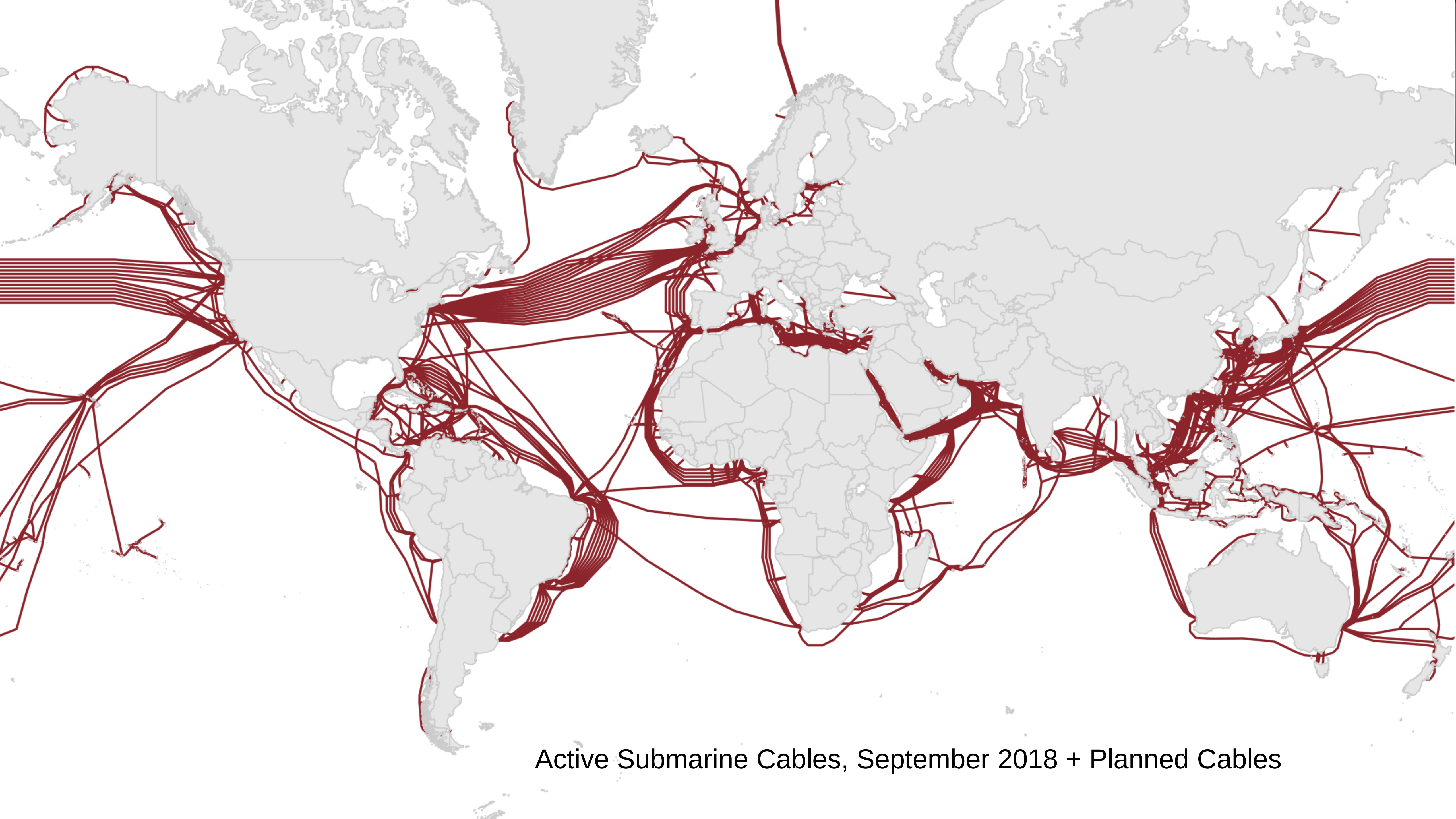
- Zombie Cables (commercial retirement) – cable remains operational, but not actively selling capacity or engaging in additional upgrades
- Dismembered Cables (partial retirement) – only specific spans or branches are decommissioned
  - e.g. Americas-I, Columbus-II, CANTAT-3
- Death Row Cables ("soft" decommissioning) – maintenance contract cancelled, but cable remains in service until the next fault
- Dead Cables (full decommissioning)

Traits of the New Technologies in Cables

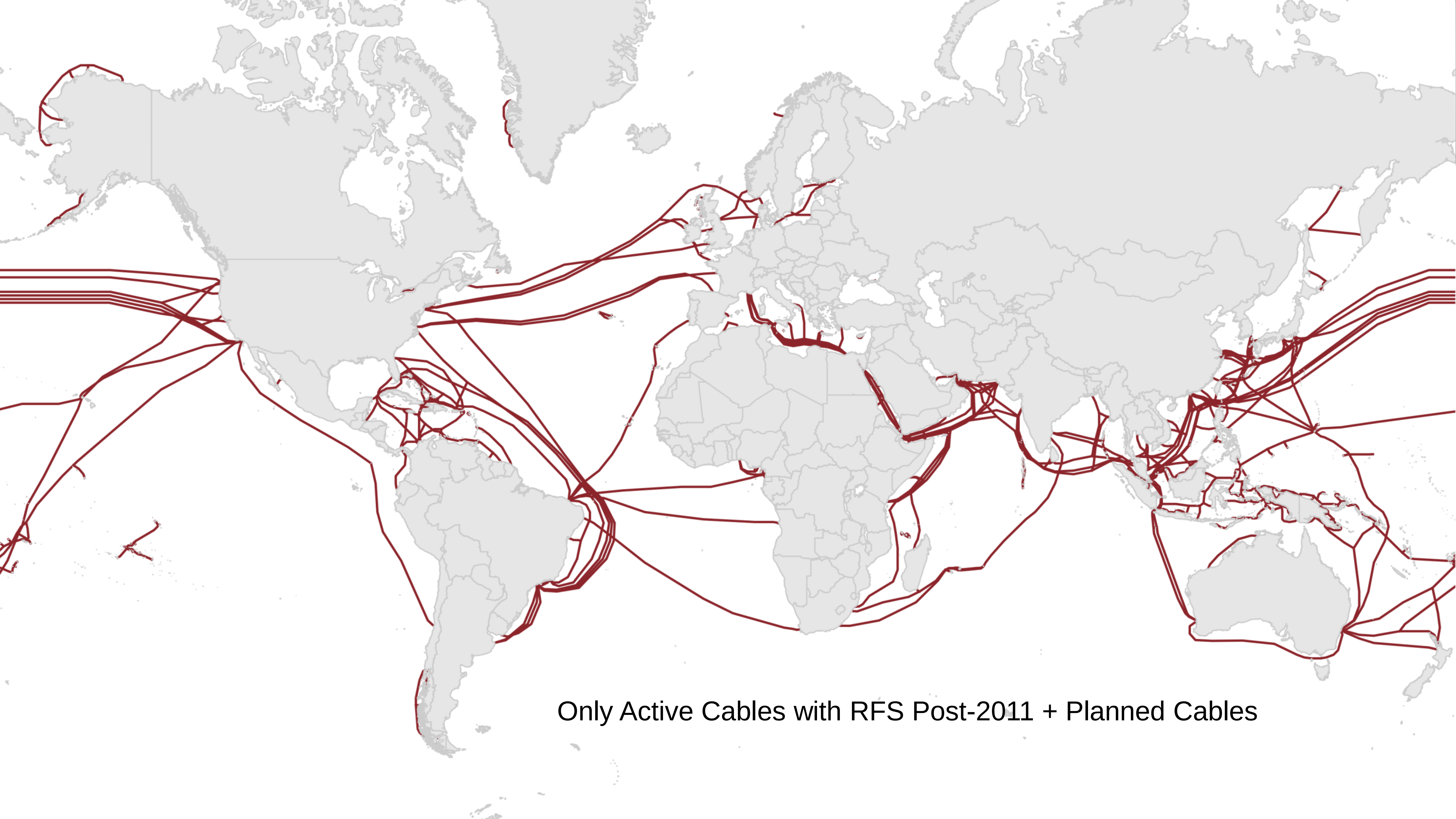
- Not a one-for-one replacement
  - Higher fiber pair count in new cables
  - New routings and landings
  - Different topologies (R.I.P. - self-healing rings)
- Not always the same companies involved, several new builders
  - Content providers: Google, Facebook, Amazon, Microsoft
  - Seaborn Networks
  - Aqua Comms
  - RTI
  - Hawaiki
  - Super Sea Cable Networks



Active Submarine Cables, September 2018

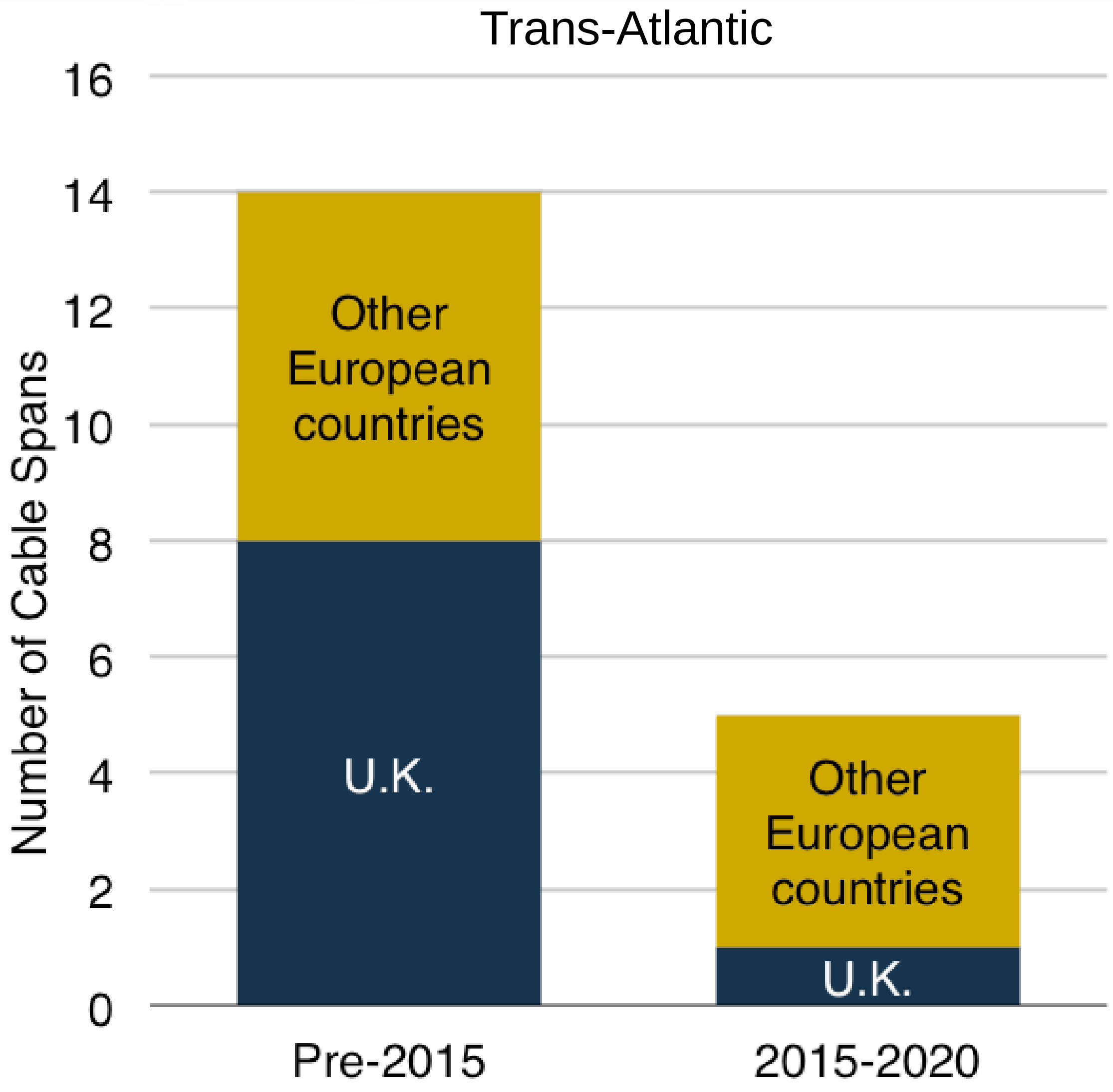


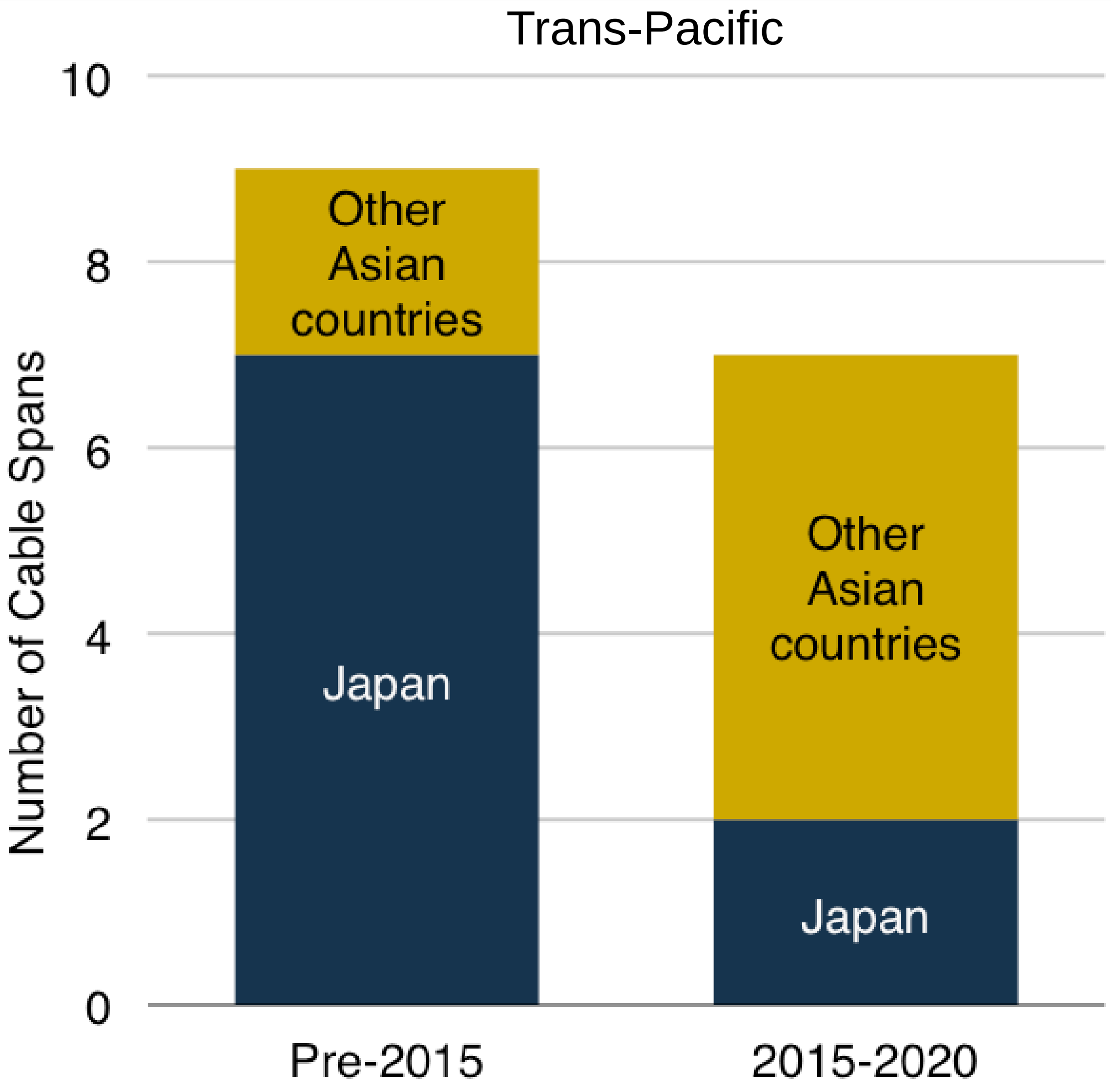
Active Submarine Cables, September 2018 + Planned Cables



Only Active Cables with RFS Post-2011 + Planned Cables

New cables evolving beyond Japan and the U.K.

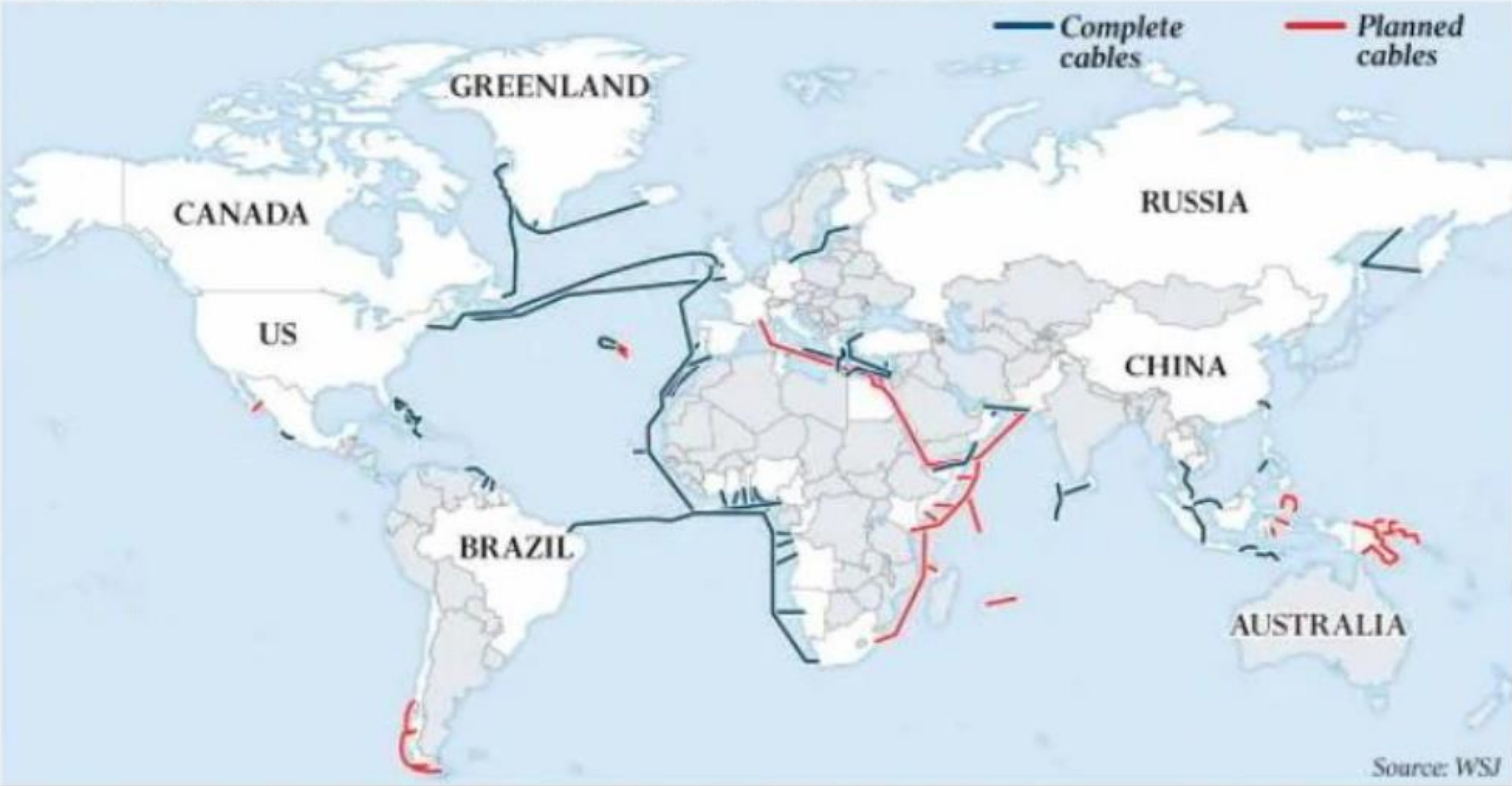




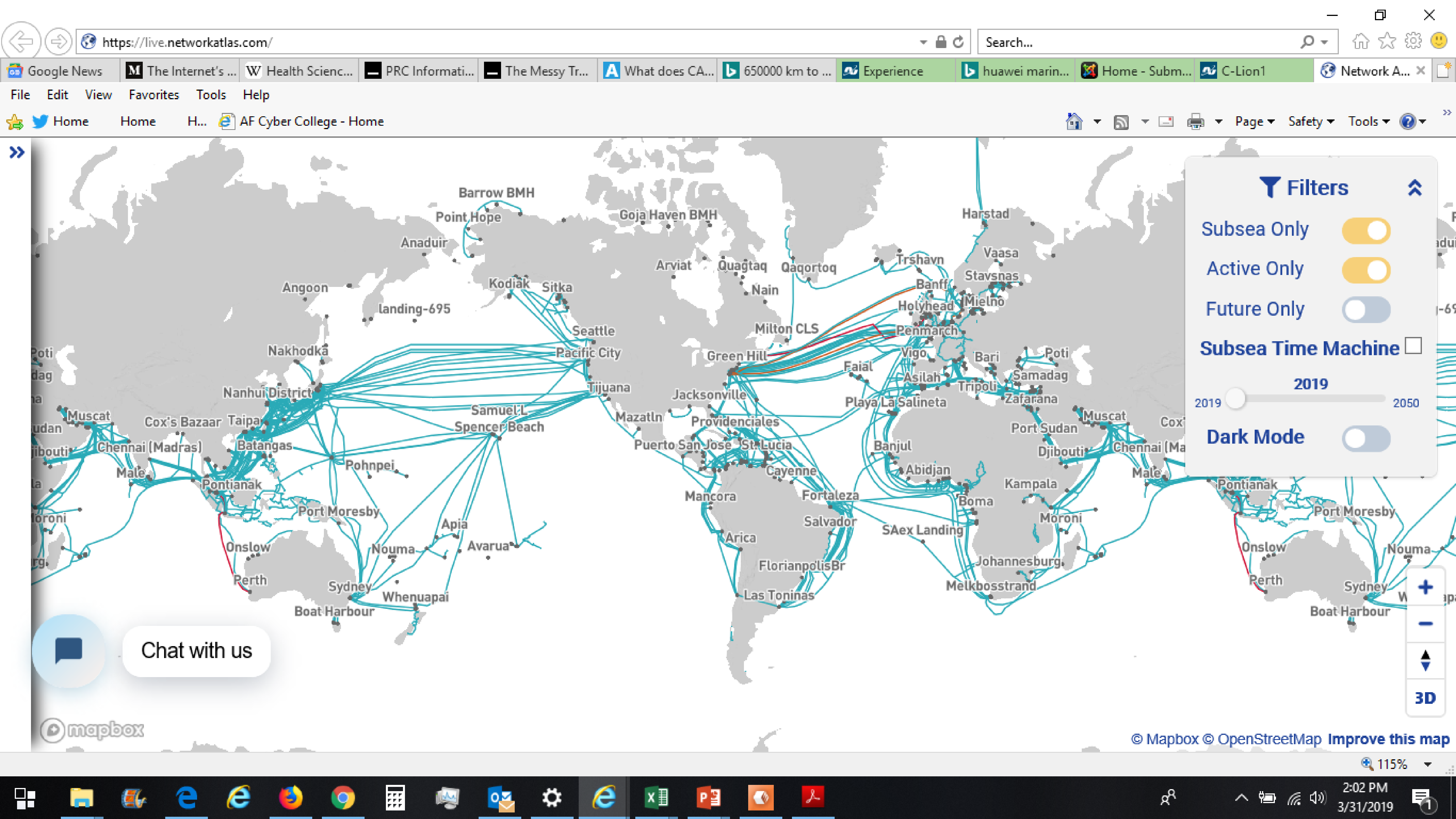
Few Thoughts on the Next Generation of Cables

- Ecosystem Collapse - The retirement of cables using consortium maintenance agreements may increase the cost for other cables covered under the agreement due to the reduction in total kilometers covered
- Mass Migration - Customers migrating capacity off of retired cables will serve as new revenue sources for other cables
- Rise of New Players - Even if cable retirements are slow to materialize, this does not change the fact that many new cables will be needed to meet the forecasted demand requirements
- Most UK and Japanese cables are older technology
  - "Friendly" cables currently dominate over 550,000 miles of cable runs
  - Most laid between 2000-2002; many will be due for retirement
- Huawei Marine currently has over 30,000 miles of cable on 90 projects
  - 5% that will increase

Huawei Marine's undersea cable network



Source: WSJ



Filters

Subsea Only ●

Active Only ●

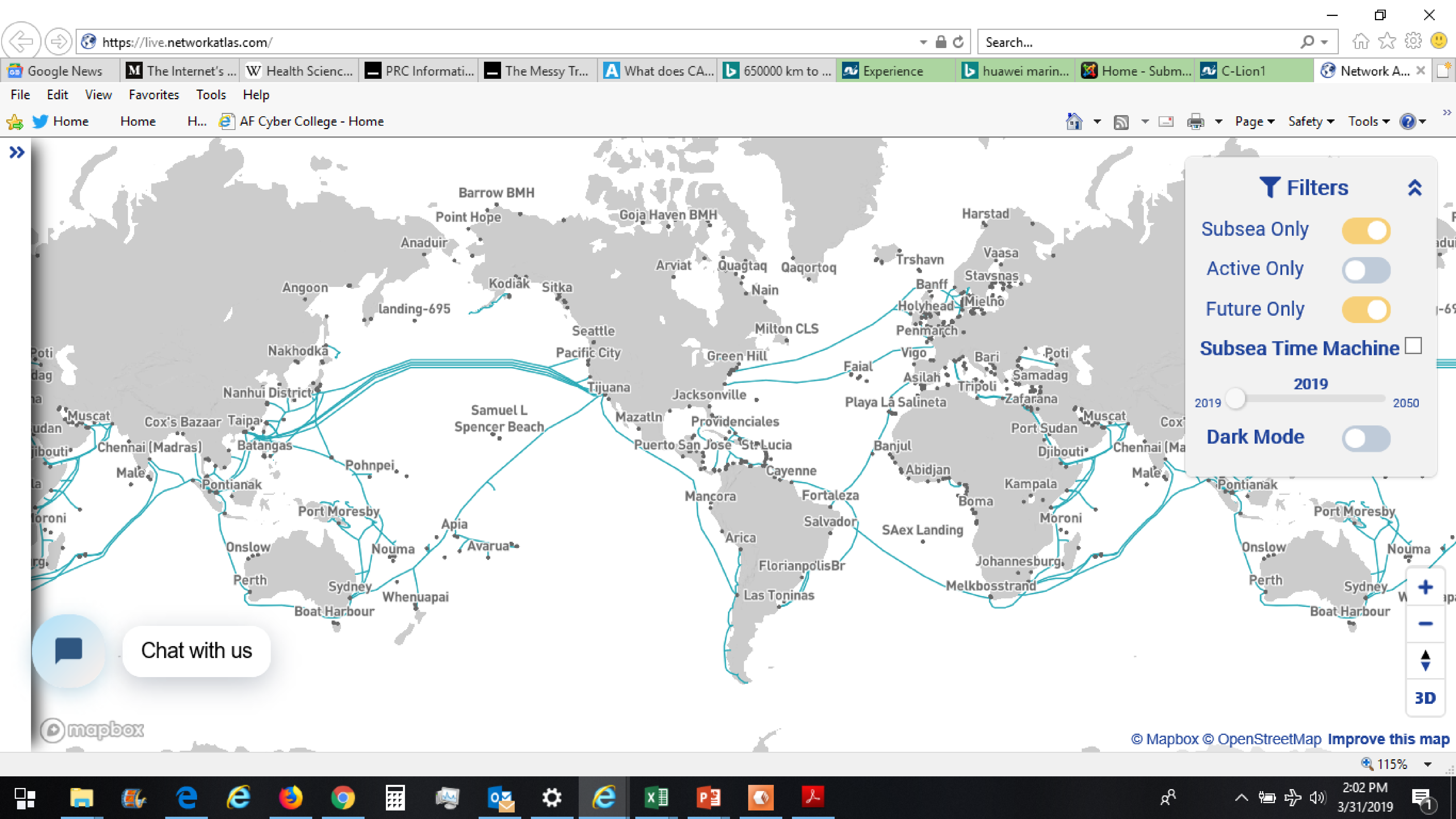
Future Only ○

Subsea Time Machine ☐

2019

2019 2050

Dark Mode ○



Filters

Subsea Only ☑

Active Only ☐

Future Only ☑

Subsea Time Machine □

2019

2019 2050

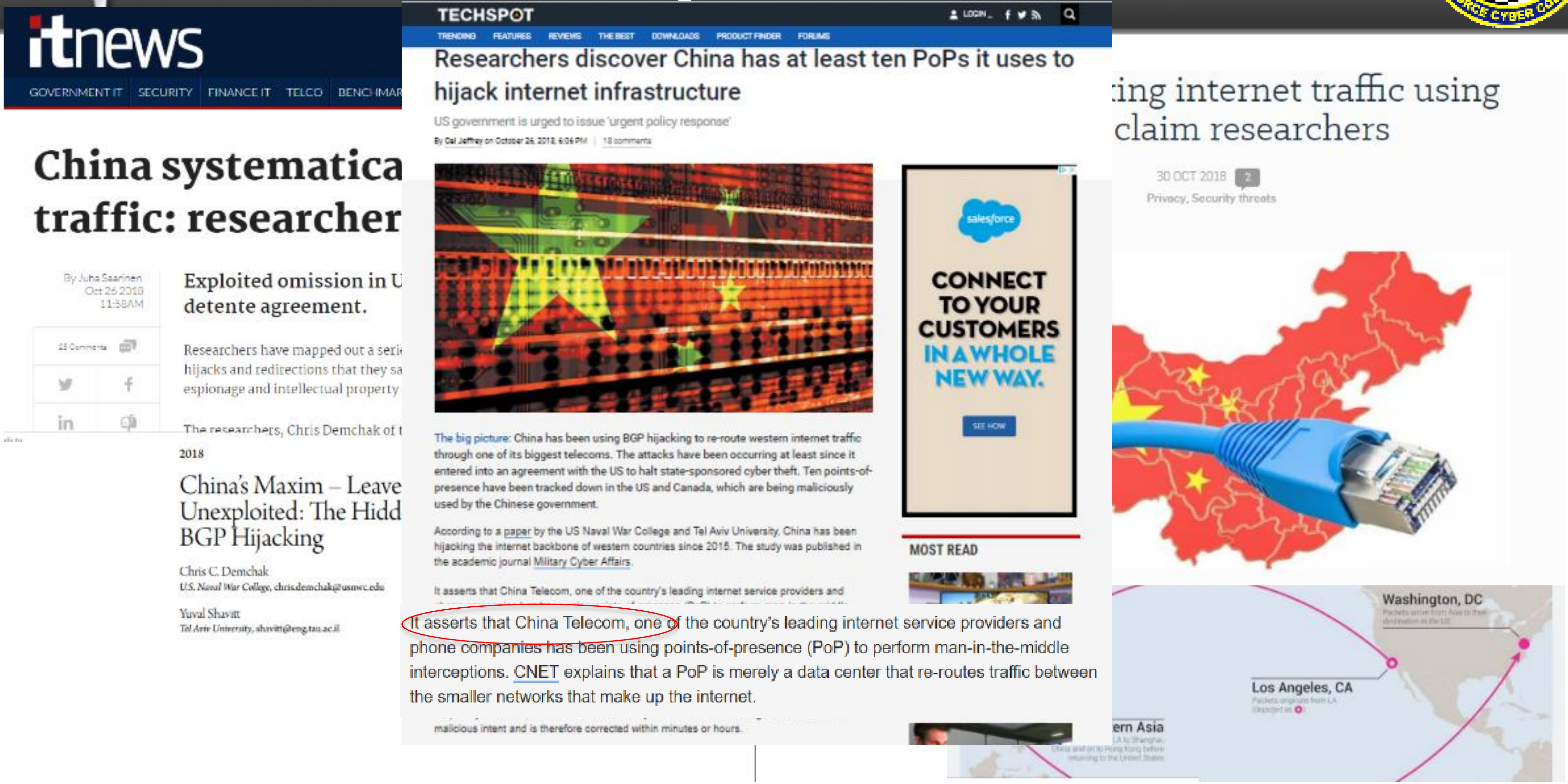
Dark Mode ☐

Chat with us

China Telecom PoP Evaluation Process

- Reviewed Nov 2018 Paper
- Located Suspected NSA Listening Posts on Canadian website
- Google China Telecom US Office Locations
- Review on Google Maps Proximity
- Conclusions?

China Hijacks Internet



itnews

GOVERNMENT IT | SECURITY | FINANCE IT | TELCO | BENCHMAR

China systematica traffic: researcher

By Juha Saarinen
Oct 26 2018
11:58AM

25 Comments

Exploited omission in U detente agreement.

Researchers have mapped out a seri hijacks and redirections that they sa espionage and intellectual property

The researchers, Chris Demchak of t

2018

China's Maxim – Leave Unexploited: The Hidd BGP Hijacking

Chris C. Demchak
U.S. Naval War College, chris.demchak@usnwc.edu

Yuval Shavitt
Tel Aviv University, shavitt@eng.tau.ac.il

TECHSPOT

LOGIN

TRENDING | FEATURES | REVIEWS | THE BEST | DOWNLOADS | PRODUCT FINDER | FORUMS

Researchers discover China has at least ten PoPs it uses to hijack internet infrastructure

US government is urged to issue 'urgent policy response'

By Cal Jeffrey on October 26, 2018, 6:06 PM | 18 comments

The big picture: China has been using BGP hijacking to re-route western internet traffic through one of its biggest telecoms. The attacks have been occurring at least since it entered into an agreement with the US to halt state-sponsored cyber theft. Ten points-of-presence have been tracked down in the US and Canada, which are being maliciously used by the Chinese government.

According to a paper by the US Naval War College and Tel Aviv University, China has been hijacking the internet backbone of western countries since 2015. The study was published in the academic journal Military Cyber Affairs.

It asserts that China Telecom, one of the country's leading internet service providers and

It asserts that China Telecom, one of the country's leading internet service providers and phone companies has been using points-of-presence (PoP) to perform man-in-the-middle interceptions. CNET explains that a PoP is merely a data center that re-routes traffic between the smaller networks that make up the internet.

malicious intent and is therefore corrected within minutes or hours.

MOST READ

ing internet traffic using claim researchers

30 OCT 2018 2

Privacy, Security threats

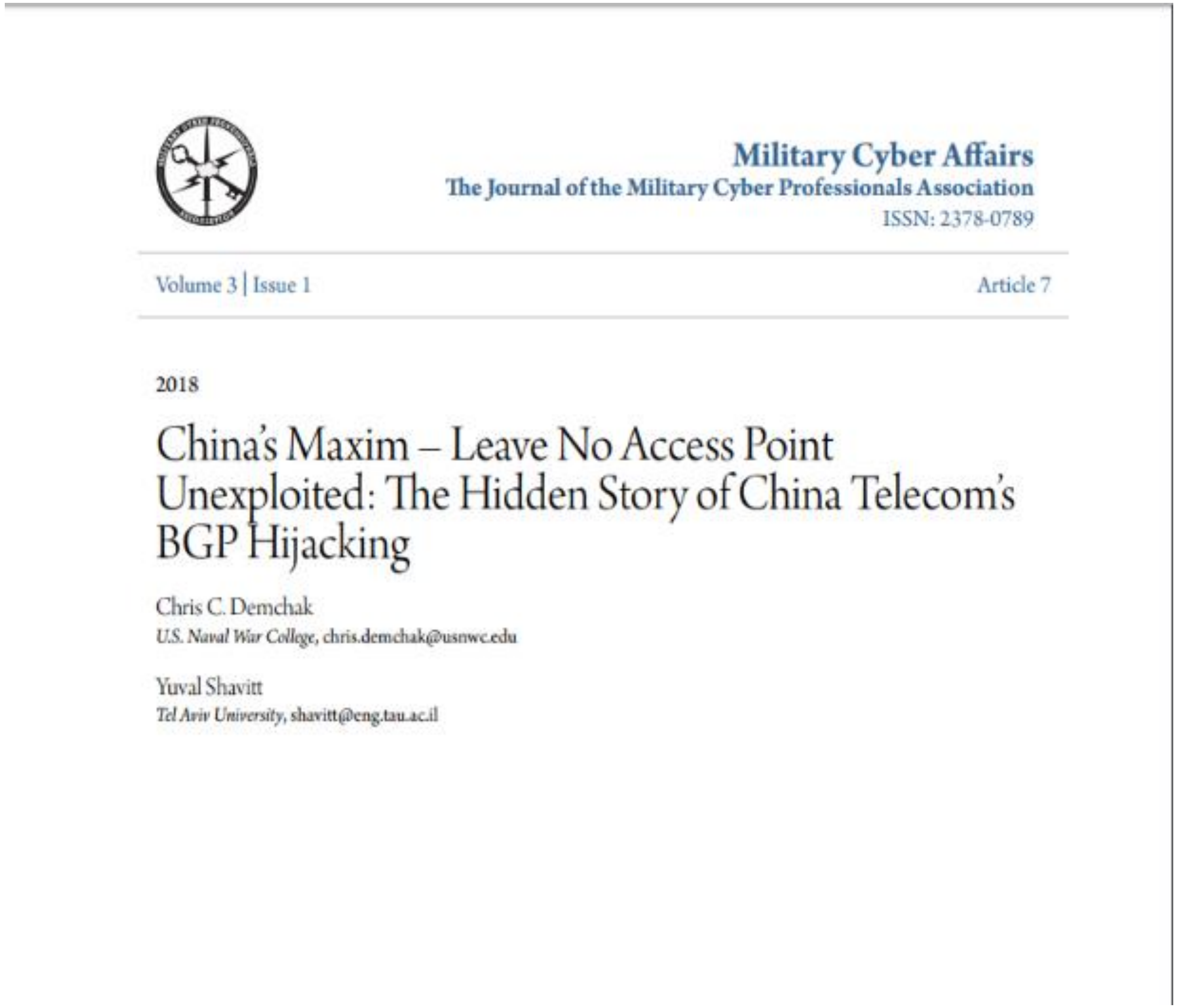
Washington, DC
Packets arrive from Asia to their destination in the US
Los Angeles, CA
Packets originate from LA (depicted as ○)
tern Asia
LA to Shanghai, and on to Hong Kong before returning to the United States

China Hijacks Internet

- “Starting from February 2016 and for about 6 months, routes from Canada to Korean government sites were hijacked by China Telecom and routed through China.”

- “On October 2016, traffic from several locations in the USA to a large Anglo-American bank headquarters in Milan, Italy was hijacked by China Telecom to China.”

- “Traffic from Sweden and Norway to the Japanese network of a large American news organization was hijacked to China for about 6 weeks in April/May 2017.”



Military Cyber Affairs
The Journal of the Military Cyber Professionals Association
ISSN: 2378-0789

Volume 3 | Issue 1 Article 7

2018

China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking

Chris C. Demchak
U.S. Naval War College, chris.demchak@usnwc.edu

Yuval Shavitt
Tel Aviv University, shavitt@eng.tau.ac.il

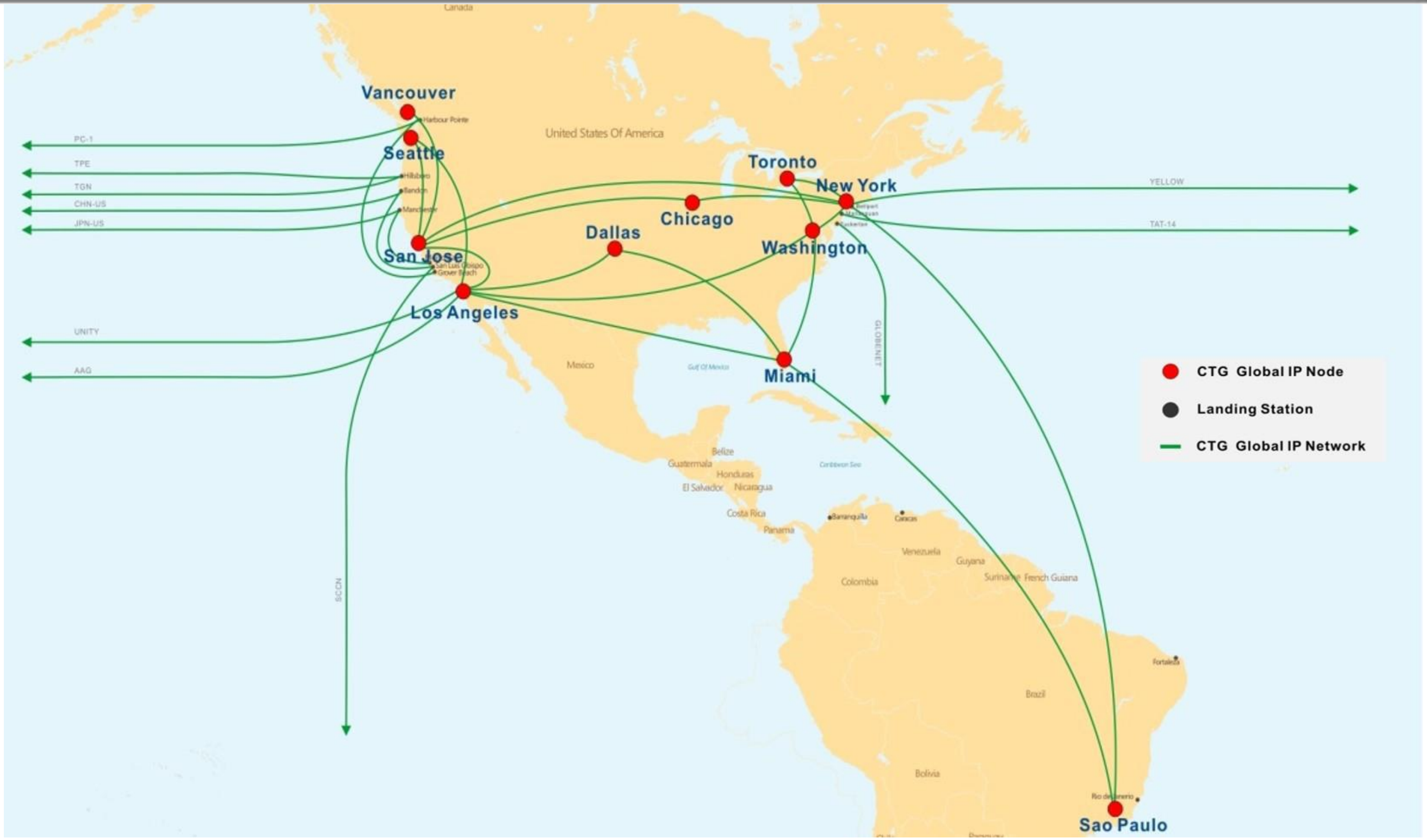
Border Gateway Protocol (BGP) Hijacks

- Geography has not been “defeated” by the global cyberspace; no “death of distance”. Proximity still extremely important.
  - The closer a network is to the attacker or its complicit ISP, the more likely an attack will succeed because defending administrators are less likely to have enough time to detect, analyze, and mitigate the attack.
- In 2008, Pakistan Telecom (Tier 1 AS for Pakistan) hijacked all YouTube traffic for several hours as administrators made mistakes in using routing to censor a clip considered non-Islamic.
- In 2010, China Telecom hijacked 15% of the global Internet traffic for 18 minutes.
  - *Accident, experiment or demonstration?*
- *In Nov2018 Internet traffic rerouted thru RU and PRC for 2 hours.*

Chinese Points of Presence (PoP) in Western Hemisphere

Chinese PoPs

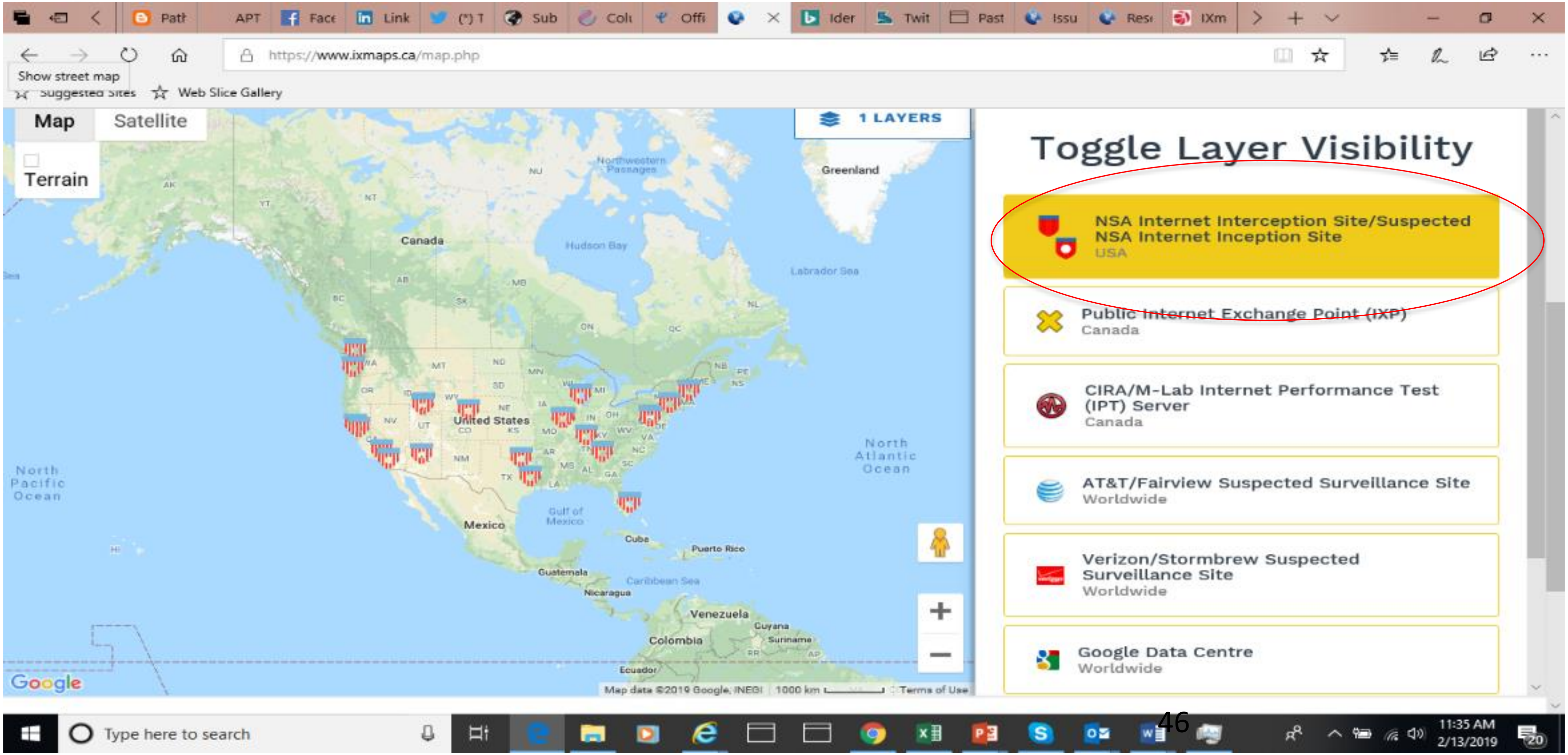
- Bypasses 2015 Xi-Obama agreement on military units hacking US
  - Located near major subsea cables landfalls
  - Located major US & Canadian exchange points
- Capable of highjacking network traffic with minimal detection
  - Patterns of traffic can be revealed in traceroute research
- ***No US PoPs in China***
  - Recommend an *'Access Reciprocity'* policy for the west
- Major Chinese exchange points in Beijing, Shanghai, and Hong Kong (3)



(image taken from the CT web site)

A 'point-of-presence' (PoP) is a major point of connection where a long-distance telecommunications carrier such as Verizon or British Telecom connects to a local network and picks up the local traffic – or transit traffic – to move it onwards towards its various destinations.

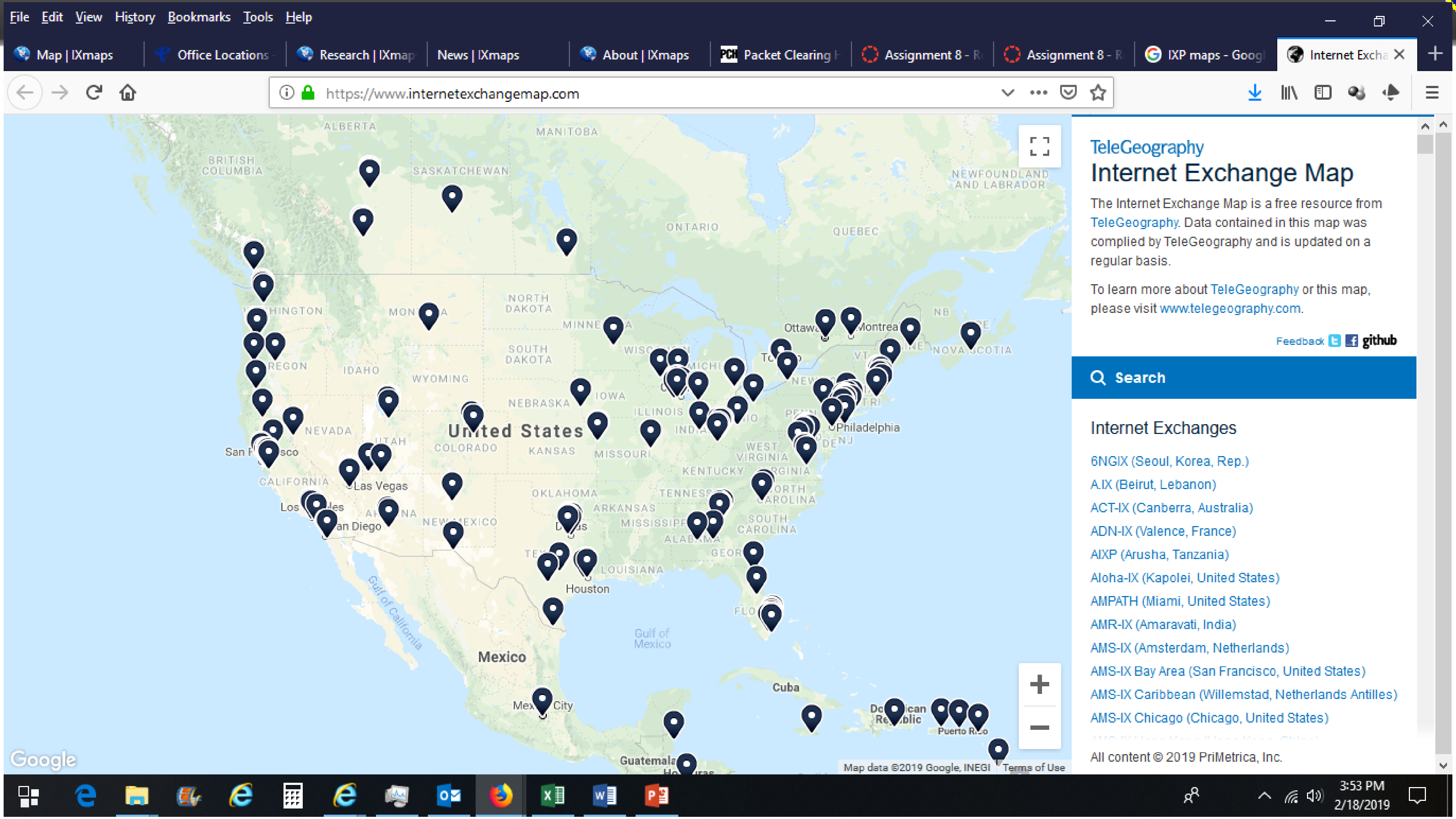
Canadian Site Maps
NSA Listening Posts



Toggle Layer Visibility

- NSA Internet Interception Site/Suspected NSA Internet Inception Site
  USA
- Public Internet Exchange Point (IXP)
  Canada
- CIRA/M-Lab Internet Performance Test (IPT) Server
  Canada
- AT&T/Fairview Suspected Surveillance Site
  Worldwide
- Verizon/Stormbrew Suspected Surveillance Site
  Worldwide
- Google Data Centre
  Worldwide

Worldwide Map of IXPs



TeleGeography

Internet Exchange Map

The Internet Exchange Map is a free resource from TeleGeography. Data contained in this map was complied by TeleGeography and is updated on a regular basis.

To learn more about TeleGeography or this map, please visit www.telegeography.com.

Feedback github

Search

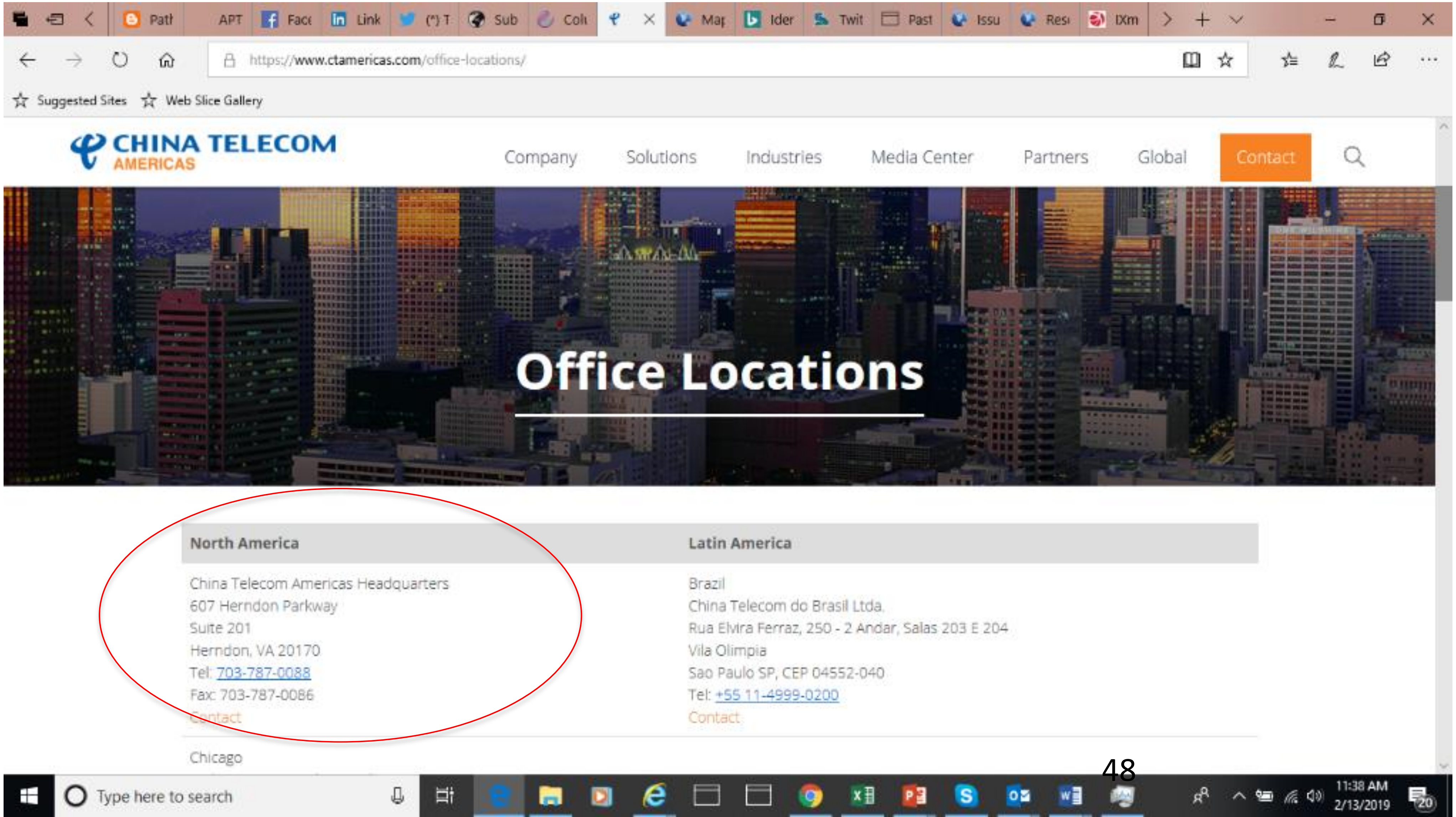
Internet Exchanges

- 6NGIX (Seoul, Korea, Rep.)
- A.IX (Beirut, Lebanon)
- ACT-IX (Canberra, Australia)
- ADN-IX (Valence, France)
- AIXP (Arusha, Tanzania)
- Aloha-IX (Kapolei, United States)
- AMPATH (Miami, United States)
- AMR-IX (Amaravati, India)
- AMS-IX (Amsterdam, Netherlands)
- AMS-IX Bay Area (San Francisco, United States)
- AMS-IX Caribbean (Willemstad, Netherlands Antilles)
- AMS-IX Chicago (Chicago, United States)

All content © 2019 PriMetrica, Inc.

https://www.internetexchangemap.com/

China Telecom on Google

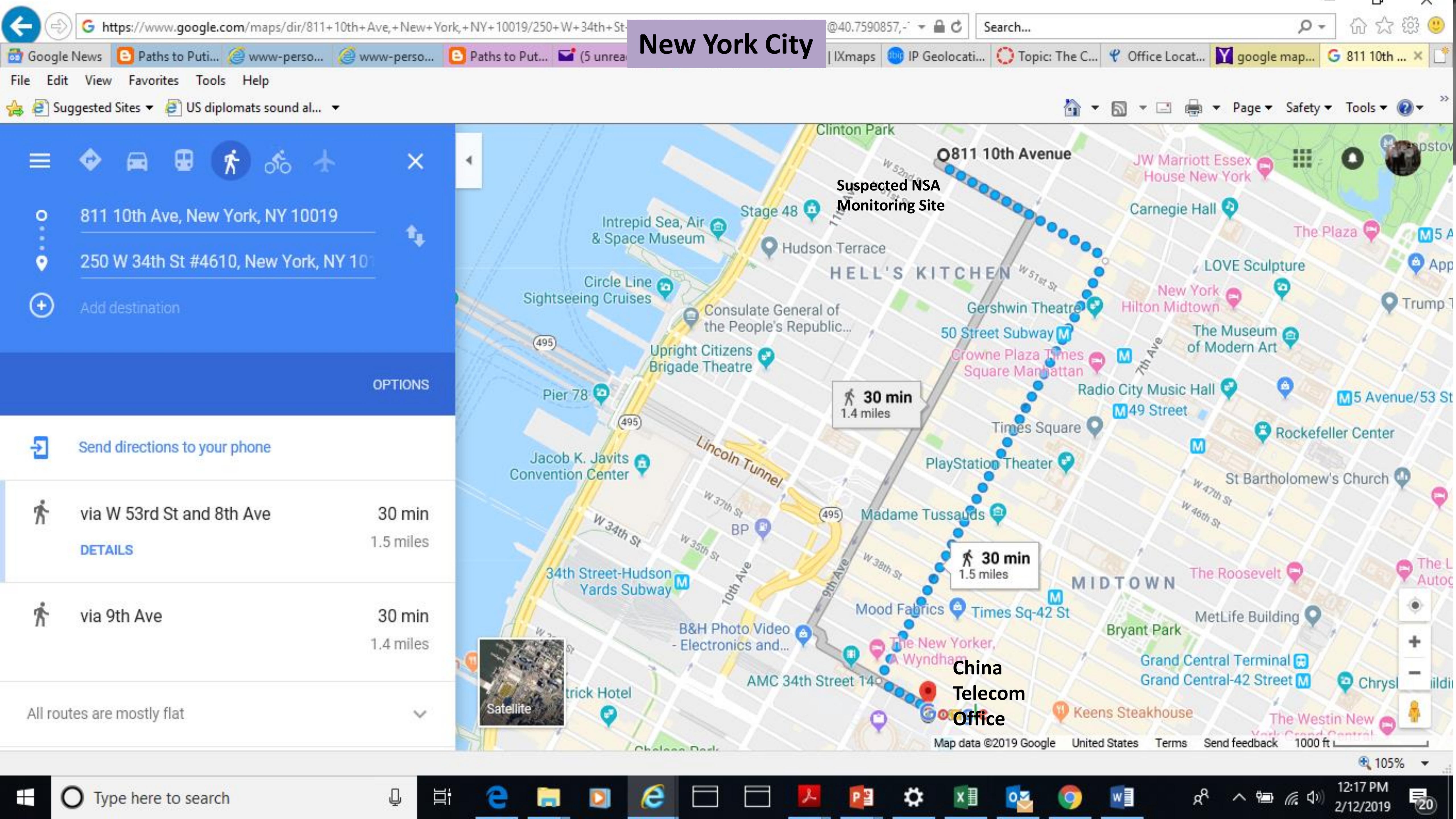


Office Locations

North America	Latin America
China Telecom Americas Headquarters 607 Herndon Parkway Suite 201 Herndon, VA 20170 Tel: 703-787-0088 Fax: 703-787-0086 Contact	Brazil China Telecom do Brasil Ltda. Rua Elvira Ferraz, 250 - 2 Andar, Salas 203 E 204 Vila Olimpia Sao Paulo SP, CEP 04552-040 Tel: +55 11-4999-0200 Contact

Chicago

New York City



https://www.google.com/maps/dir/811+10th+Ave,+New+York,+NY+10019/250+W+34th+St-

811 10th Ave, New York, NY 10019

250 W 34th St #4610, New York, NY 10

Add destination

OPTIONS

Send directions to your phone

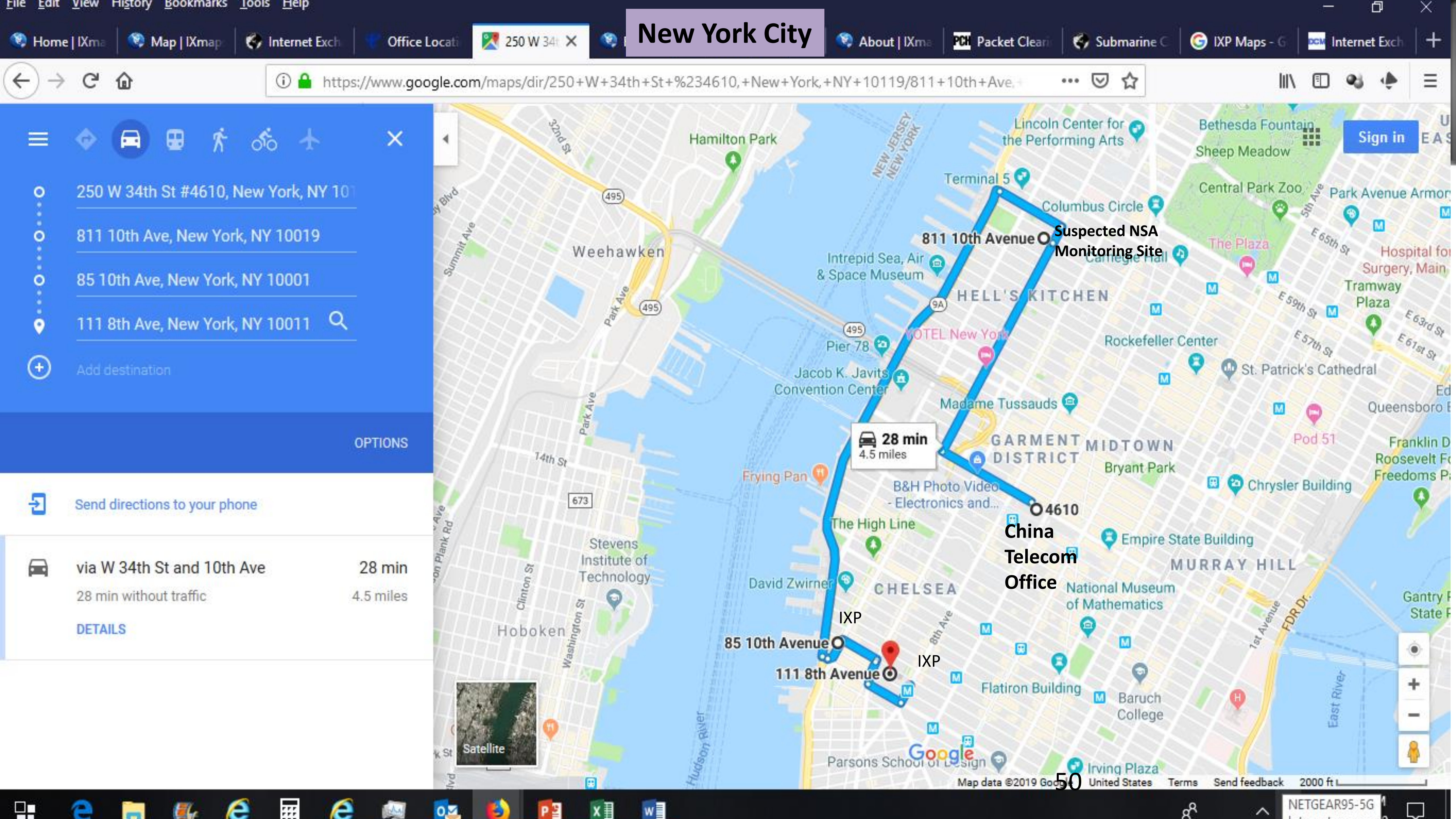
via W 53rd St and 8th Ave DETAILS	30 min 1.5 miles
via 9th Ave	30 min 1.4 miles

All routes are mostly flat

Suspected NSA Monitoring Site

China Telecom Office

New York City



https://www.google.com/maps/dir/250+W+34th+St+%234610,+New+York,+NY+10119/811+10th+Ave,

250 W 34th St #4610, New York, NY 10

811 10th Ave, New York, NY 10019

85 10th Ave, New York, NY 10001

111 8th Ave, New York, NY 10011

Add destination

OPTIONS

Send directions to your phone

via W 34th St and 10th Ave — 28 min

28 min without traffic — 4.5 miles

DETAILS

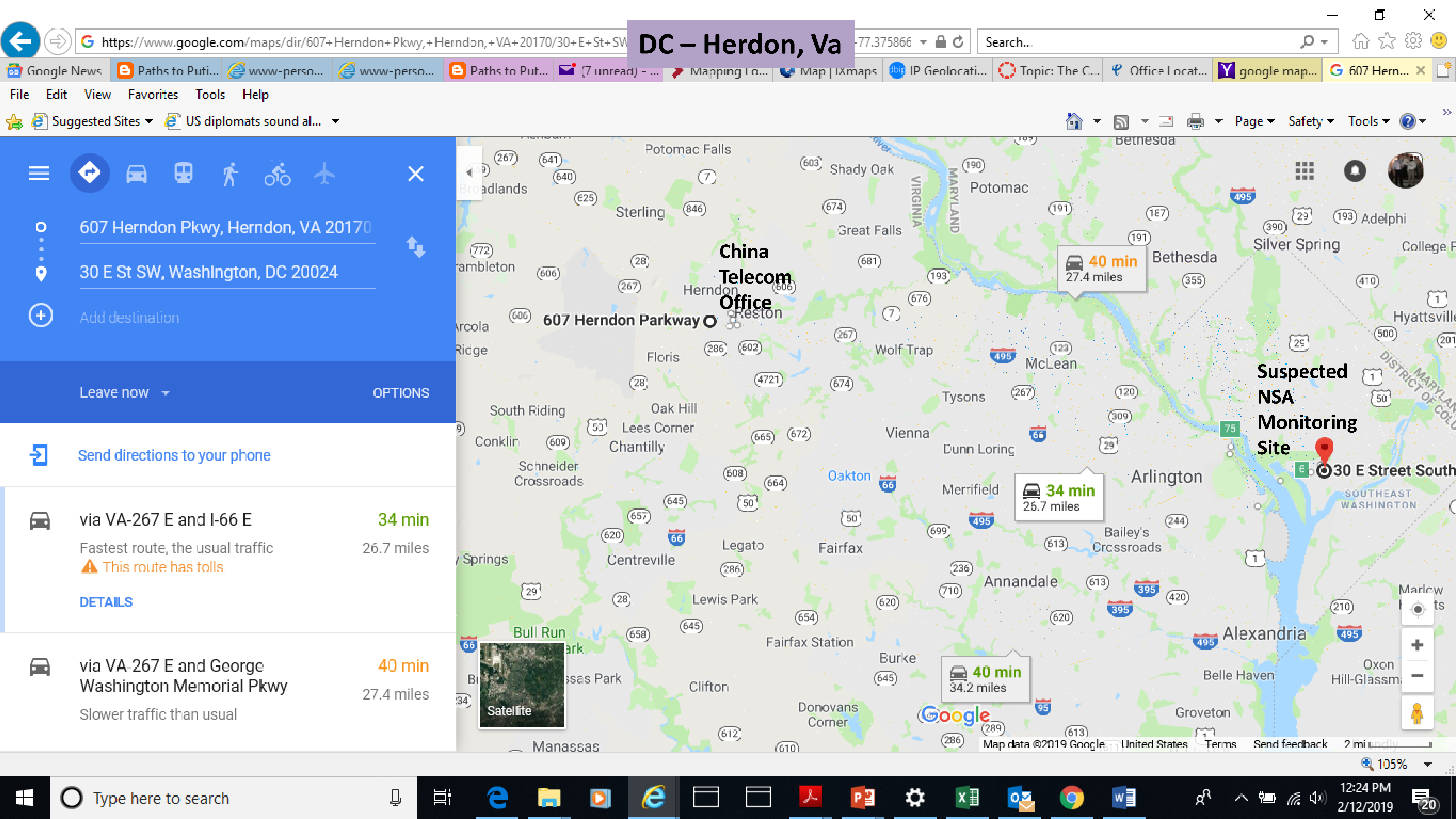
Suspected NSA Monitoring Site

China Telecom Office

IXP

IXP

DC – Herdon, Va



https://www.google.com/maps/dir/607+Herndon+Pkwy,+Herndon,+VA+20170/30+E+St+SW ... 77.375866

607 Herndon Pkwy, Herndon, VA 20170

30 E St SW, Washington, DC 20024

Add destination

Leave now OPTIONS

Send directions to your phone

via VA-267 E and I-66 E — 34 min — 26.7 miles

Fastest route, the usual traffic

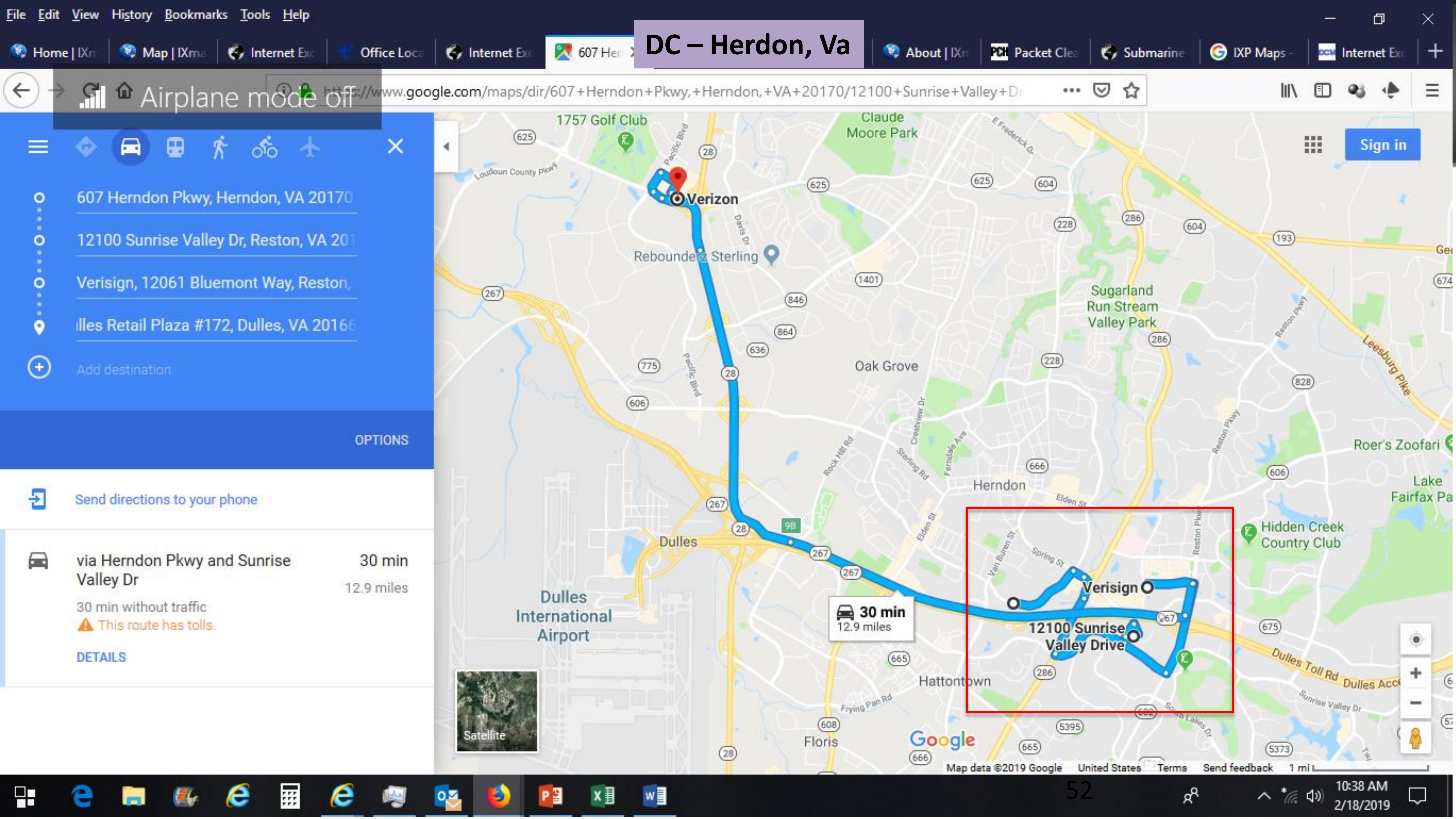
⚠ This route has tolls.

DETAILS

via VA-267 E and George Washington Memorial Pkwy — 40 min — 27.4 miles

Slower traffic than usual

DC – Herdon, Va



607 Herndon Pkwy, Herndon, VA 20170

12100 Sunrise Valley Dr, Reston, VA 201

Verisign, 12061 Bluemont Way, Reston,

lles Retail Plaza #172, Dulles, VA 2016

Add destination

OPTIONS

Send directions to your phone

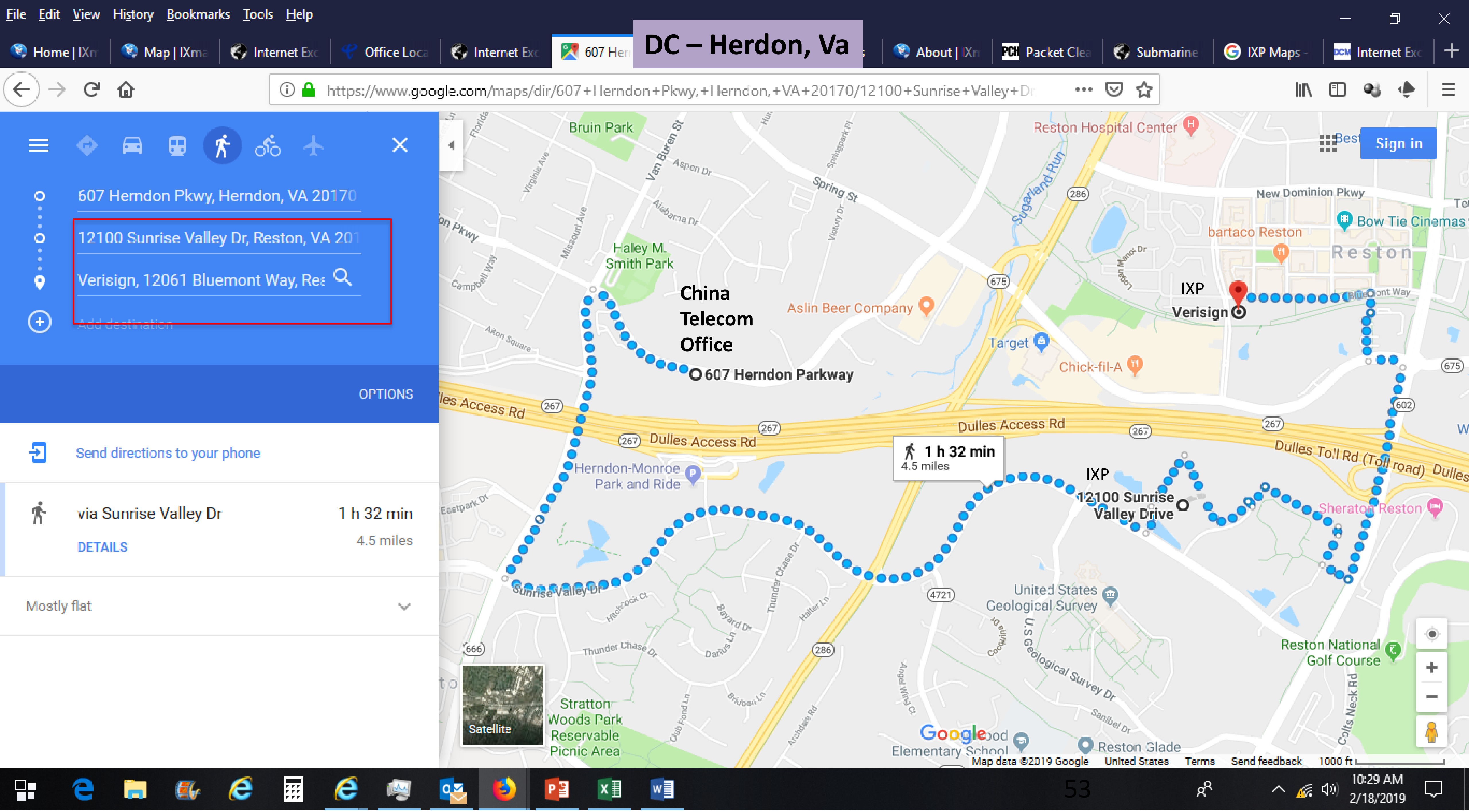
via Herndon Pkwy and Sunrise Valley Dr — 30 min — 12.9 miles

30 min without traffic

⚠ This route has tolls.

DETAILS

DC – Herdon, Va



https://www.google.com/maps/dir/607+Herndon+Pkwy,+Herndon,+VA+20170/12100+Sunrise+Valley+Dr

607 Herndon Pkwy, Herndon, VA 20170

12100 Sunrise Valley Dr, Reston, VA 201

Verisign, 12061 Bluemont Way, Res

Add destination

OPTIONS

Send directions to your phone

via Sunrise Valley Dr 1 h 32 min

4.5 miles

DETAILS

Mostly flat

1 h 32 min

4.5 miles

China Telecom Office

607 Herndon Parkway

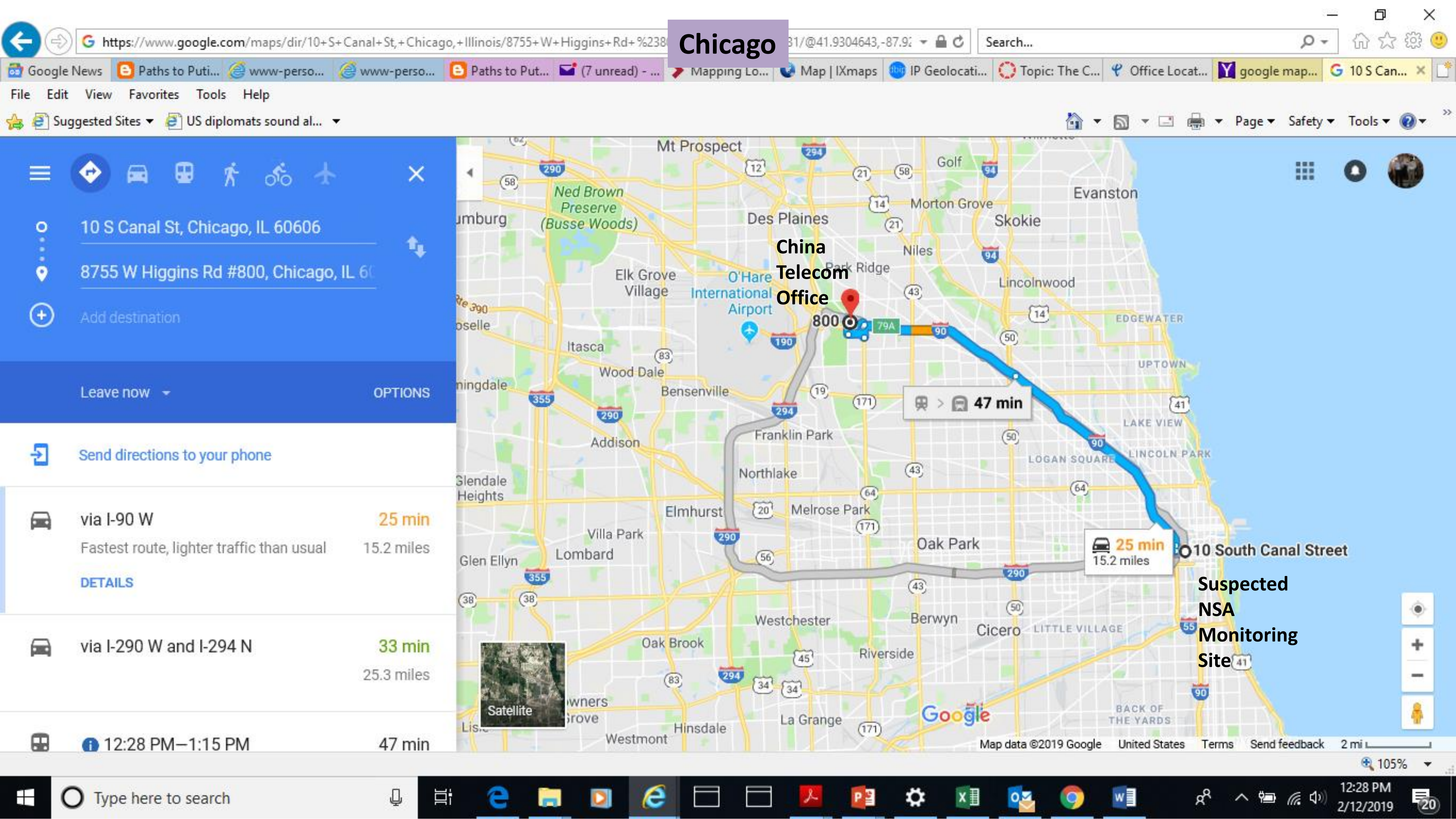
IXP

Verisign

IXP

12100 Sunrise Valley Drive

Chicago



China Telecom Office

Suspected NSA Monitoring Site

https://www.google.com/maps/dir/10+S+Canal+St,+Chicago,+Illinois/8755+W+Higgins+Rd+%238 …31/@41.9304643,-87.9…

10 S Canal St, Chicago, IL 60606

8755 W Higgins Rd #800, Chicago, IL 6…

Add destination

Leave now OPTIONS

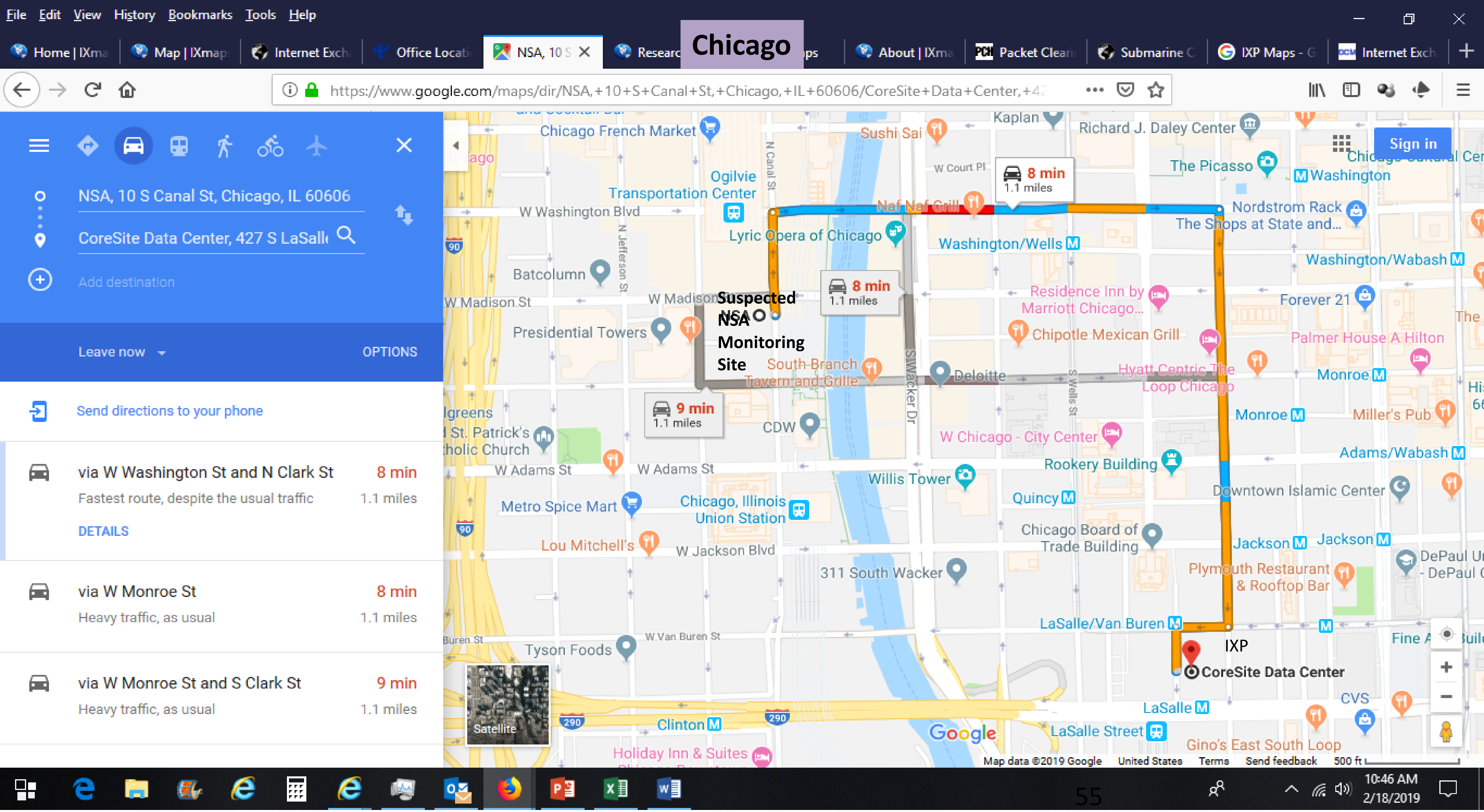
Send directions to your phone

via I-90 W 25 min
Fastest route, lighter traffic than usual 15.2 miles
DETAILS

via I-290 W and I-294 N 33 min
25.3 miles

12:28 PM—1:15 PM 47 min

Chicago



https://www.google.com/maps/dir/NSA,+10+S+Canal+St,+Chicago,+IL+60606/CoreSite+Data+Center,+42

NSA, 10 S Canal St, Chicago, IL 60606

CoreSite Data Center, 427 S LaSalle

Add destination

Leave now

OPTIONS

Send directions to your phone

via W Washington St and N Clark St — 8 min — 1.1 miles
Fastest route, despite the usual traffic
DETAILS

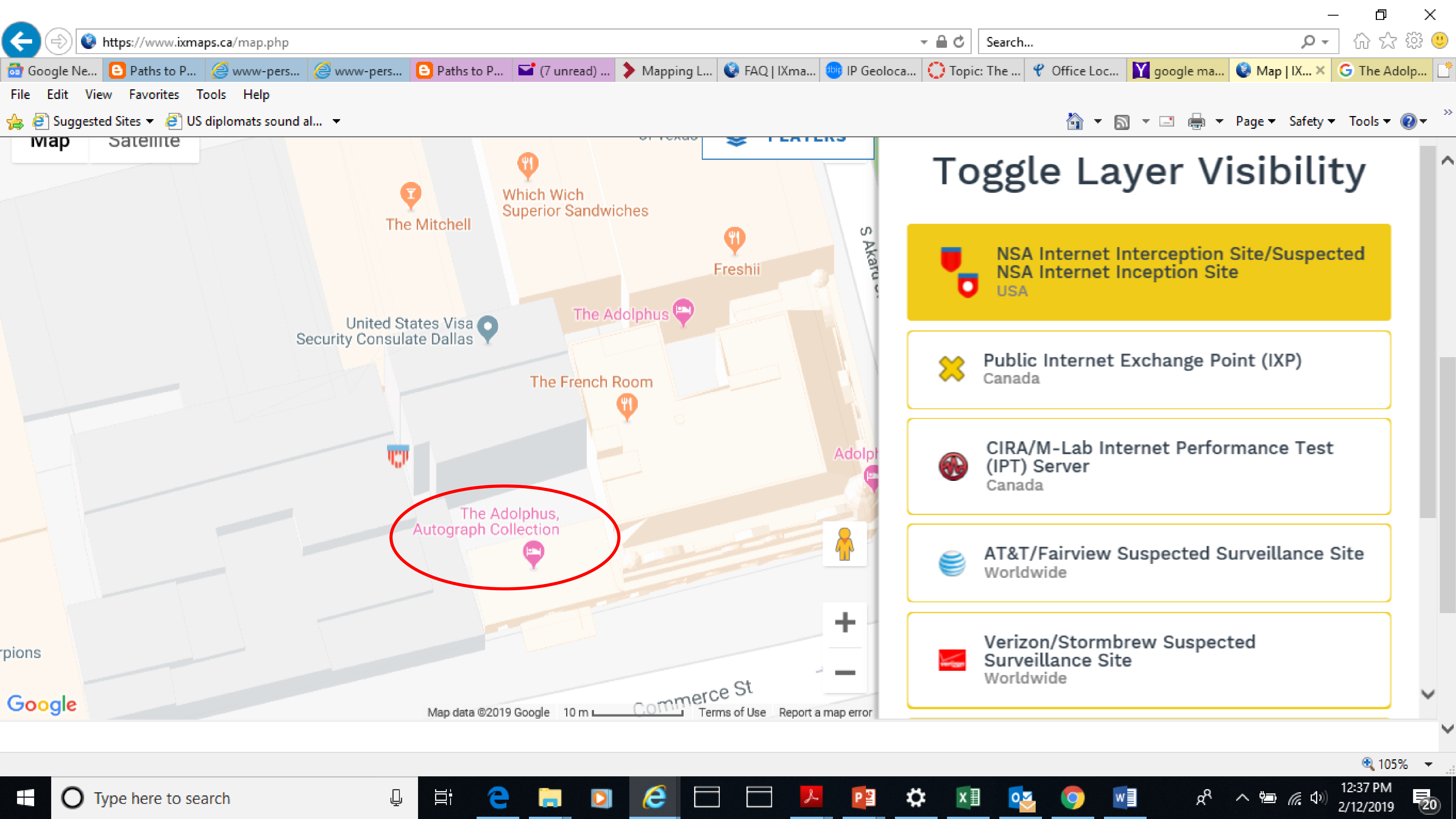
via W Monroe St — 8 min — 1.1 miles
Heavy traffic, as usual

via W Monroe St and S Clark St — 9 min — 1.1 miles
Heavy traffic, as usual

Suspected NSA Monitoring Site

IXP

CoreSite Data Center



Toggle Layer Visibility

NSA Internet Interception Site/Suspected NSA Internet Inception Site
USA

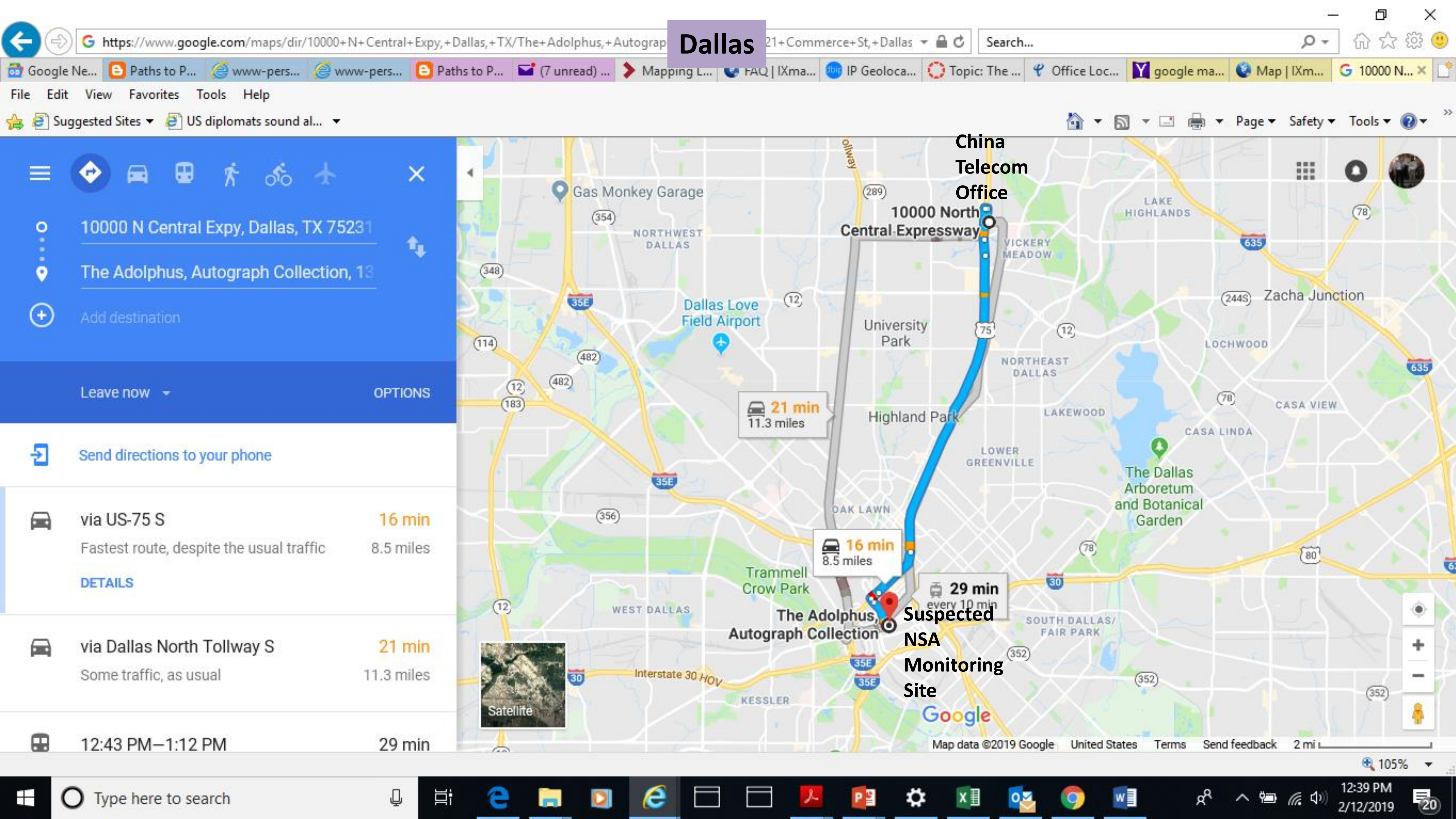
Public Internet Exchange Point (IXP)
Canada

CIRA/M-Lab Internet Performance Test (IPT) Server
Canada

AT&T/Fairview Suspected Surveillance Site
Worldwide

Verizon/Stormbrew Suspected Surveillance Site
Worldwide

Dallas



https://www.google.com/maps/dir/10000+N+Central+Expy,+Dallas,+TX/The+Adolphus,+Autograp 21+Commerce+St,+Dallas

10000 N Central Expy, Dallas, TX 75231

The Adolphus, Autograph Collection, 13

Add destination

Leave now OPTIONS

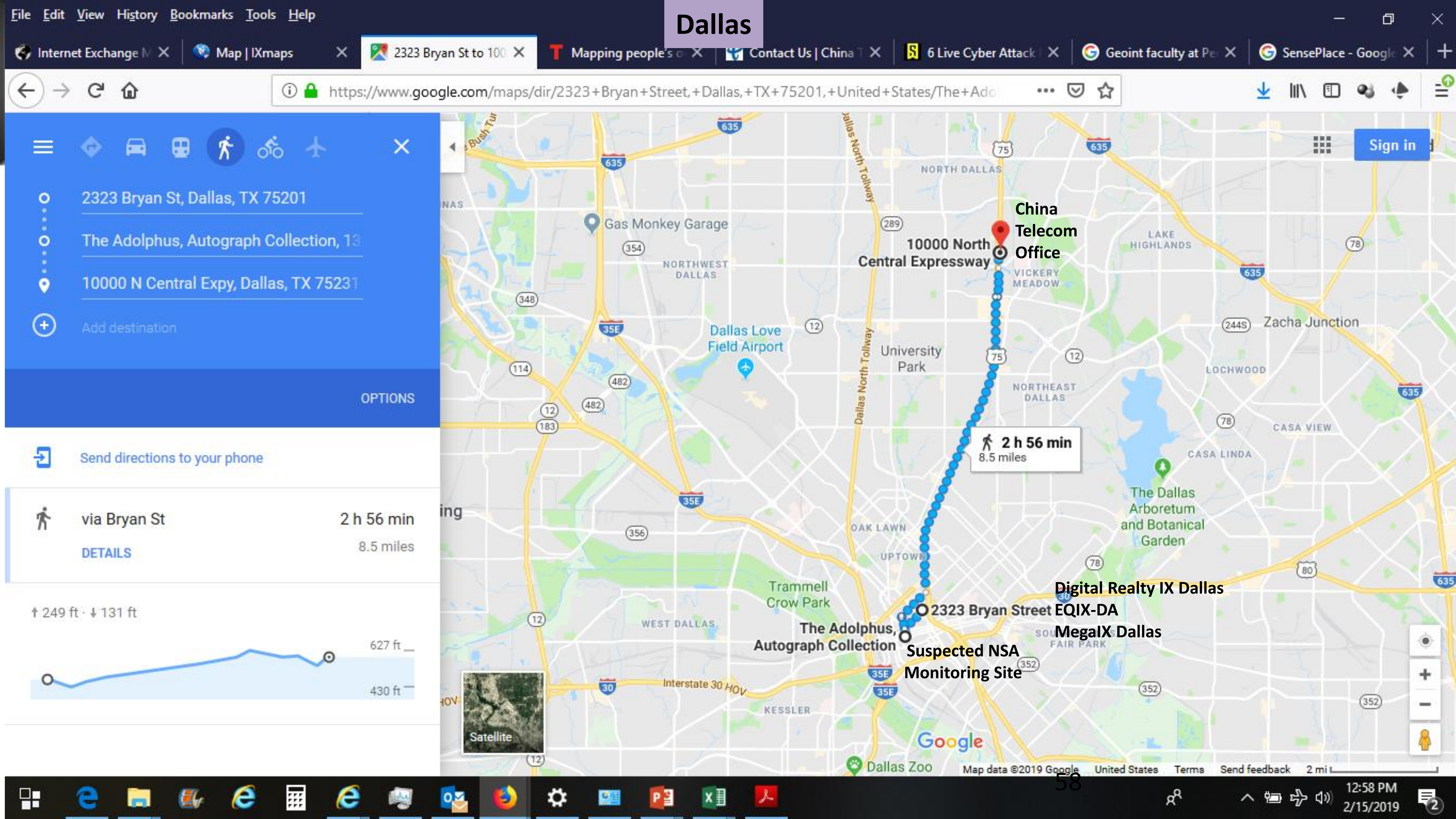
Send directions to your phone

via US-75 S	16 min	
Fastest route, despite the usual traffic	8.5 miles	
DETAILS		
via Dallas North Tollway S	21 min	
Some traffic, as usual	11.3 miles	
12:43 PM—1:12 PM	29 min	

China Telecom Office

Suspected NSA Monitoring Site

Dallas



https://www.google.com/maps/dir/2323+Bryan+Street,+Dallas,+TX+75201,+United+States/The+Ado

2323 Bryan St, Dallas, TX 75201

The Adolphus, Autograph Collection, 13

10000 N Central Expy, Dallas, TX 75231

Add destination

OPTIONS

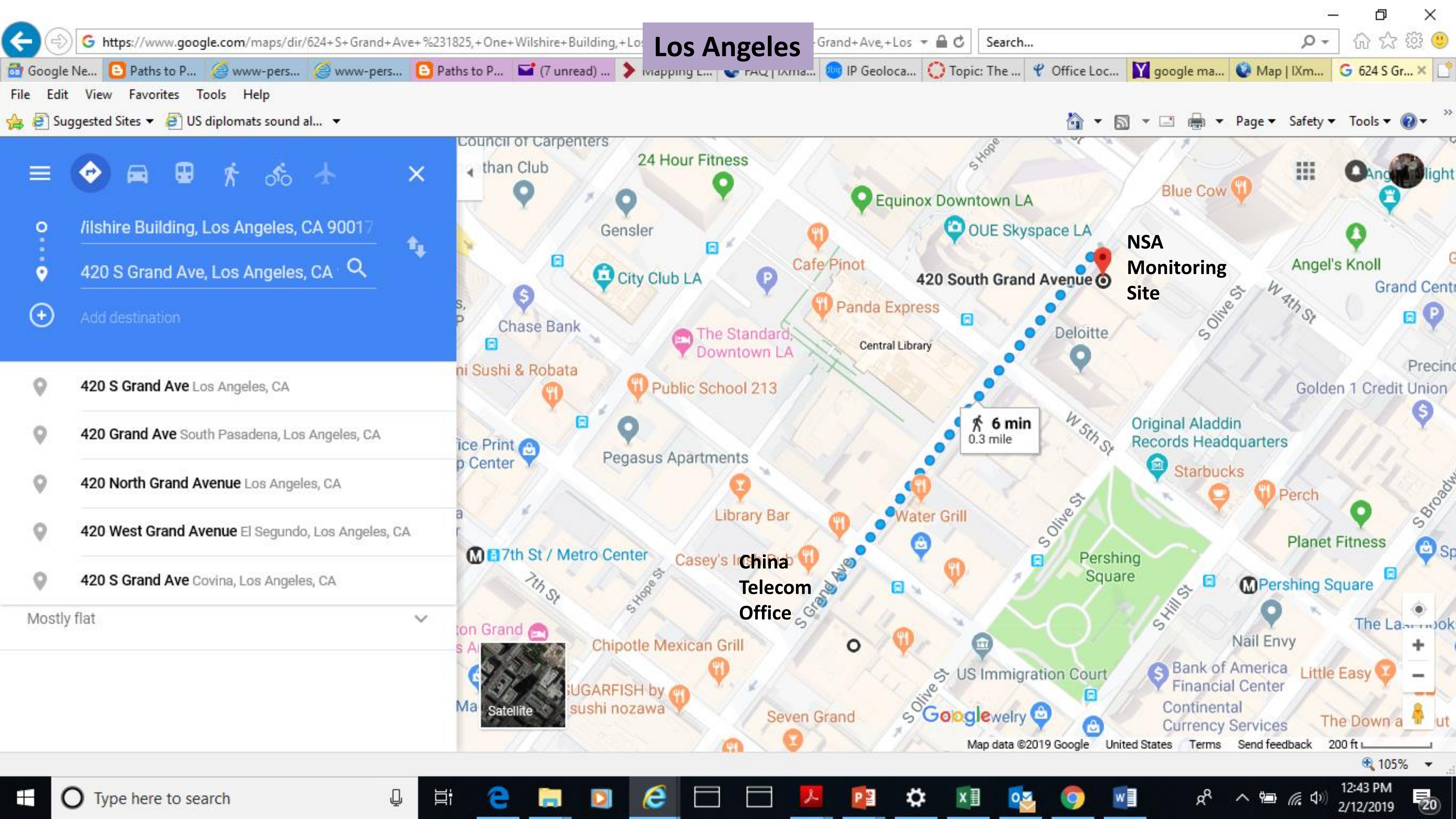
Send directions to your phone

via Bryan St — 2 h 56 min — 8.5 miles

DETAILS

↑ 249 ft · ↓ 131 ft

Los Angeles



https://www.google.com/maps/dir/624+S+Grand+Ave+%231825,+One+Wilshire+Building,+Los ... Grand+Ave,+Los

/ilshire Building, Los Angeles, CA 90017

420 S Grand Ave, Los Angeles, CA

Add destination

420 S Grand Ave Los Angeles, CA

420 Grand Ave South Pasadena, Los Angeles, CA

420 North Grand Avenue Los Angeles, CA

420 West Grand Avenue El Segundo, Los Angeles, CA

420 S Grand Ave Covina, Los Angeles, CA

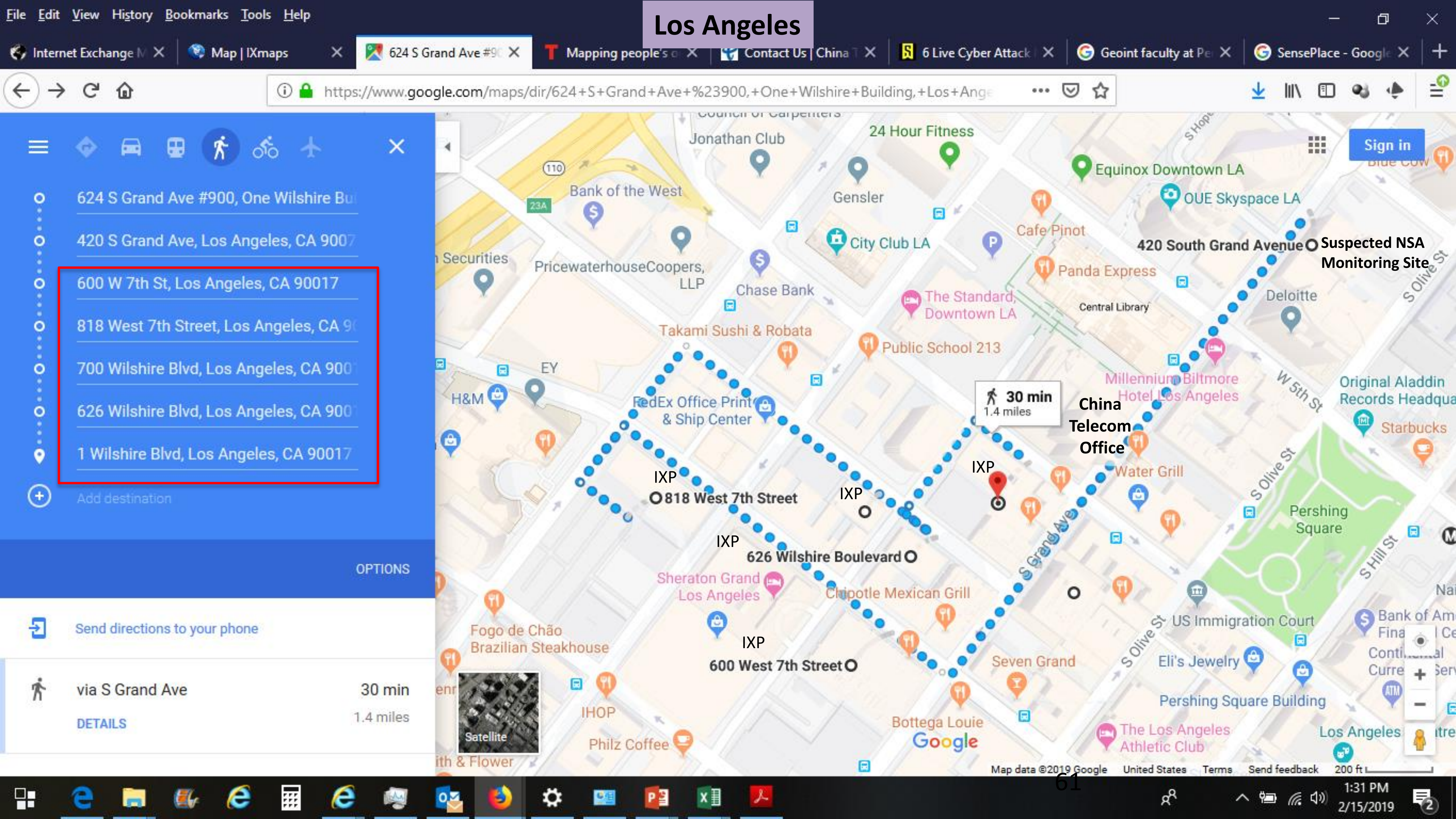
Mostly flat

6 min
0.3 mile

NSA Monitoring Site

China Telecom Office

Los Angeles



https://www.google.com/maps/dir/624+S+Grand+Ave+%23900,+One+Wilshire+Building,+Los+Ange

624 S Grand Ave #900, One Wilshire Bu

420 S Grand Ave, Los Angeles, CA 9007

600 W 7th St, Los Angeles, CA 90017

818 West 7th Street, Los Angeles, CA 9

700 Wilshire Blvd, Los Angeles, CA 900

626 Wilshire Blvd, Los Angeles, CA 900

1 Wilshire Blvd, Los Angeles, CA 90017

Add destination

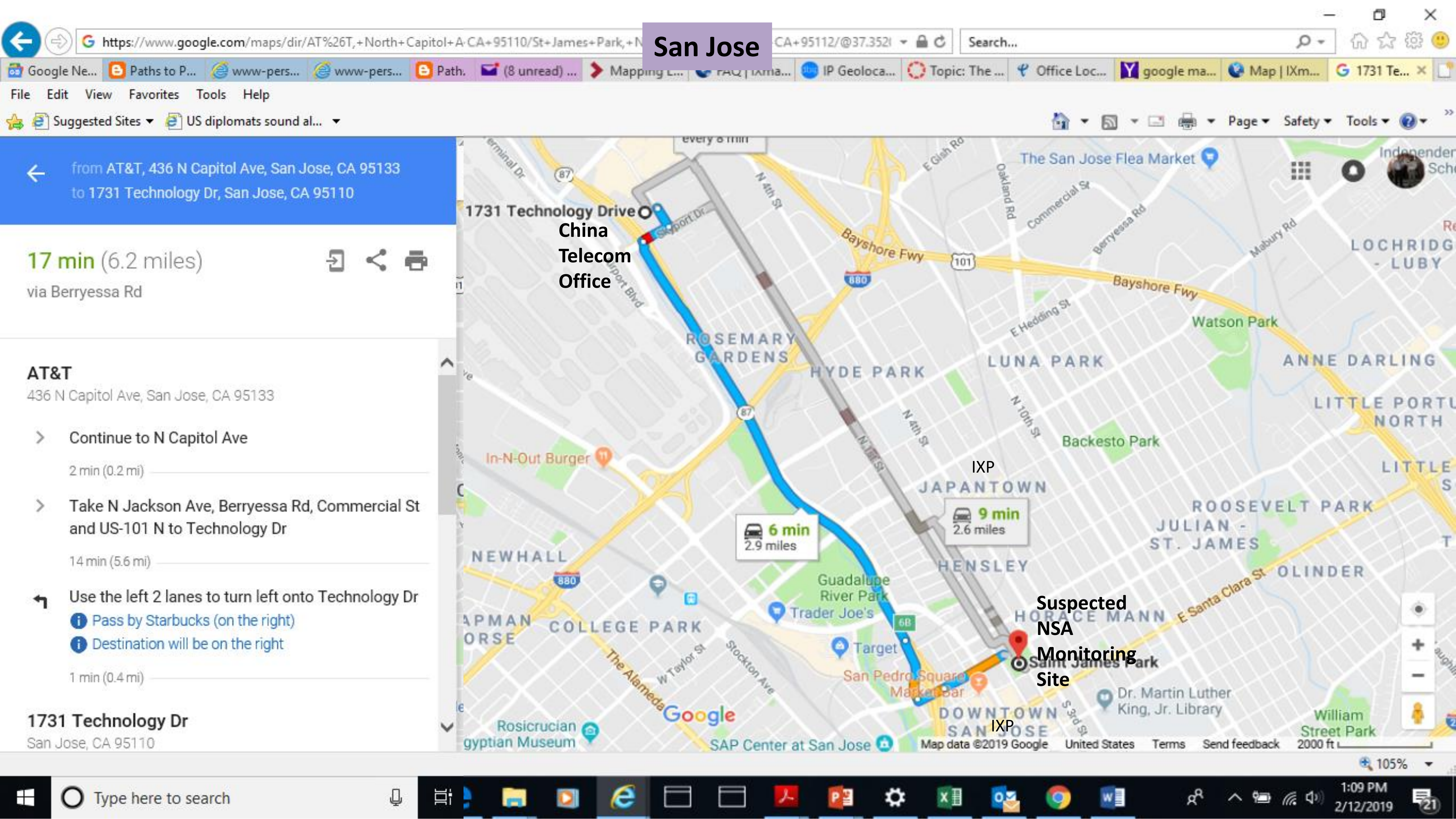
OPTIONS

Send directions to your phone

via S Grand Ave 30 min

DETAILS 1.4 miles

San Jose



from AT&T, 436 N Capitol Ave, San Jose, CA 95133
to 1731 Technology Dr, San Jose, CA 95110

17 min (6.2 miles)
via Berryessa Rd

AT&T
436 N Capitol Ave, San Jose, CA 95133

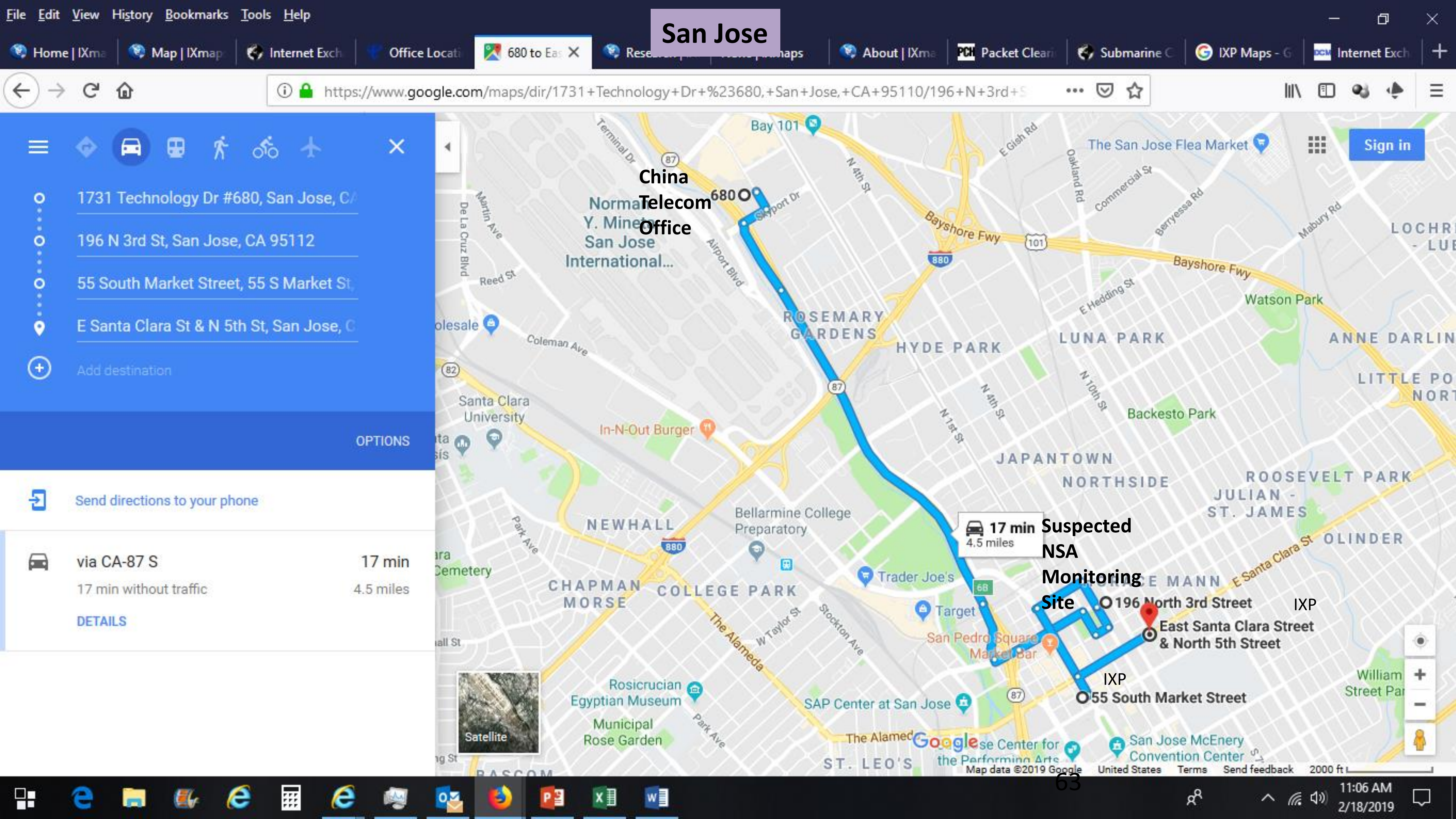
Continue to N Capitol Ave
2 min (0.2 mi)

Take N Jackson Ave, Berryessa Rd, Commercial St and US-101 N to Technology Dr
14 min (5.6 mi)

Use the left 2 lanes to turn left onto Technology Dr
Pass by Starbucks (on the right)
Destination will be on the right
1 min (0.4 mi)

1731 Technology Dr
San Jose, CA 95110

San Jose



https://www.google.com/maps/dir/1731+Technology+Dr+%23680,+San+Jose,+CA+95110/196+N+3rd+S

1731 Technology Dr #680, San Jose, C/

196 N 3rd St, San Jose, CA 95112

55 South Market Street, 55 S Market St,

E Santa Clara St & N 5th St, San Jose, C

Add destination

OPTIONS

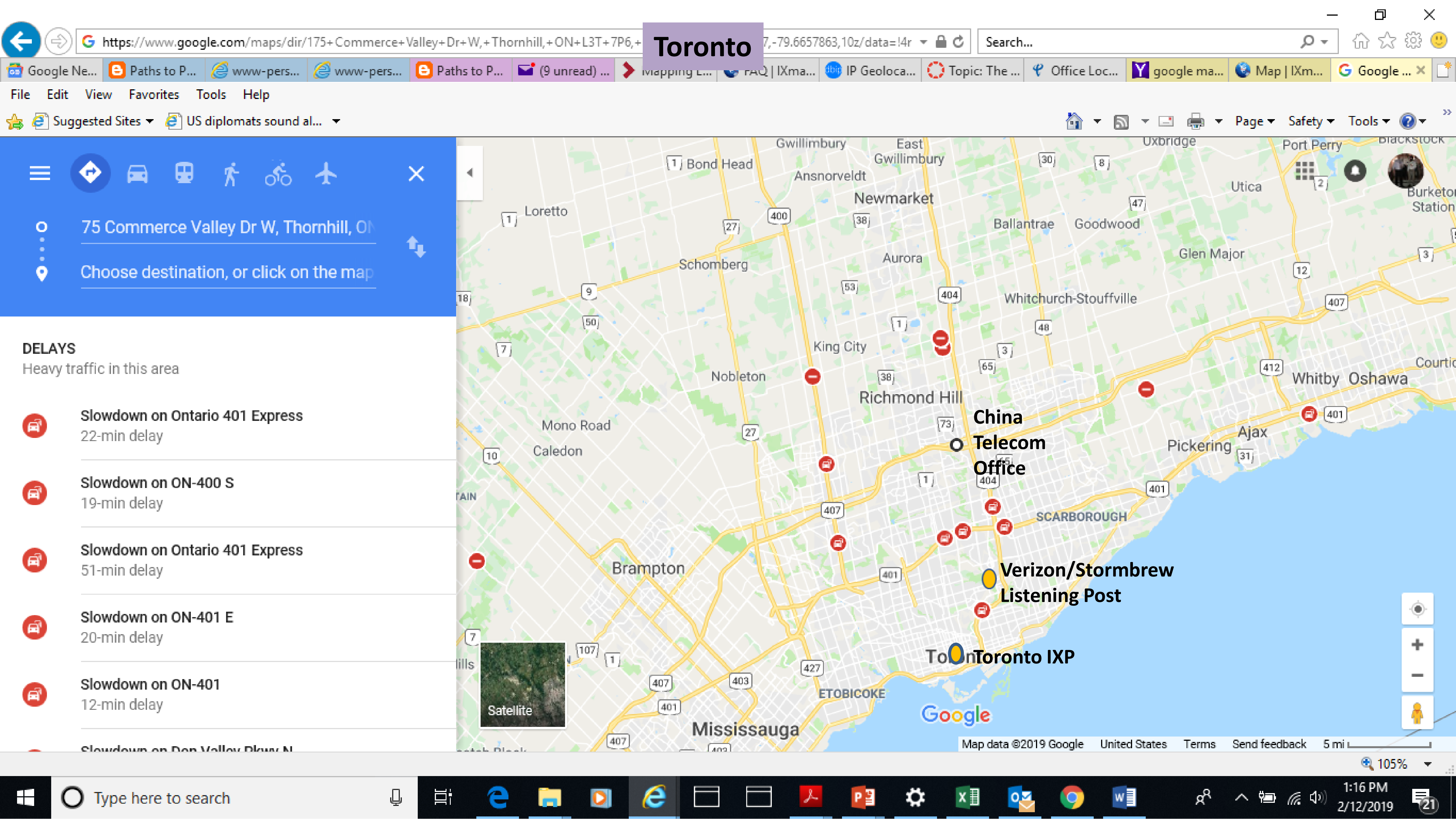
Send directions to your phone

via CA-87 S 17 min

17 min without traffic 4.5 miles

DETAILS

Toronto



https://www.google.com/maps/dir/175+Commerce+Valley+Dr+W,+Thornhill,+ON+L3T+7P6,+…7,-79.6657863,10z/data=!4r

75 Commerce Valley Dr W, Thornhill, ON

Choose destination, or click on the map

DELAYS

Heavy traffic in this area

Slowdown on Ontario 401 Express
22-min delay

Slowdown on ON-400 S
19-min delay

Slowdown on Ontario 401 Express
51-min delay

Slowdown on ON-401 E
20-min delay

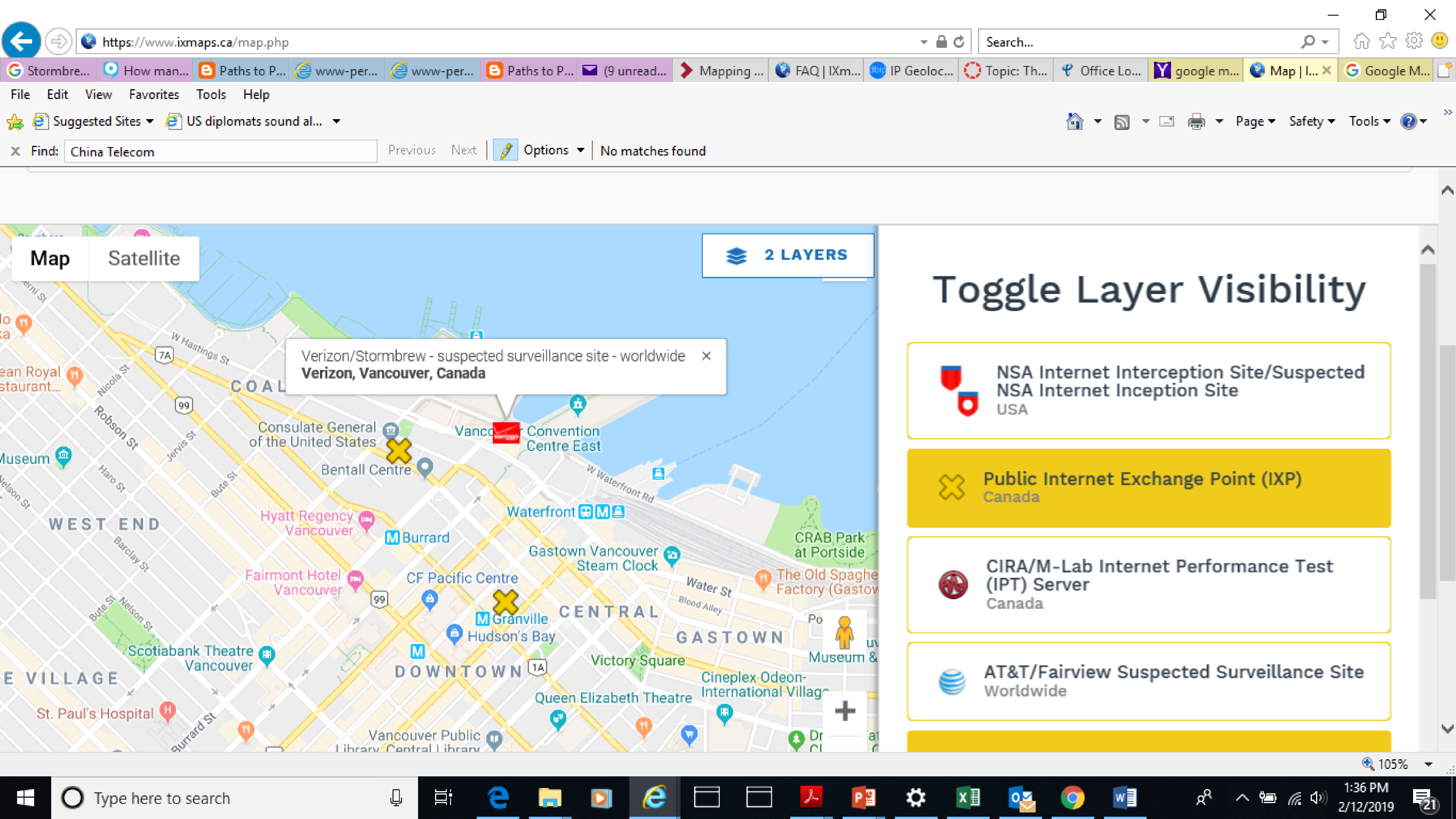
Slowdown on ON-401
12-min delay

Slowdown on Don Valley Pkwy N

China Telecom Office

Verizon/Stormbrew Listening Post

Toronto IXP



Verizon/Stormbrew - suspected surveillance site - worldwide

Verizon, Vancouver, Canada

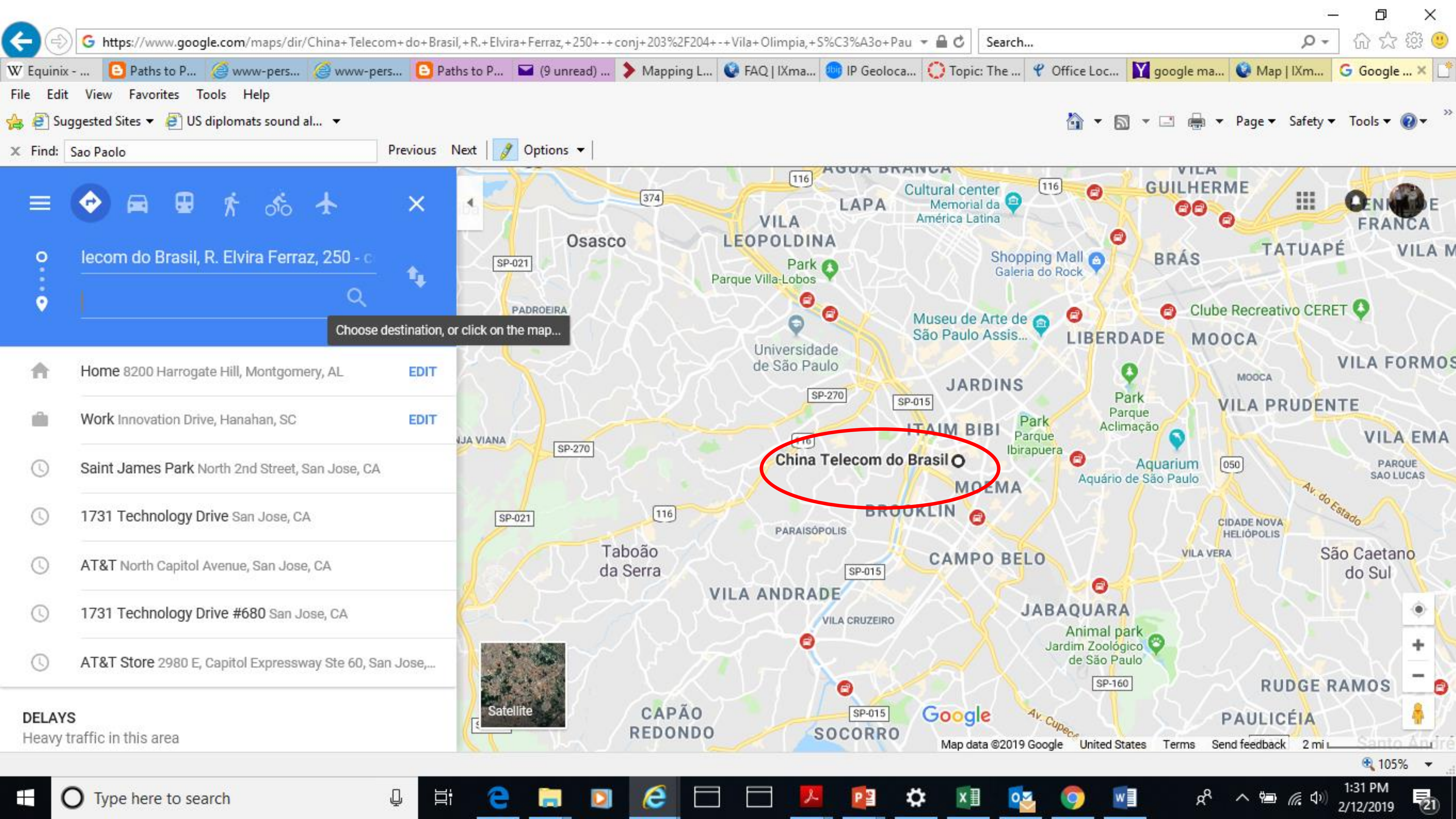
Toggle Layer Visibility

NSA Internet Interception Site/Suspected NSA Internet Inception Site
USA

Public Internet Exchange Point (IXP)
Canada

CIRA/M-Lab Internet Performance Test (IPT) Server
Canada

AT&T/Fairview Suspected Surveillance Site
Worldwide



https://www.google.com/maps/dir/China+Telecom+do+Brasil,+R.+Elvira+Ferraz,+250+-+conj+203%2F204+-+Vila+Olimpia,+S%C3%A3o+Pau

Find: Sao Paolo

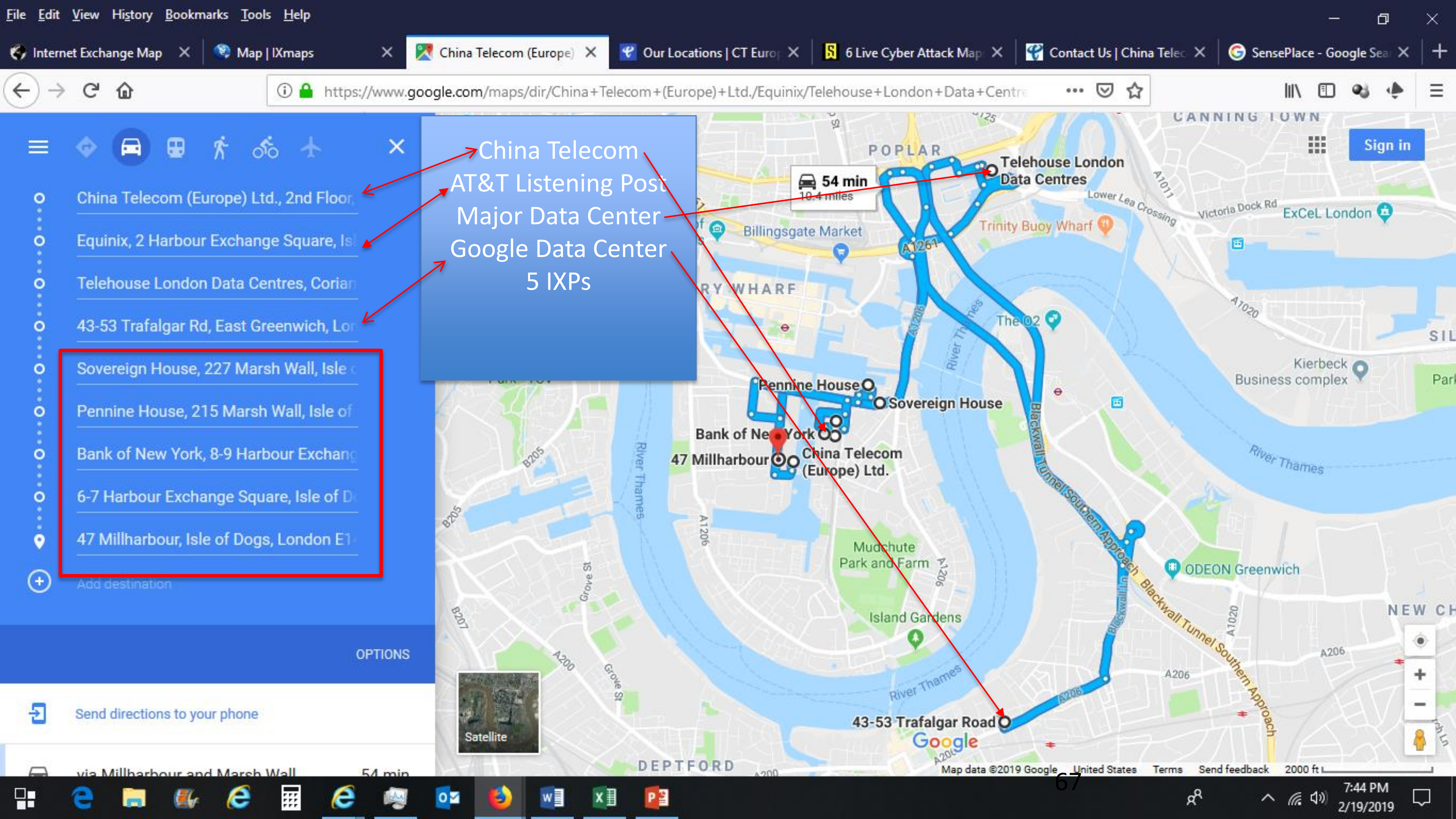
lecom do Brasil, R. Elvira Ferraz, 250 - c

Choose destination, or click on the map...

Home	8200 Harrogate Hill, Montgomery, AL	EDIT
Work	Innovation Drive, Hanahan, SC	EDIT
Saint James Park	North 2nd Street, San Jose, CA	
1731 Technology Drive	San Jose, CA	
AT&T	North Capitol Avenue, San Jose, CA	
1731 Technology Drive #680	San Jose, CA	
AT&T Store	2980 E, Capitol Expressway Ste 60, San Jose,...	

DELAYS

Heavy traffic in this area



China Telecom

AT&T Listening Post

Major Data Center

Google Data Center

5 IXPs

https://www.google.com/maps/dir/China+Telecom+(Europe)+Ltd./Equinix/Telehouse+London+Data+Centre

- China Telecom (Europe) Ltd., 2nd Floor,
- Equinix, 2 Harbour Exchange Square, Isl
- Telehouse London Data Centres, Corian
- 43-53 Trafalgar Rd, East Greenwich, Lo
- Sovereign House, 227 Marsh Wall, Isle
- Pennine House, 215 Marsh Wall, Isle of
- Bank of New York, 8-9 Harbour Exchang
- 6-7 Harbour Exchange Square, Isle of D
- 47 Millharbour, Isle of Dogs, London E1

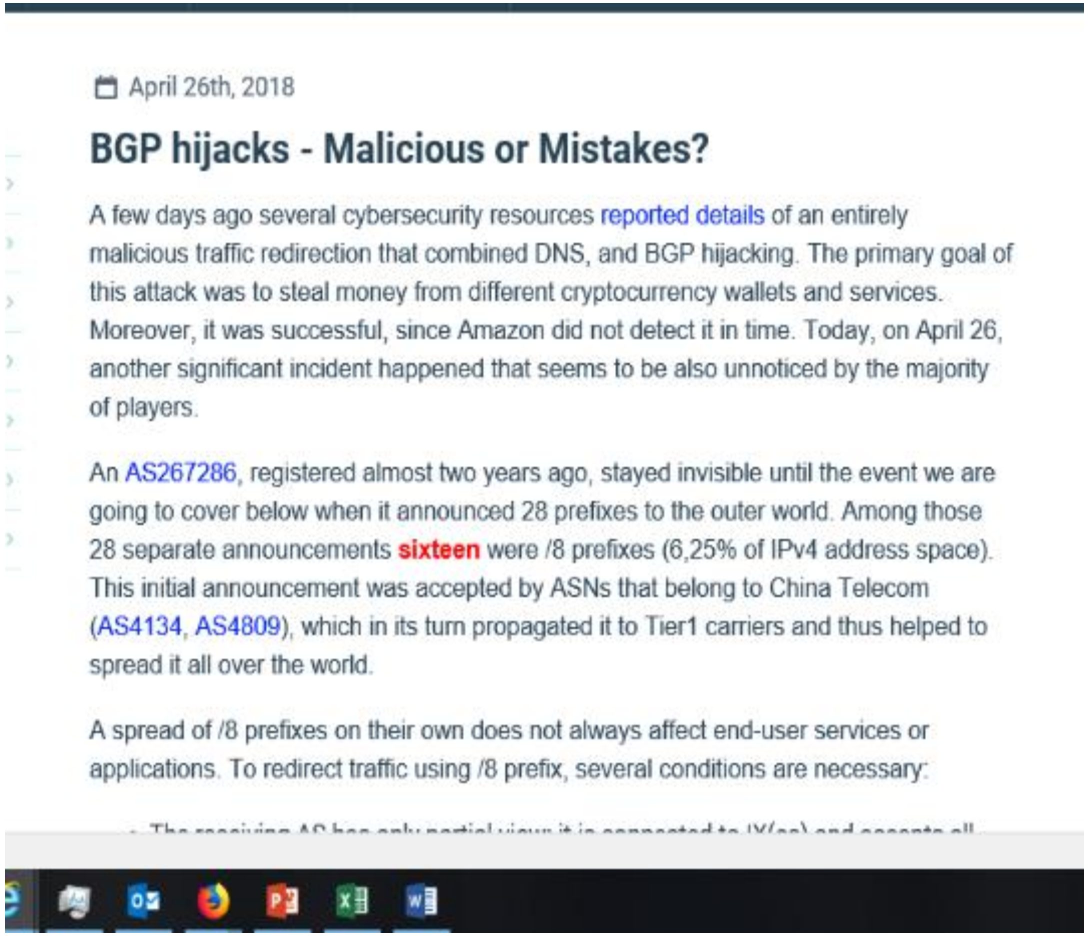
Add destination

OPTIONS

Send directions to your phone

via Millharbour and Marsh Wall 54 min

Why Sao Paulo?



April 26th, 2018

BGP hijacks - Malicious or Mistakes?

A few days ago several cybersecurity resources reported details of an entirely malicious traffic redirection that combined DNS, and BGP hijacking. The primary goal of this attack was to steal money from different cryptocurrency wallets and services. Moreover, it was successful, since Amazon did not detect it in time. Today, on April 26, another significant incident happened that seems to be also unnoticed by the majority of players.

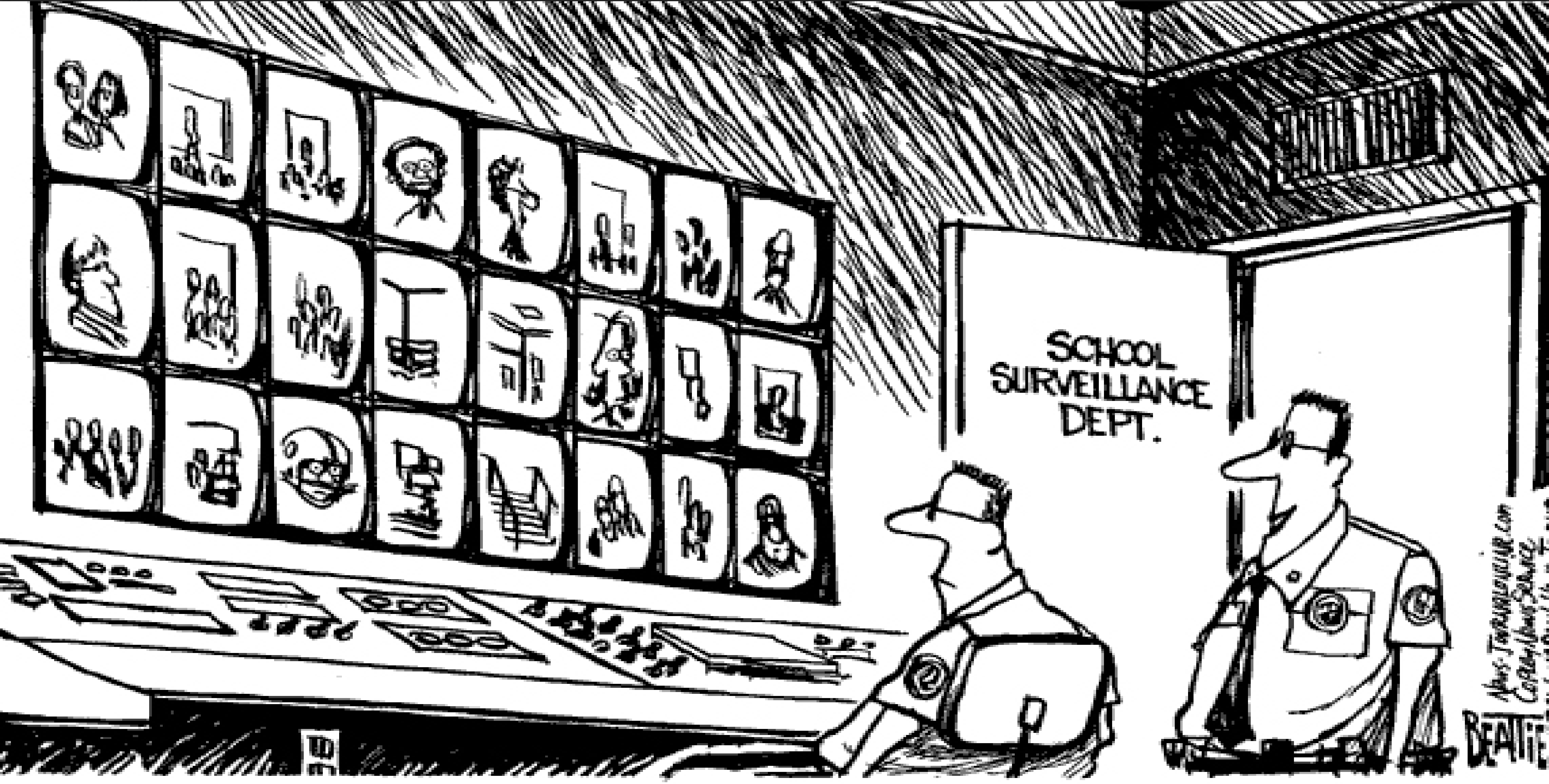
An AS267286, registered almost two years ago, stayed invisible until the event we are going to cover below when it announced 28 prefixes to the outer world. Among those 28 separate announcements **sixteen** were /8 prefixes (6,25% of IPv4 address space). This initial announcement was accepted by ASNs that belong to China Telecom (AS4134, AS4809), which in its turn propagated it to Tier1 carriers and thus helped to spread it all over the world.

A spread of /8 prefixes on their own does not always affect end-user services or applications. To redirect traffic using /8 prefix, several conditions are necessary:

- The receiving AS has only partial view: it is connected to IX(es) and accepts all

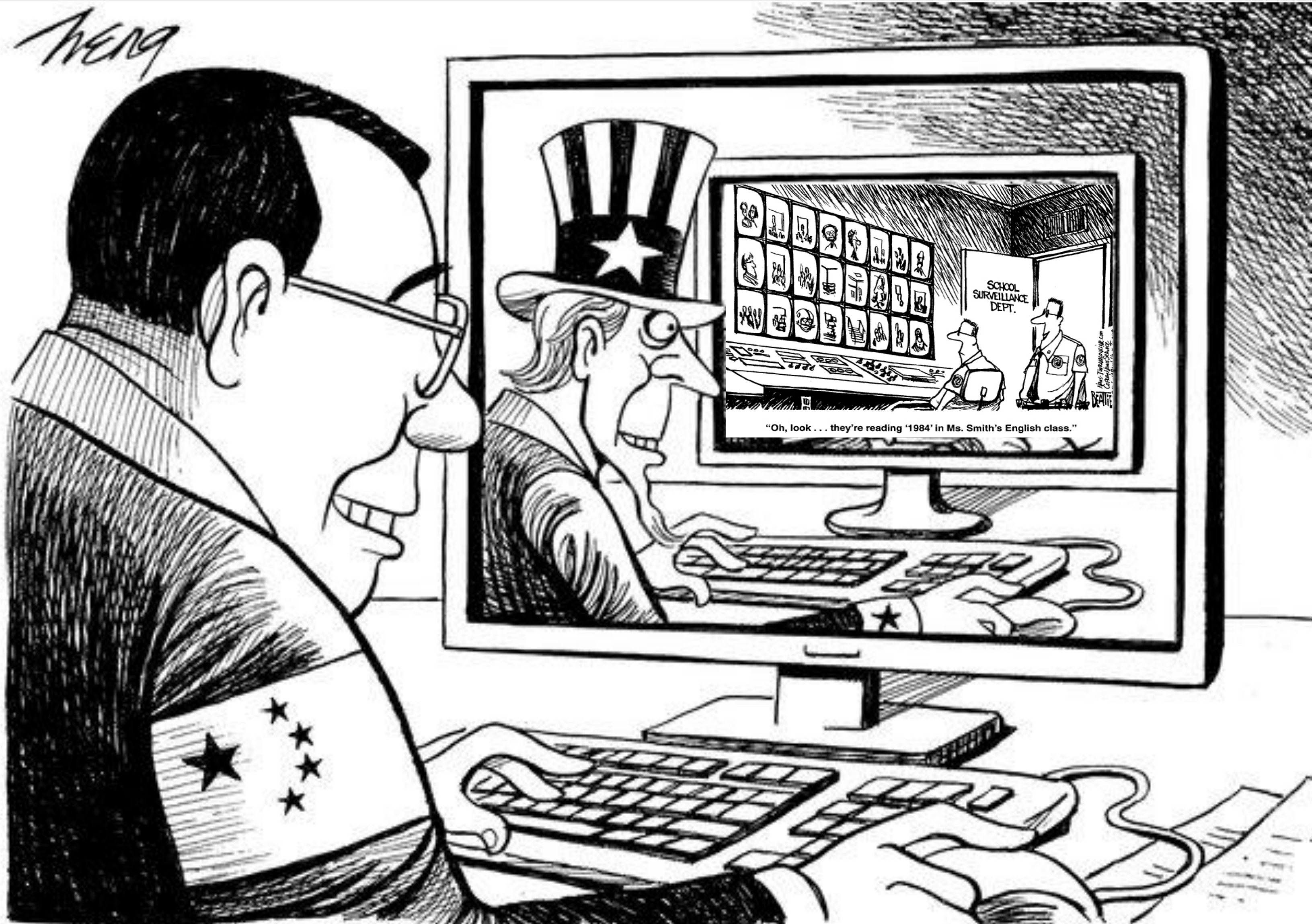
https://radar.qrator.net/blog/bgp-hijacks-malicious-or-mistakes

- An AS267286, registered in 2016, stayed invisible until the event we are going to cover below when it announced 28 prefixes to the outer world.
- This initial announcement was accepted by ASNs that belong to China Telecom (AS4134, AS4809), which in its turn propagated it to Tier1 carriers and thus helped to spread it all over the world.
- To redirect traffic using /8 prefix, several conditions are necessary:
- The receiving AS has only partial view: it is connected to IX(es) and accepts all routes from that source, but accepts only default routes from upstream providers.
- The /8 is distributed through IX, while legitimate more specific routes are not present there.
- With high probability, we can state that those /8 prefixes were distributed at **São Paulo IX, the biggest IX in Brazil.**



"Oh, look . . . they're reading '1984' in Ms. Smith's English class."

And Watching the Watchers…


Heng
SCHOOL SURVEILLANCE DEPT.
BEATTIE
News-Journalonline.com
Copley News Service
"Oh, look . . . they're reading '1984' in Ms. Smith's English class."