SIGPwny

SP2024 Week 12 • 2024-04-14

Location-Based OSINT

Henry Qiu

Announcements

- Shirts are in the process of being ordering

ctf.sigpwny.com

sigpwny{quick.quit.garage}

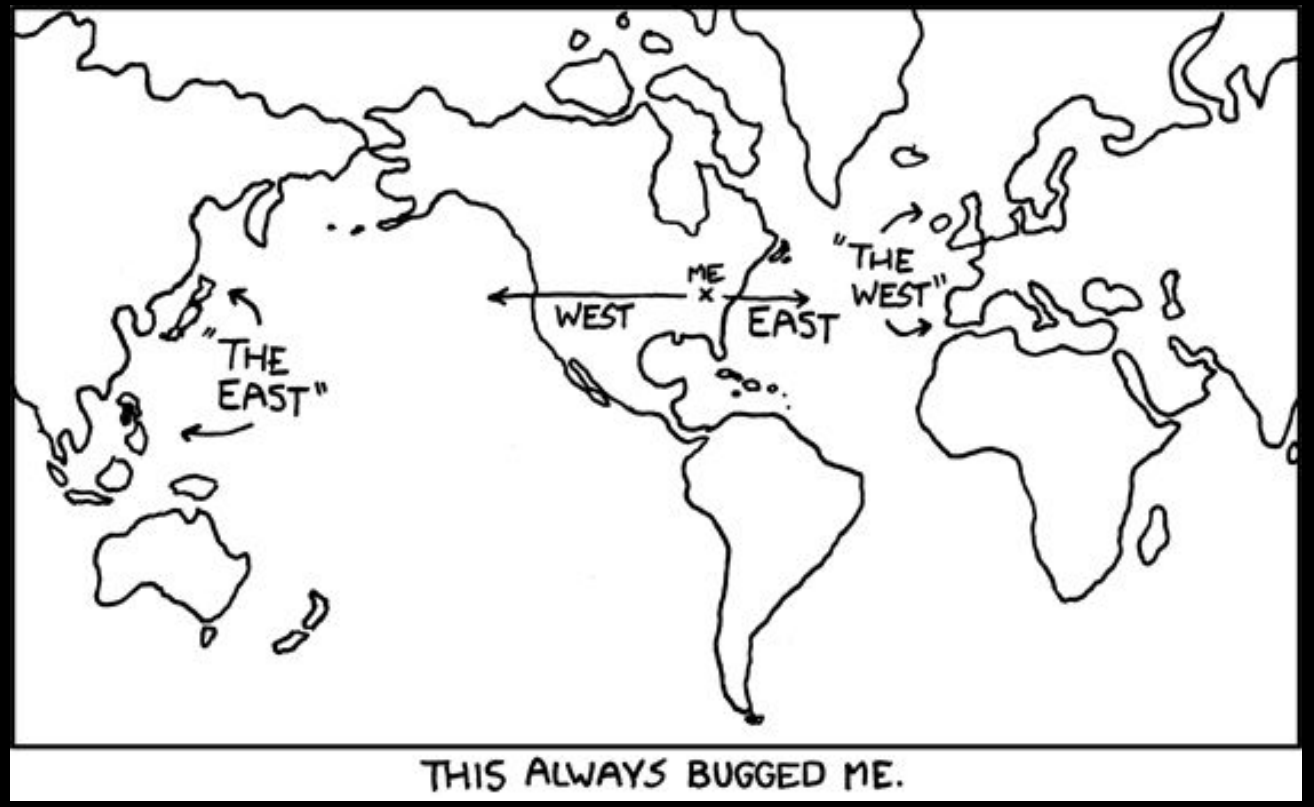


Table of Contents

Disclaimer

A Warning (OSINT Ethics)

OSINT, especially HUMINT (Human Intelligence) is functionally **stalking, especially if you are trying to find someone's location.**

DON'T BE A CREEP

Make sure you have permission before OSINTing someone/thing

You could find something you don't like / aren't supposed to

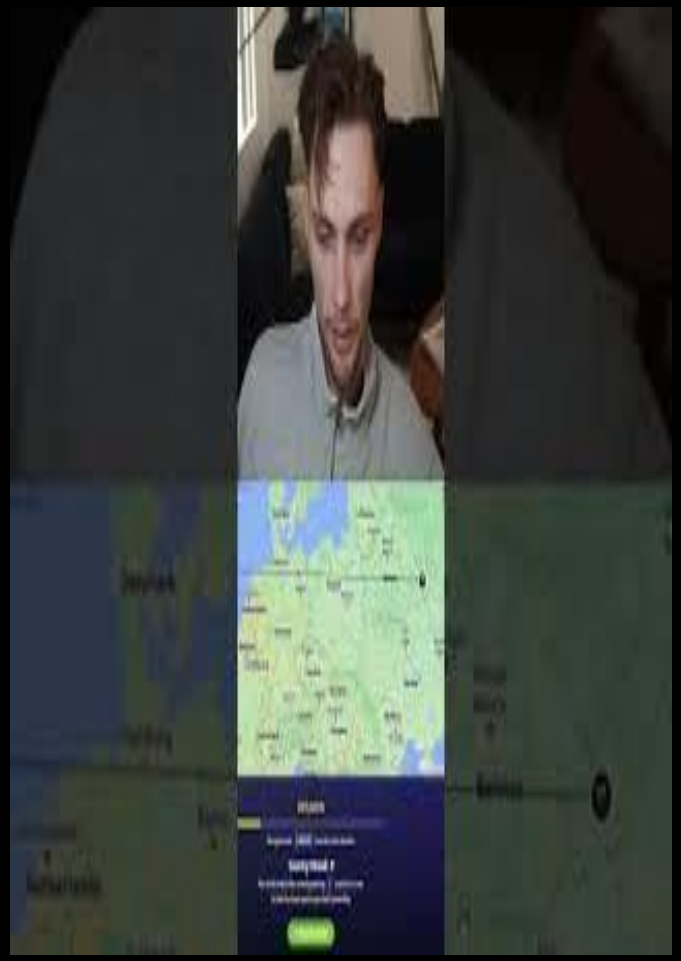
Explicit OSINT Code of Ethics

1. You will **not INTERACT** with any user without first confirming with absolute certainty that they are a part of the challenge. In the case of these challenges, there is **no need to create any content**
2. You will **not perform any port scans on backend services** or attempt to do any investigation by logging in to any of the aforementioned accounts. This is **not web hacking**
3. You will **not perform invasive investigative OSINT on other people without their explicit consent**. This includes friends, family, coworkers, and strangers.

While exceptions exist to this code, those exceptions don't apply here!

Geoguessr vs CTF OSINT

Rainbolt



He’s a Geoguessr god, but…

Geoguessr vs CTF OSINT

- Geoguessr is a game that gives players RANDOM locations, in which players have to identify where they are.
- So the minutiae details like telephone poles, antennas, water tanks, etc are very helpful for identifying a region in the world

- However, in CTF-style OSINT, typically we are given a (set of) images, to identify a PRECISE location. This type of “meta strategy” in Geoguessr doesn’t work well anymore. We’ll typically receive meaningful details in the image to help identify the location.

About this meeting

- Although this meeting will not cover the geoguessr-specific strategies, it will cover most of the information you can extract from a given image. The rest is just hard work matching to find the location.
- It will cover certain tools/tricks that’s usually in such questions.

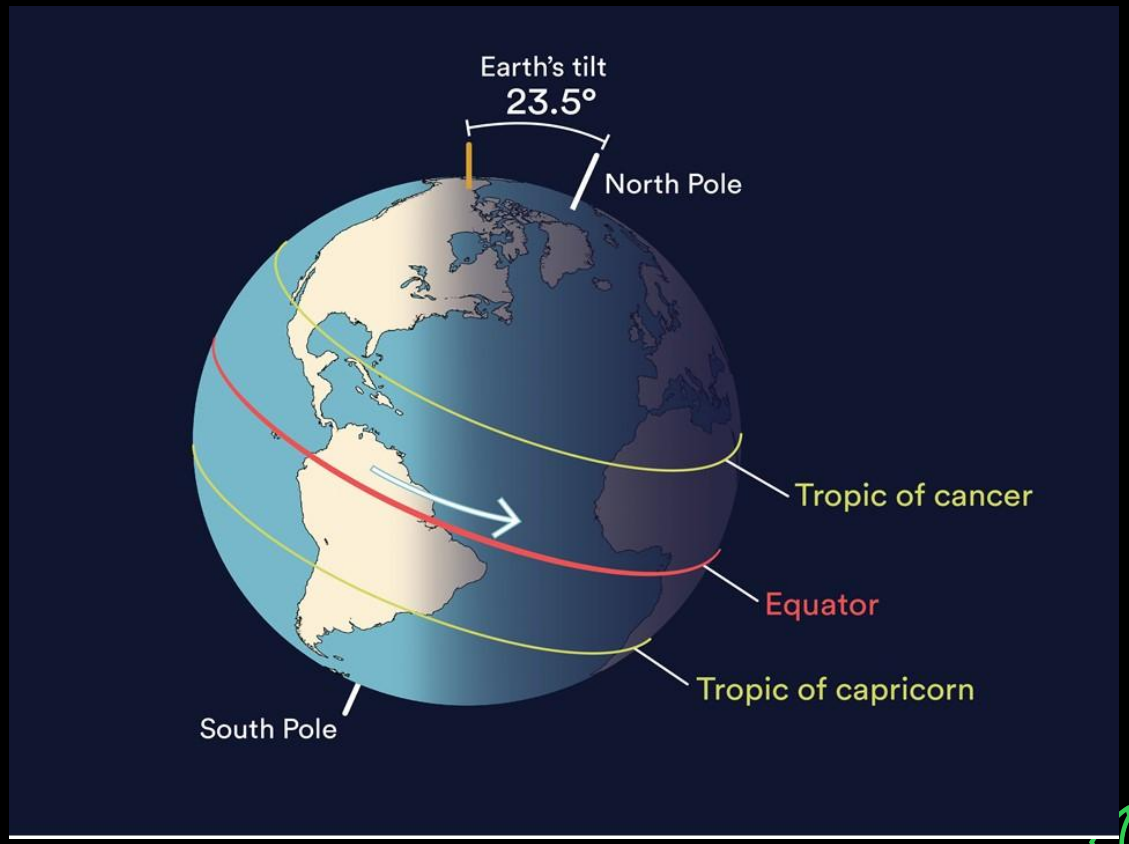
- Also, this meeting is an intentional info dump because it covers aspects people can refer back to, so it will be LONG.

Geography

Sun direction

Common sense: Sun always rises in the east and sets in the west because Earth rotates eastward.

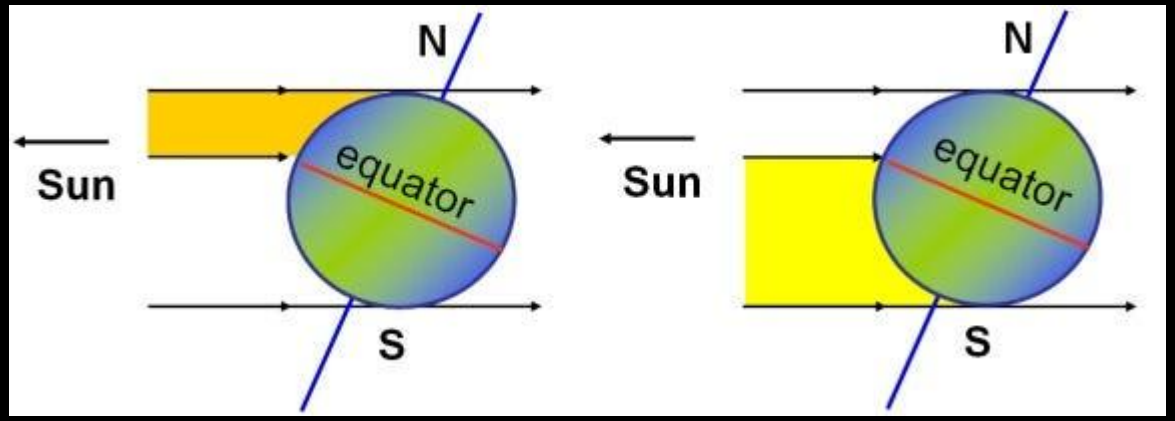
Sun can be directly found overhead at noon in regions between tropic of cancer & tropic of capricorn.



Sun direction

We can identify the hemisphere by this fact -

Generally, If the sun is in the north, you're in the Southern Hemisphere. If the sun is in the south, you're in the Northern Hemisphere.



What are the limitations of this approach?

Sun direction

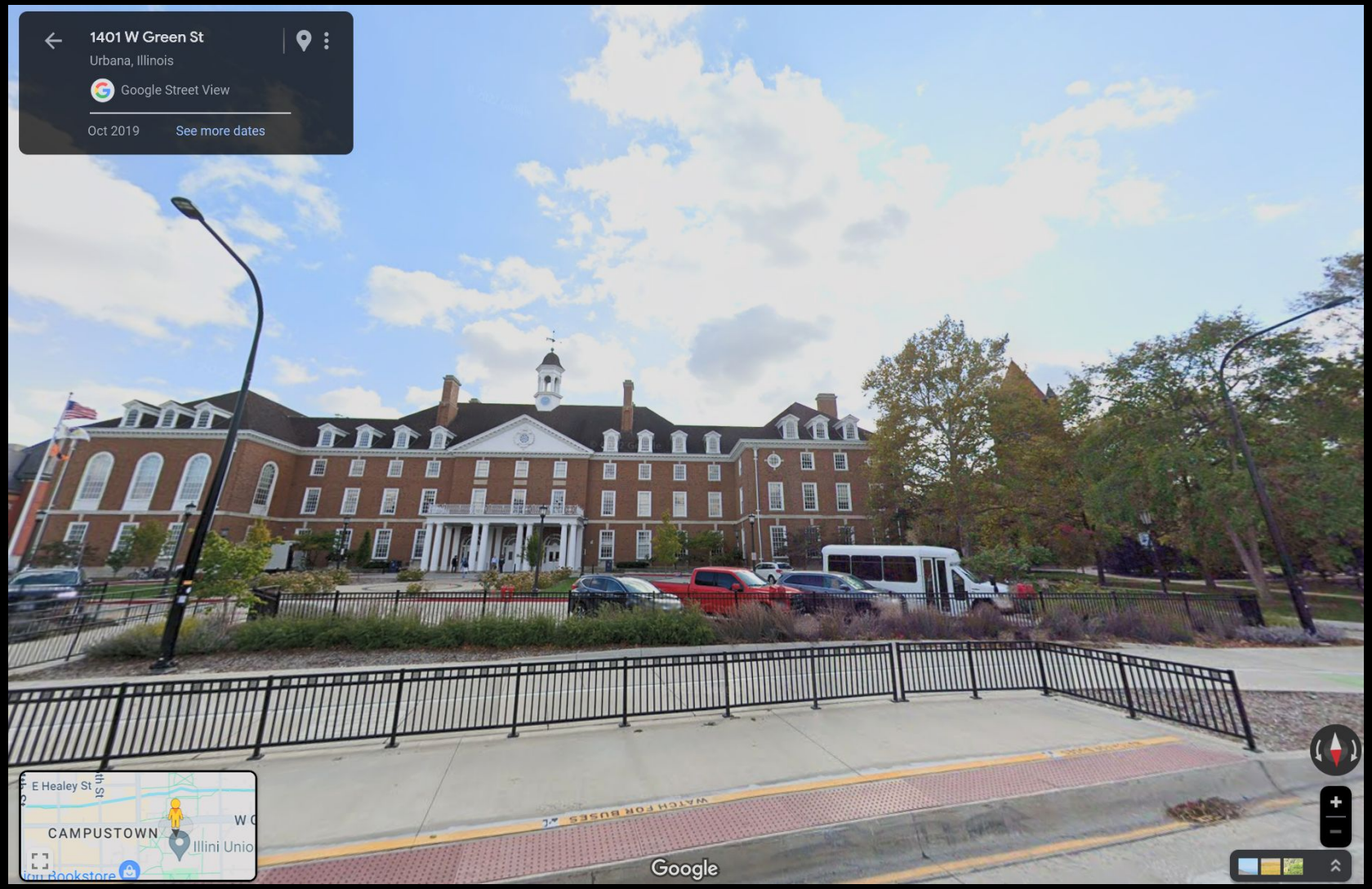
Limitations:

- does not apply to equatorial countries
- applicability & accuracy vastly depend on weather & season

Fixes:

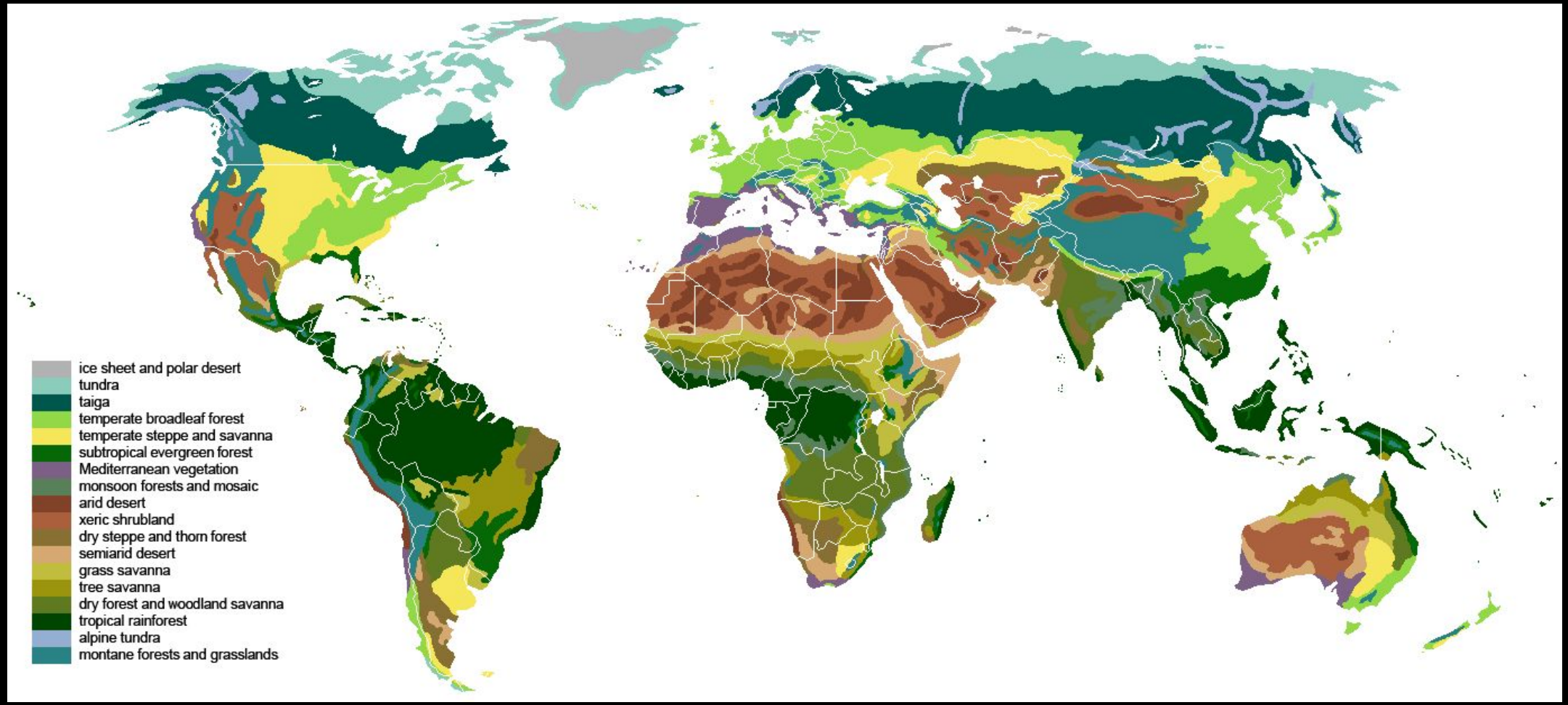
- Look at other reference points - the shadows, the solar panels, etc.
- Use it as only a reference over a rule

Sun direction - Obvious

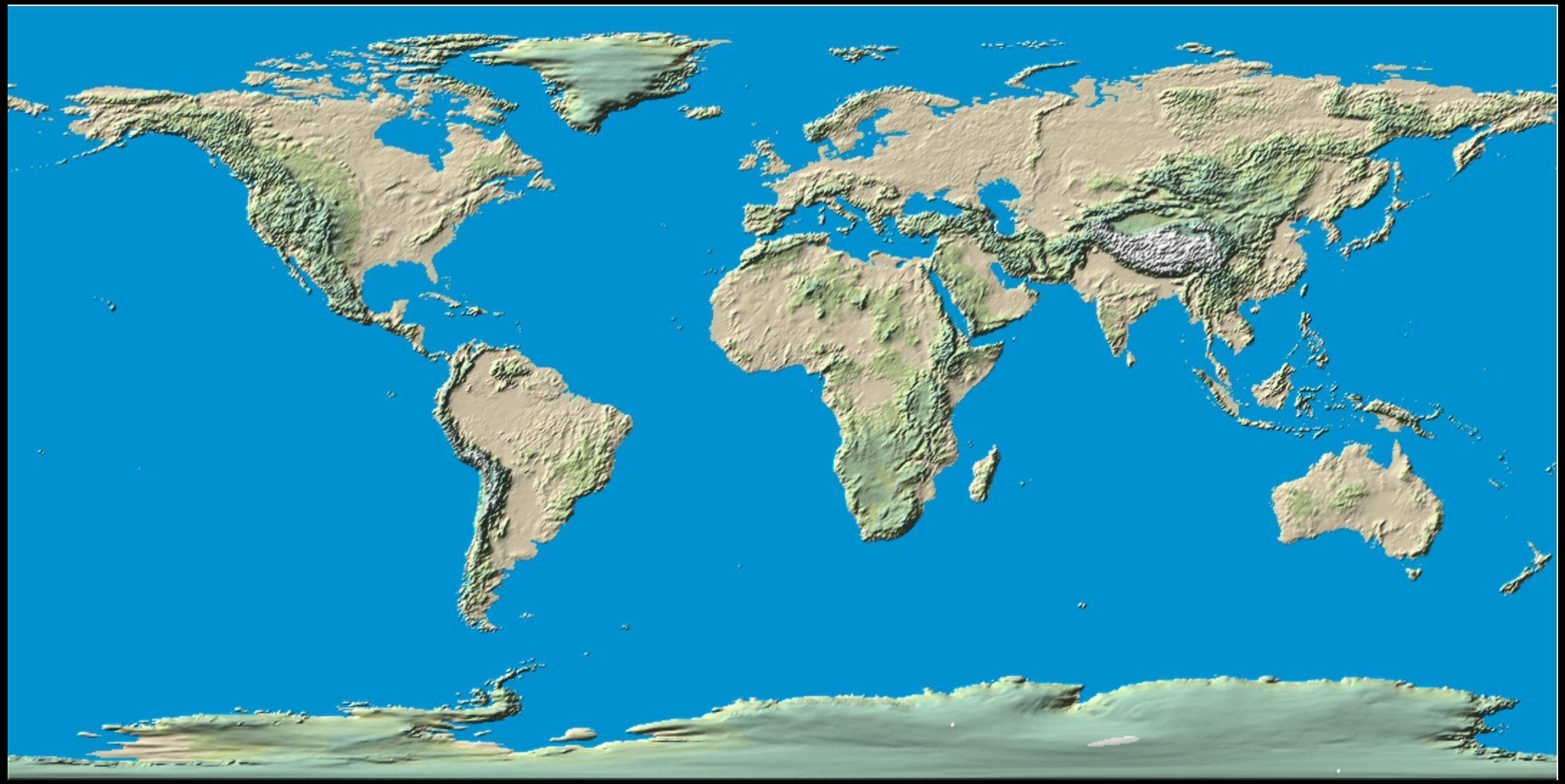


Sun direction - WTF

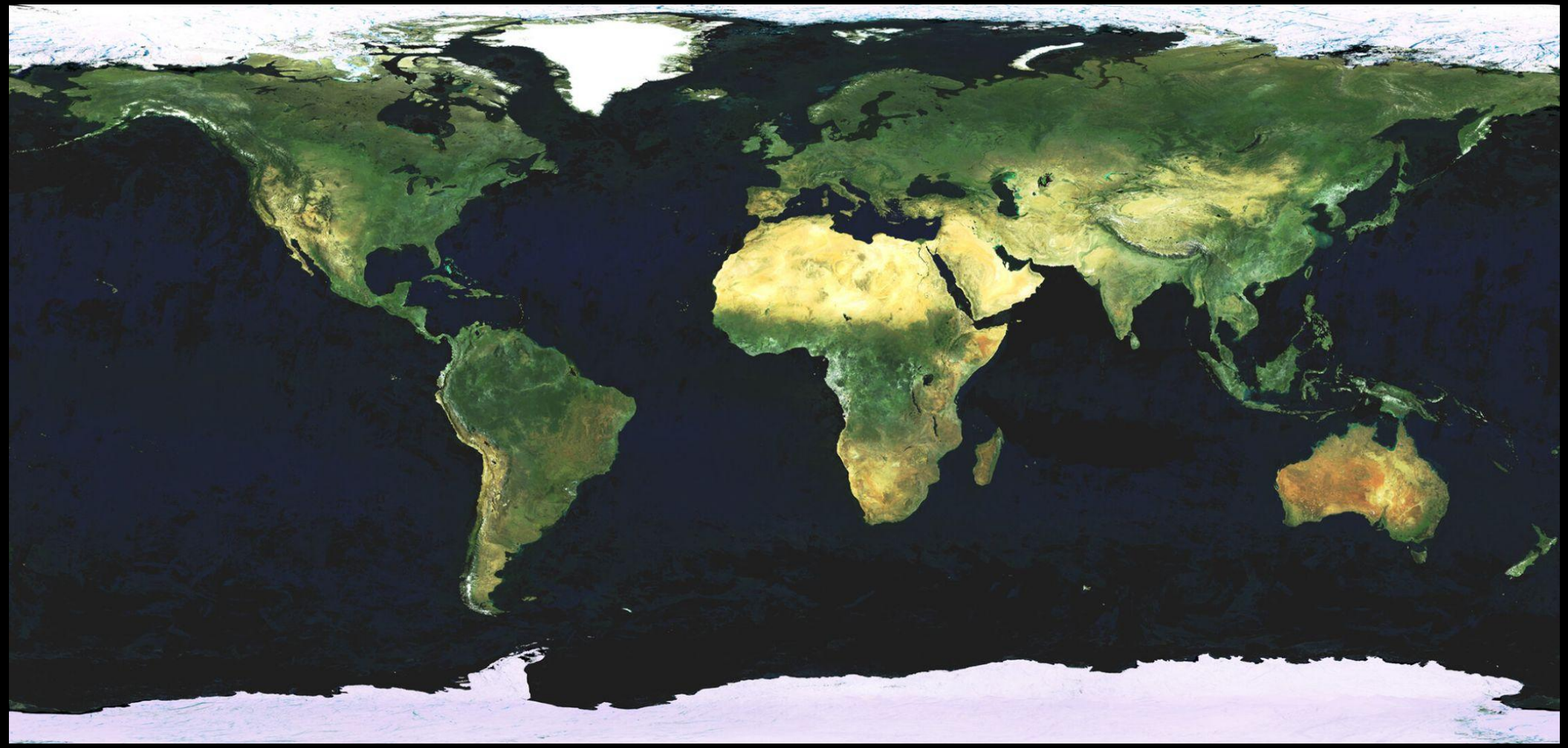
Terrain & Vegetation - Biome Map



Terrain & Vegetation - Elevation Map



Terrain & Vegetation - Sat Map



Obvious US example

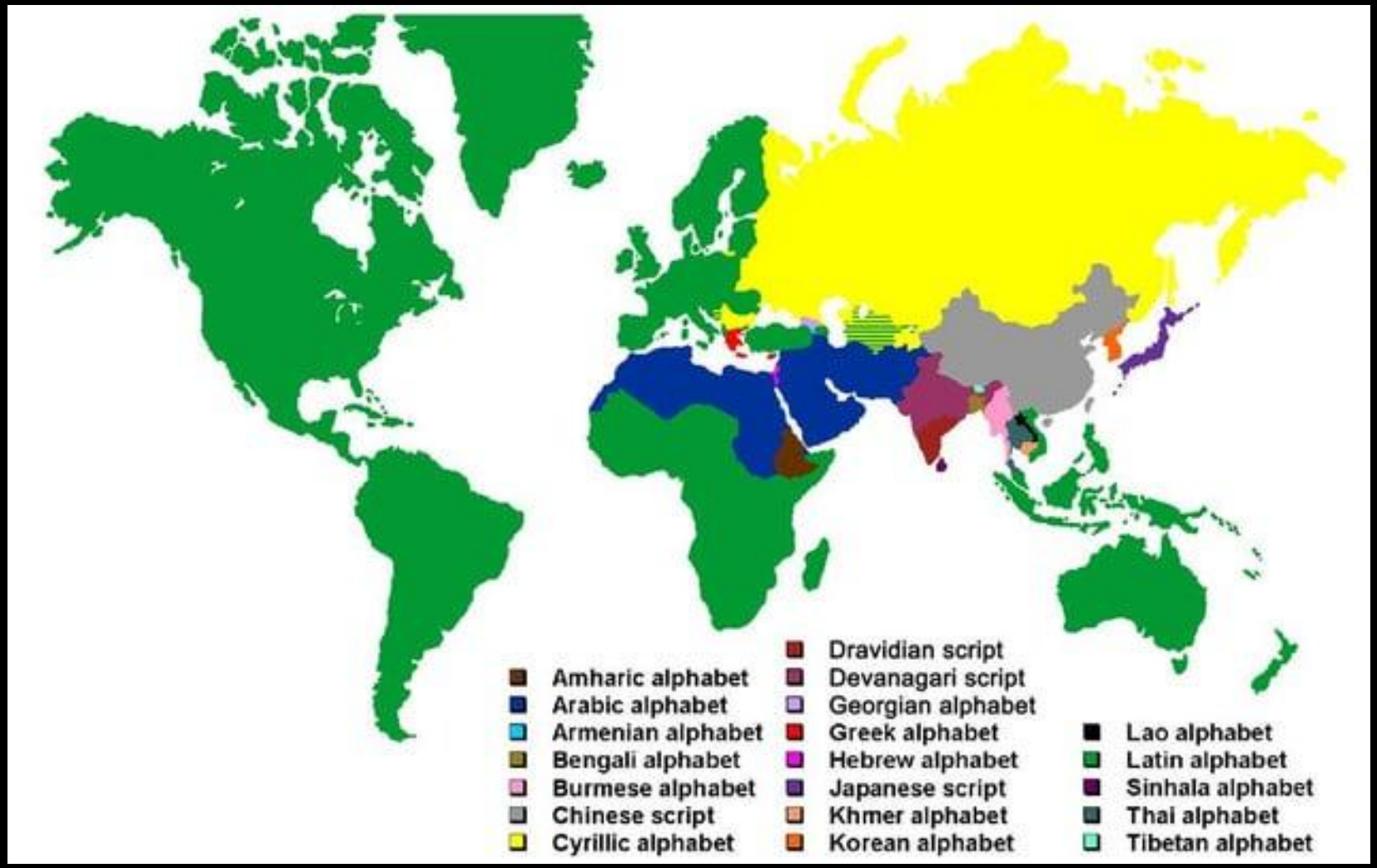
From the previous biome map, this is shrubland.

The area with most shrubland and arid climate is the Rocky Mountains.

This is street view of a random highway in Wyoming.

Human Factors

Languages


Amharic alphabet
Arabic alphabet
Armenian alphabet
Bengali alphabet
Burmese alphabet
Chinese script
Cyrillic alphabet
Dravidian script
Devanagari script
Georgian alphabet
Greek alphabet
Hebrew alphabet
Japanese script
Khmer alphabet
Korean alphabet
Lao alphabet
Latin alphabet
Sinhala alphabet
Thai alphabet
Tibetan alphabet

Languages

- Automatic method: Get a screenshot of the image and give it to Google reverse image search / Google Translate, it will identify the text, auto-detect the language, and translate for you

- Manual method: After identifying the alphabet, Google “[language] keyboard” and manually match the text with the keyboard. It’s especially handy in identifying text that Google has trouble with, e.g. Colorful text on a billboard

Languages

- Latin-Based script: Easy for English speakers to recognize and type, and for the unknown letters we can just Google them. Google translate also has a high accuracy.
- e.g. You can Google “c with a tail” for ç

- Greek alphabet: You learned enough physics and math to identify them. Google does a good job at them. Greek is only spoken in Greece and adjacent areas, and Cyprus.

Languages

- Cyrillic alphabet: Somewhat Easy for English speakers to recognize. Letters are mainly derived from Greek, so resembles Latin alphabet. Google is also good for them.
- e.g. Белый кот учится ловить мышей.

- Note that the letters have vastly different pronunciations than Latin. й is actually a short I and л is actually L.

Asian Languages

- Hill that Americans die on
- https://en.wikipedia.org/wiki/Languages_of_Asia
- I originally split these up into five categories, but due to time constraints I'll only include an overview for Arabic, South and East Asia.
- Detailed coverage will be included in the appendix.

Middle East

- Arabic script & Hebrew: Used across Middle East. slightly harder for English speakers to recognize and for Google to identify. Write from **right to left**.

تخت جمشید

تخت جمشید یا پارسه (یا پرسپولیس، پرسه‌پلیس، هزارستون، صدستون و یا چهل‌منار) نام یکی از شهرهای باستانی ایران است که طی سالیان پیوسته، پایتخت باشکوه و تشریفاتیِ پادشاهی ایران در زمان امپراتوری هخامنشیان بوده‌است. در این شهر باستانی کاخی به نام تخت جمشید وجود دارد که در دوران زمامداری داریوش

אבגדהוזח
טיכלמנסע
פצקרשת
רומחץ

South Asia

- Indo-Aryan family: Non-South India. Have a horizontal line in most characters.
- Also use a vertical bar as periods

- Dravidian languages: South India. Have lots of circles in the characters.

सभी मनुष्यों को गौरव और अधिकारों के मामले में जन्मजात स्वतन्त्रता और समानता प्राप्त है। उन्हें बुद्धि और अन्तरात्मा की देन प्राप्त है और परस्पर उन्हें भाईचारे के भाव से बर्ताव करना चाहिए।

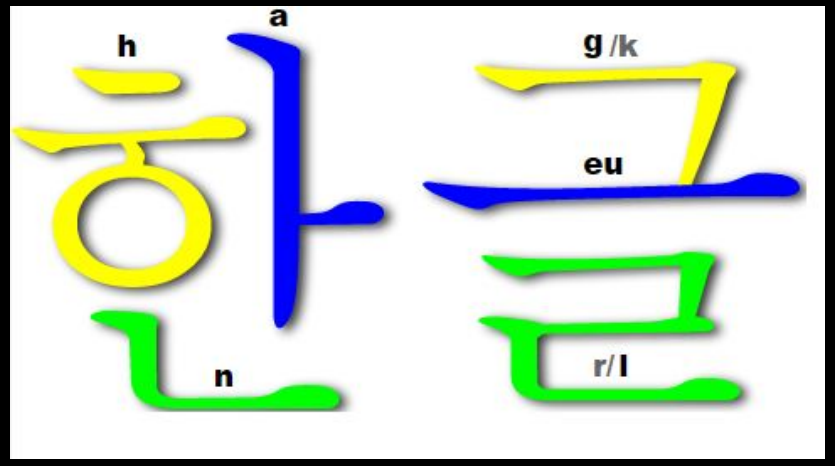
Hindi example

Tamil example

East Asia

- Korean: syllable block letter like LEGO bricks, so super easy to type on a keyboard

- Has a lot of right angle



- Japanese: It uses a mix of Hiragana, Katakana and Hanji (Chinese characters).

- So it has complicated characters mixed with simply, curvy characters

すべての人間は、生まれながらにして自由であり、かつ、尊厳と権利とについて平等である。人間は、理性と良心とを授けられており、互いに同 胞の精神をもって行動しなければならない。

Transportation: Cars

Side of road is extremely important, and can exclude half of the world just by this information alone.

Transportation: Cars

Can you tell me the country based on the side of road and language?

This is a shared taxi in Thailand.

Transportation: Cars

- Due to globalization and urbanization, the car make and type is usually not indicative of region. There are some trends and exceptions to this rule in the appendix.
  - EVs tend to appear in more developed countries while developing countries tend to have more traditional cars.

  - Countries favor their own car brands A LOT. US - Ford, UK - Land Rover, Vauxhall, France - Citroen, Peugeot, South Korea - Kia, Hyundai, Daewoo, Eastern European - Lada, …

  - Chances are, if you don’t recognize a brand, it’s likely local and you should investigate

Transportation: Car plates

- Typically, a country or a region has a unified style of plates. There are many websites covering them, and license plates typically include the language, so it's pretty identifiable.

Europe: (typically longer)

JP, TW and SK:
(white and taller)

Colombia:
(only yellow plate in S.A.)

Transportation: Car plates

- If we can get a full license plate number, we can typically extract more location information from it. We can reference Wikipedia and websites like www.worldlicenseplates.com.

北京现代 = Beijing Hyundai

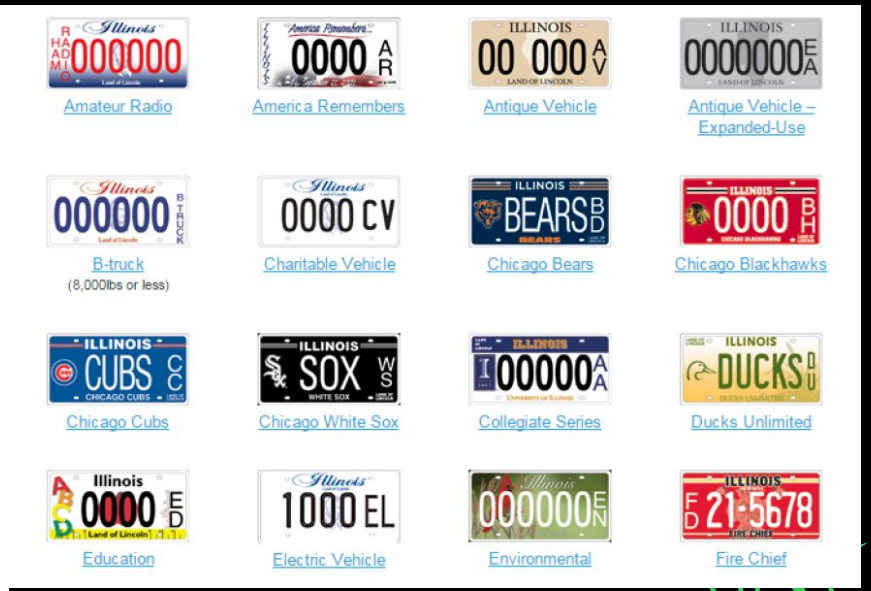
贛 = abbr. of Jiangxi province

K = Xinyu City in Jiangxi Prov.

(Each city has a letter code)

Transportation: America be like

- While most of the world agrees that license plates should be simple, North America disagrees and says, license plate is a perfect place for arts. (Yes, including Canada and Mexico)



Transportation: Subway

- Subway types: Light rail vs Heavy rail
- Light rail: Typically in the form of street cars, taller, narrower, shorter in total length, slower, runs on the surface and may intersect with traffic
- Heavy rail: Typically in the form of metro / trains, wider, longer, faster, runs on dedicated tracks, typically underground.

Transportation: Identifying Subway

- Subways usually have direct information like line number, line color, company marking, station name.
- We can also try to figure out its manufacturer and then location since there are only so many manufacturers.

Chicagoan like to take the L

Can you find where this is?

Transportation: Subway

Can you identify which subway system it is?

Hint: Look at overall style and subway dashboard

Then lookup relevant color

Answer: Green Line in Boston

Because Boston has the oldest subway system in the US, and its green line is remnants of a streetcar system.

Transportation: Buses

- There are two major North American bus companies - Gillig and New Flyer. Their buses are very similar.
- If you see something resembles MTD bus, with yellow/ white display, you know you're in North America.

Transportation: Buses

- There are more diversity in other regions, but using the identification methods to see the car's brand, livery, plate, language, etc.
- For example, Europeans favor brands like Mercedes and Solaris Bus.

Buildings / Landmarks / City vibes

- Two important factors to identify a city is its population density and age. These would reflect on all the aspects - housing height, style, development, road width, marking, etc.

- For example, due to city planning regulatory differences, two largest cities in the US (LA and NYC) have vastly different vibes. LA has more suburbs and lower buildings, while manhattan is filled with skyscrapers.

Buildings / Landmarks / City Vibe

Can you identify where this is?

Hint: Look at the sheer amount of skyscrapers

Answer: Of course it’s NYC.

This photo was taken on a train inbound to Manhattan.

Case study: Japan vs Europe

Case study: Europe vs Japan

Methods & Misc

General Methodology

- Find the image: Google reverse image search
- Extract information: Search any meaningful words that appear in the image, which could contain road / location names
- Enumeration: Google Street View / Earth in suspected region
- Coordinates: Right-click on Google maps to get coordinates and convert to desired format, remember to try surrounding coordinates to prevent the “miss by one” error.
- Last Resort: Use other details to gradually expand your search zone, until you found a new suspected region.

What3words

- Meeting Flag is ACM room in what3words
- “What3words is a proprietary geocode system designed to identify any location on the surface of Earth with a resolution of about 3 metres.”
- Intended purpose is emergency services, because it’s more convenient than a conventional coordinate system
- Often gets abused by CTFs

- Other coordinate systems are rarely used, except the standard GCS

Next Meetings

2024-04-18 • **This Thursday**

- Social Engineering with Emma and Sagnik

2024-04-25 • **Next Thursday**

- MPC (Multi-Party Computation) with Sagnik

ctf.sigpwny.com

`sigpwny{quick.quit.garage}`

Meeting content can be found at sigpwny.com/meetings.

SIGPwny

Appendix

Car Exception - Cuba

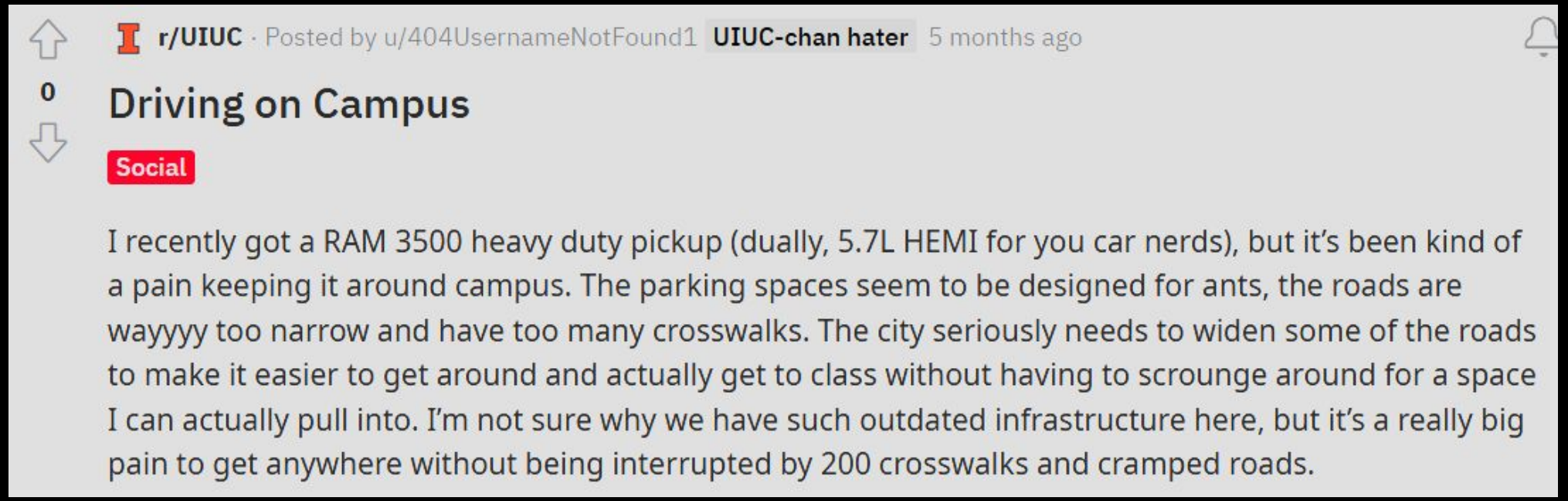
- Due to the U.S. embargo in 1962, they could not import newer vehicles, so they have so many vintage cars.

Car Exception - Japanese Kei car

- Super compact car, usually seen in Japan or other Asian countries. Can be identified using plate & super narrow street.

Car Exception - American pickup

- Sure, using pickup trucks to haul goods is a legitimate use. But when you see an abundant of pickup trucks, with just a flatbed (Asian countries tend to put racks on their trucks), in a gigantic parking lot, you bet it's 🇺🇸. (This is not a shitpost btw)



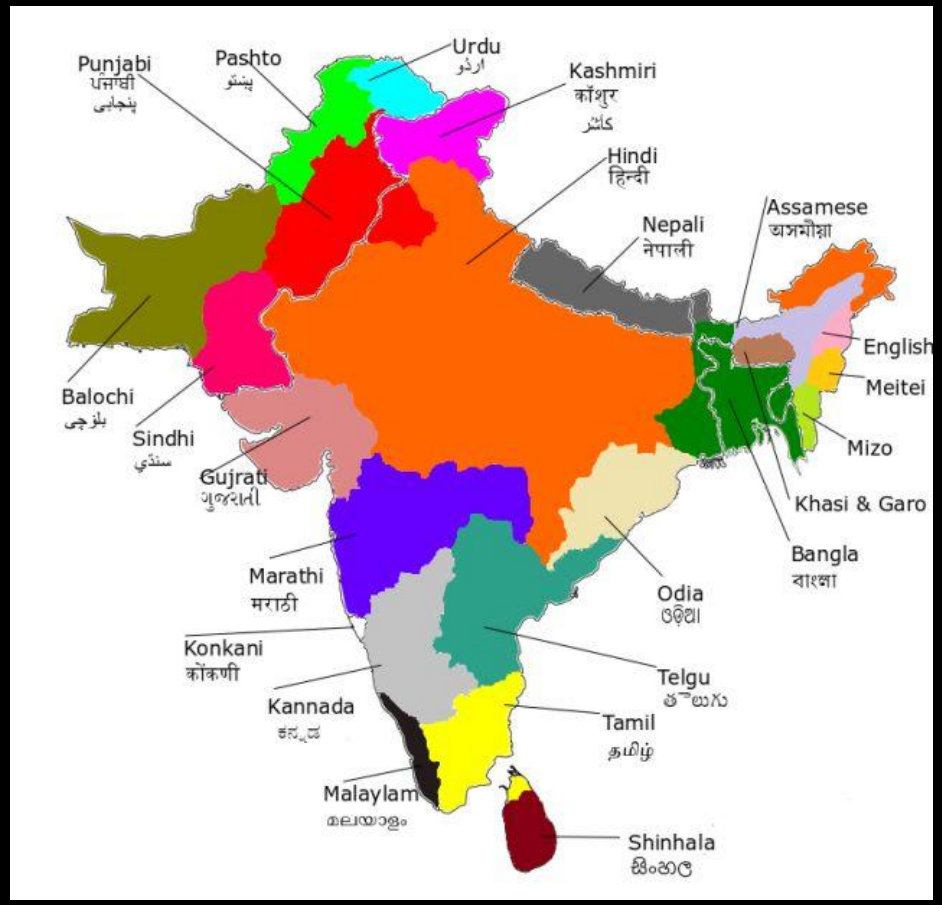
Central Asia

- Due to the presence of Soviet Union, many countries have Cyrillic alphabet and have Russian as a secondary official language.
- Many central Asian languages use multiple alphabets in a unique variant to represent the pronunciation.

South Asia

- The northwestern part has middle east influence, so many used Arabic alphabet.

- Other languages have a very curvy alphabet due to having to write on palm leaves



South Asia

- Indo-Aryan family: Non-South India. Have a horizontal line in most characters.
- Also use a vertical bar as periods

- Dravidian languages: South India. Have lots of circles in the characters.

सभी मनुष्यों को गौरव और अधिकारों के मामले में जन्मजात स्वतन्त्रता और समानता प्राप्त है। उन्हें बुद्धि और अन्तरात्मा की देन प्राप्त है और परस्पर उन्हें भाईचारे के भाव से बर्ताव करना चाहिए।

Hindi example

Tamil example

Southeast Asia

- Thai & Laos: Also contains lots of circles and curves, but the characters look to be the same size and way narrower.

- Others use Latin alphabet with local variation. For example, Vietnamese is monosyllabic with accents.

ปิดทองหลังพระ

Thai example

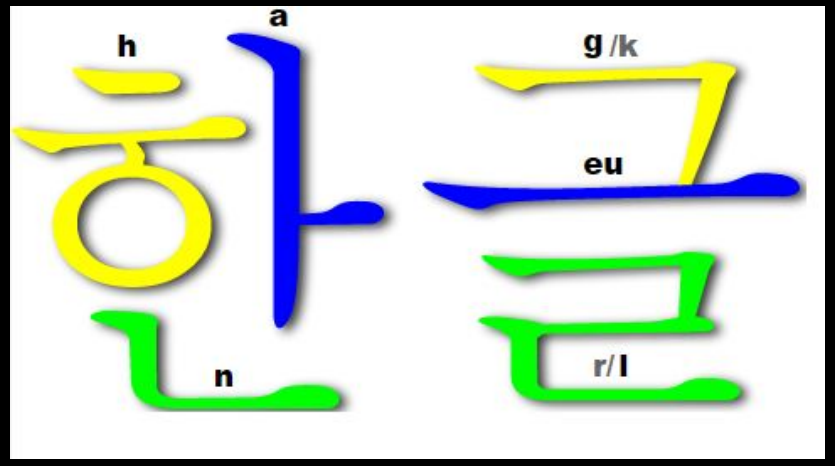
Thập kỷ cuối cùng của thế kỷ 20 đã chứng kiến sự phát triển của Hiệp hội các nớc Đông - Nam á (ASEAN) thành một tổ chức bao gồm tất cả 10 nớc trong khu vực. Lợi ích chung về hòa bình, ổn định, phát triển của mỗi nớc và cả khu vực đã liên kết tất cả các nớc Đông - Nam á vào một gia đình ASEAN, vợt qua những khác biệt trong thể chế chính trị, xã hội, bản sắc văn hóa, tôn giáo và chênh lệch về trình độ phát triển kinh tế, đẩy lùi vào quá khứ thời kỳ của những chia rẽ, định kiến và thù địch.

Vietnamese example

East Asia

- Korean: syllable block letter like LEGO bricks, so super easy to type on a keyboard

- Has a lot of right angle



East Asia

- Chinese: all the characters appear to be the same size, and mostly square

- Most characters contain multiple strokes, giving it a complicated appearance.

East Asia

- Japanese: It uses a mix of Hiragana, Katakana and Hanji (Chinese characters).

- So if you see complicated characters mixed with simply, curvy characters it’s Japanese.

ん ン n	わ ワ wa	ら ラ ra	や ヤ ya	ま マ ma	は ハ ha	な ナ na	た タ ta	さ サ sa	か カ ka	あ ア a
		り リ ri		み ミ mi	ひ ヒ hi	に ニ ni	ち チ chi	し シ shi	き キ ki	い イ i
		る ル ru	ゆ ユ yu	む ム mu	ふ フ fu	ぬ ヌ nu	つ ツ tsu	す ス su	く ク ku	う ウ u
		れ レ re		め メ me	へ ヘ he	ね ネ ne	て テ te	せ セ se	け ケ ke	え エ e
	を ヲ wo	ろ ロ ro	よ ヨ yo	も モ mo	ほ ホ ho	の ノ no	と ト to	そ ソ so	こ コ ko	お オ o

ctf.sigpwny.com

`sigpwny{quick.quit.garage}`

Meeting content can be found at sigpwny.com/meetings.

SIGPwny