Question on April 23

1. セキュリティ面での過保護は逆に攻撃があった際に修復不可能な状態を生むかもしれないというお話があったが、この過保護を防ぐべくなされている策に関しても興味が湧いた。

➔事故を隠さず公表して、情報の共有を広く行う ですね。 恥ずかしい・都合の悪い情報の公開/公表は、多くの場合「不都合な真実・事実」かね、、、そうなると、「匿名化」が必要になる場合が少なくないですね。

➔みんながちゃんと報告しない時には、法律化で対応になる(なっちゃった)。

2. セキュリティにコストの保障も含まれるというのは今回の講義での新たな気づきでした。しかし、サイバーセキュリティの文脈でこの点に関する考慮や技術があまりないように、仮に保障するとして、どうやって保障するのかが難しいと思いました。流出してしまった情報は戻らず、その価値も人によって違うと考えたからです。もし、何かすでに考えられている案や例があれば教えていただきたいです。

➔ 可能でリーズナブルな措置を 自分で行うですね（自助）

3. 事後の対応が重要であるというのは大事な考え方だと思った。事後の対応を良くするには深い知識が必要となりそうで、経験が重要になってくると思った。

4. 生成AIに入力した情報は漏れると思うが、実際にそれで問題になった事例があったら教えてはしいです。そしてやはりそれを防ぐ手段はないのでしょうか
   ➔結局は、自助だね。
   ➔データの流通でのAAA機能ですね。 Authentication（認証）・Authorization（認可）・Accounting（アカウンティング／監査）
   ➔これが、、、Agentic AI では、既に問題になっていますね。
5. どんなに発達しようがセキュリティにおいて結局一番のウィークポイントは人間ですね…
   ➔ デジタル ファースト＆完結へ ？
6. ChatGPTといった生成AIに入力した情報が悪用されることはあるのでしょうか。
   ➔ 利用という名の(別目的での)悪用？
7. 物理的な戦争においてはミサイル、核といった強力な攻撃手段ほどコストが大きくなり、特殊な設備が必要になるため容易に行使できないのに対して、情報セキュリティにおける強力な攻撃とはどのようなものなのでしょうか。
   ➔ 物理的設備の機能不全、さらには 破壊も可能でしょ。

8. プライバシーに主観的な面が強いのならば、プライバシーの侵害を主張した側が有利になりやすいのでしょうか？
   ➔ 存在することの証明は簡単だけど、存在”しない”ことの証明は難しいねぇ。
9. 鍵の証明をする機関の信頼性はどのように担保されているのか気になりました。
   ➔ TRUST ですね。。 政府は 信用できる？
10. プライバシーをどこまで考えるかは難しいと感じました。人によって許容範囲は変わるけれど、国として考えるなら一律的な基準が必要で、結局「適当」に合わせることになるけれど、その基準が難しいと思いました。
11. 過保護なセキュリティーほど安全なセキュリティーではないことは少し以外であったのと、セキュリティーというのが意外と曖昧な定義であることは驚いた。
12. セキュリティの安全（安心）性と分散化は両立が難しく、ユーザ側に寄せていくことでサイバー攻撃による漏洩リスクを下げることができるのかなと思ったが、その際ユーザ側のデバイスには計算資源がどれくらい必要になるか、それとも暗号化アルゴリズムなどの仕組みの効率化などで可能になるのかなどの点で、どれほどの実現性があるのか疑問に思った。二段階認証や生体認証など、最終的には物質すなわち改ざん不能なもの＋即時利用可能な利便性を持つという意味で、アルゴリズムに人体の情報を組み込むことが現実的なoptionとして導入が進んでいきそうだと思った。（量子コンピュータの出現により、素数の鍵ではランダムさが足りなくなると考えられるため）

13. 著作権・知的財産権も，情報セキュリティも，（パンデミックへの対応も）「閉鎖は逆効果」という全く同じ論理で考えられるというのが新鮮でした． 暗号の安全性に関して，暗号化規則を知るのに必要なデータの数が「十分に多い」ことで安全性を担保しているとありましたが，それを超える数のデータをAIが処理して暗号を破ってしまうということもありえるのかなと思いました．

14. プライバシーは公然の事実になるとプライバシーではなくなるというのは、普段我々が貴重な情報である住所年齢などなどの情報をあらゆる場面で記載しないといけない状況下でその感覚になってしまいプライバシーを保守しようという考えが薄まっているのか？と感じました。

    ➔ Once Onlyで情報の共有で利便性を向上させています。 Dark Sideがあることを 認識・意識して 進めないとね。

15. 過度な規制について以降の説明で、いいかげん(てきとー)と良い加減(適当)のニュアンスの違いを強調するようトーンを変えて説明していたところが印象に残りました。 セキュリティについて、今では攻撃側が有利になってしまったという話がありましたが、今後守備側優位に転換する機会は来るのでしょうか。攻撃手段は守備側の戦略に応じて対抗するように生まれてくるでしょうし、守備側はなんとかして事後策を強化するしかないような気もします。

    ➔ Dark Side と戦う 連合軍 が 必要になるね。

16. セキュリティ攻撃者の大半が組織内部であるという点について、Linuxのxzバックドア事件を思い出しました。組織内部の攻撃者からの巧妙な攻撃を防ぐために、ゼロトラストという観点でどのような対策を取れば良いのか疑問に思った。
    - ➔ 通信の監視 (SOC：Security Operation Center)ですかね。
17. セキュリティは完全にはならず、さらにそのセキュリティ対策は突き詰める程コストがかかるものだと認識している。ここで、経営判断の観点からは、ある一定以上のセキュリティ対策は合理的でないと判断されると思うのだが、それによるインシデントはどのようにケアするのか？保険という形で金銭面での転嫁は可能なはずだが、信用であったりブランドといった、いわゆるのれんの損失はどのようにリスク転嫁するのか疑問に思った。
    - ➔ ① 事後対策(復旧)を意識した防衛。②のれんの損失額 vs セキュリティー対策費
    - ➔ 被害を受け、結果、TSMC は、サイバーセキュリティー基準を作り サプライチェーンの企業に これを調達条件に入れた(Soft Law での対処)。
18. 通信の秘匿性という話題と、チームにおける情報共有とが少し似ているような気がしました。チーム内のある特定のメンバーに対して情報を共有/確認したいとき、そのメンバーにDMを送るか、チームのグループチャット内でメンションするかの二つで分かれると思います。チームの連携を高めるためにはできるだけチーム全体で共有する情報を増やしたほうがいいと思われる反面、プライベートに関わる情報（会議の欠席理由など）まで全体への共有を強制するのは酷です。そして、その境界は人や時期、チームの規模などに大きく依存しています。こう考えると、チーム内の特定の個人と情報共有をしたいときは、何か一つのルールを決めるというよりは、それが誰で何の共有を求めているのかに応じて対応を変えていく必要があると思いました。

19. 私は正直プライバシーの侵害とか言われても、銀行乗っ取られるとか住所特定されて襲われるとかじゃない限り、LINEを見られるとかはわりとどうでもいいと思ってしまうので、あまりプライバシー保護をそんなに全力でやる必要性がわからないのですがどう思いますか。会社とかで機密情報を守らないといけないのはわかりますが、個人を守る必要性がわかりません

    ➔一度開いた 穴は、広がります/広げよう/利用しよう とする 輩が 存在する。

    ➔この輩が、権力者だったら 怖くない？

20. アメリカではFBIが容疑者のネットの監視・傍受などを行って情報を得たり逮捕したりしていると思いますが、これはどうやって実現しているか純粋に気になるというのと、これはプライバシーやセキュリティの観点でどう思われますか。 ➔ 質問19 だね。

21. 最近のサービス開発では、確実かつ低コストのセキュリティ対策として、認証にはクラウドサービスの提供する認証機能を利用するケースが増えているそうです。今までいろんなインターネットのサービスをご覧になってきたと思いますが、そうした認証に対する取り組みの変遷についてなにか感じたことが今までにあれば教えていただきたいです。

“Cloud-by-Default” for multiple pay off

(June 2018 by Japanese gov.)

1. サイロ構造の各省庁のシステムを共有のインフラとして相互接続させ、省庁の壁を越えたデータの自由な利用を実現する。
2. 基盤のサイバーセキュリティ対策は、専門家に任せる。
   (*) オンプレ施設担当人事の 固定費削減 も兼ねる。
3. CAPEXとOPEX, {人件費を含む,} を削減する。
   (*) ハード・ソフト・人： 所有(BS) から 利用(PL)
4. 自然災害&サイバー攻撃に対するBCPを拡充する。
5. 地球温暖化への貢献として、省エネを実現する。

22. プライバシー関連の話題の時に、セクハラは人の容姿などの要素によって境界が分かれるため難しいという話題に対して、ここにAIを使うことで基準を測ることができ得るという話が興味深く感じた。AIはあくまで人ではないため、一般的な感覚を客観的に判断してもらうという状況には適任であると納得でき新たな視点を持てた。
23. イノベーションが積み重なる、つまり過去の産物が増えるほど、しがらみも増え、自由を失うということですか。
    ➔ 「しがらみ」は 事故の防止対策かなぁ。。。 完全が好きな人は、事故を防止するために 「ルールを作る」。 ルールが積み重なる。 Hard Lawは変更に時間がかかる。 Soft Lawは 早く変えらえる。 さて、ルールを作りたい人、捨てたがらない人が 困りますね。 あれれ？？？「規制緩和」？
24. セキュリティに対する施作の一つとしてやらされるではなく、やりたくなるというものがあったが、大抵の場合セキュリティ導入はコスト増など消極的理由が多く、ぱっと思い当たる例がなかったので、積極的理由たり売る事象があれば紹介して欲しいです。
    ➔ 火災・生命・交通 保険の例を 出しました。

24. 安心できるが安全でない状態がセキュリティのあるべき姿だと仰っていましたが、逆に(ほぼ)安全だが安心できない状態として、何か具体例はありますか？

➔ 3.11の時の 原子力発電所とか。

25. プロアクティブな対処についてですが、防御のために攻撃しているかしていないかの線引きが難しそうだなと感じました。実際過剰防衛になったようなケースはあるのでしょうか。

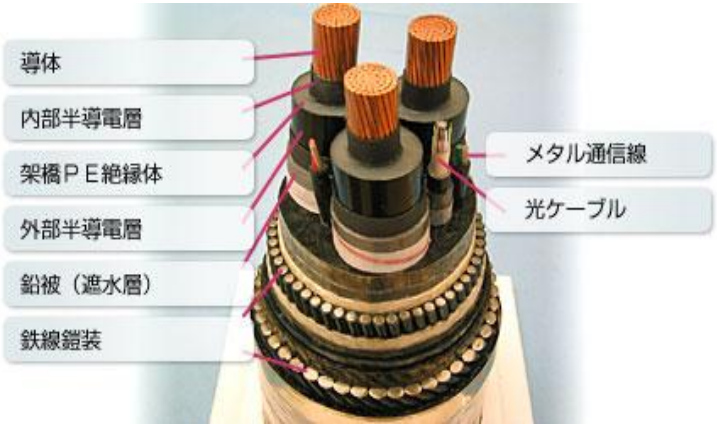
➔過剰防衛にならないように、慎重に!!!

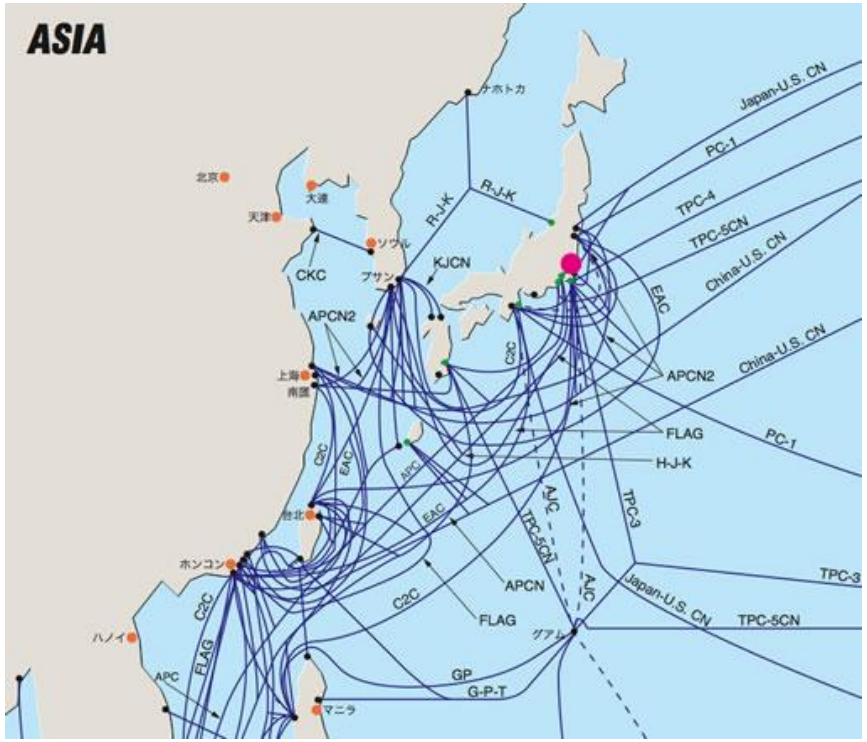
➔過剰防衛を正当化して、戦争は始まってるのが事実かなぁ。

26. 署名のところで、証明する第3のサーバからの証明書が偽造されていないか判別できるのか気になりました。

➔ 難しいね。ということで、相互チェックのブロックチェーンが出てきたかな。

27. 海底ケーブルの敷設の歴史を知りたいです。何らかの目的で海底ケーブルを切断する国も存在すると聞きますが、データ漏洩をふさぐためなのでしょうか。

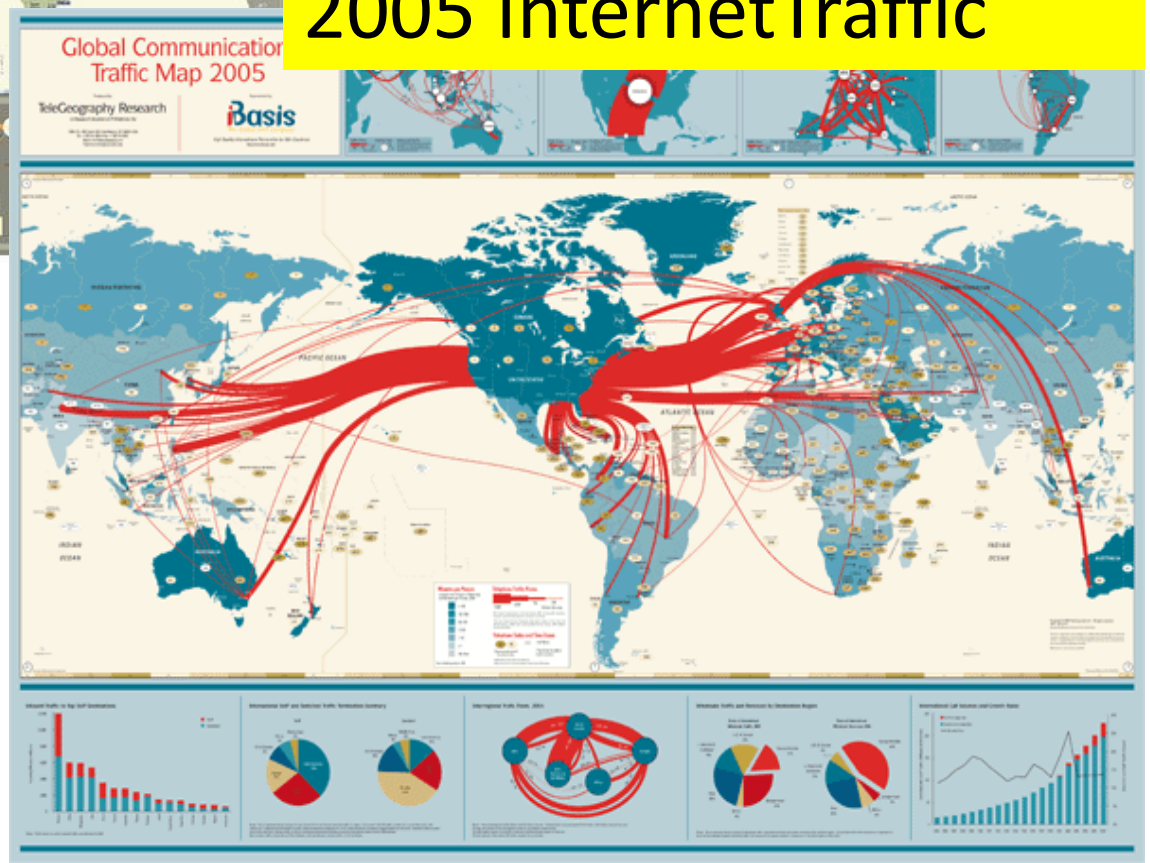

導体
内部半導電層
架橋ＰＥ絶縁体
外部半導電層
鉛被（遮水層）
鉄線鎧装
メタル通信線
光ケーブル


ASIA
ナホトカ
北京
大連
天津
ソウル
CKC
プサン
KJCN
R-J-K
R-J-K
APCN2
上海
南匯
C2C
EAC
APCN2
Japan-U.S. CN
PC-1
TPC-4
TPC-5CN
China-U.S. CN
China-U.S. CN
FLAG
PC-1
H-J-K
TPC-3
台北
ASC
EAC
TPC-5CN
AJC
ホンコン
APCN
FLAG
C2C
C2C
TPC-3
Japan-U.S. CN
TPC-5CN
グアム
ハノイ
FLAG
APC
GP
G-P-T
マニラ

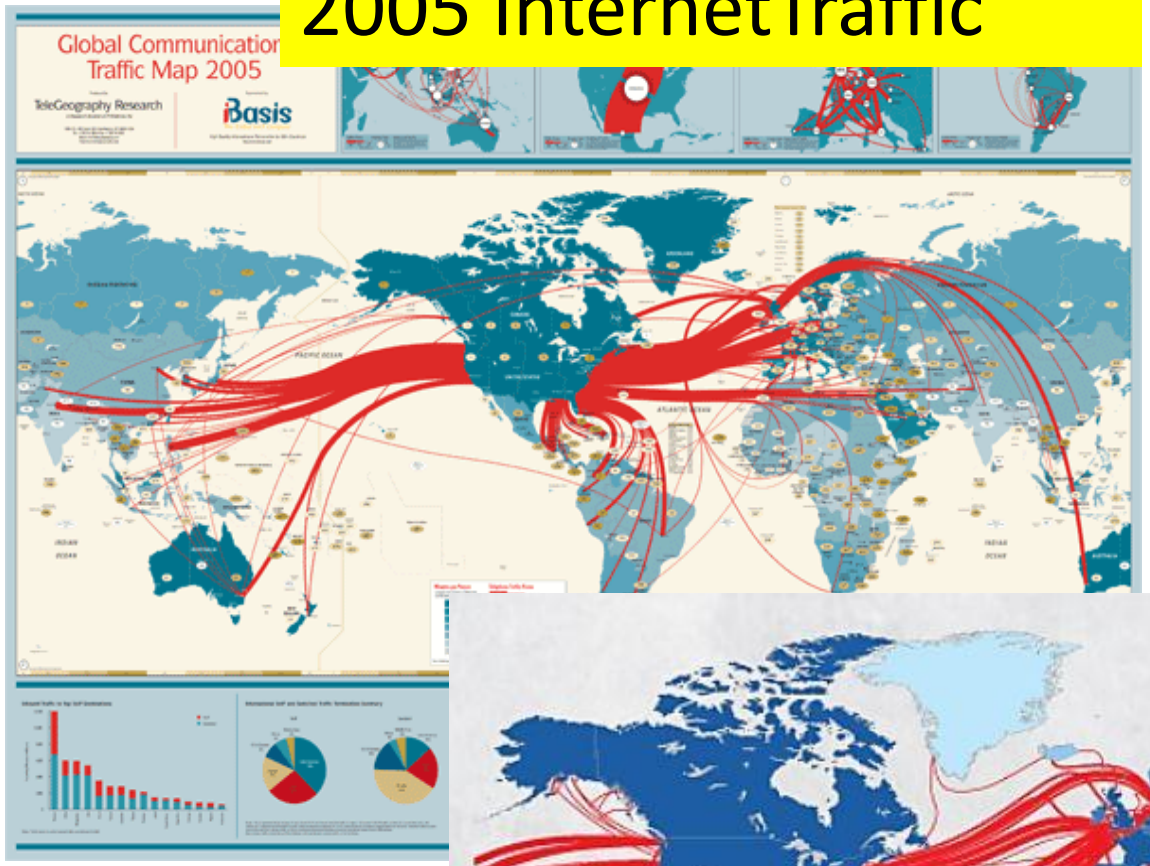

97/08/01 , 11:40:24 , 01277m
(cm)
(C) JAMSTEC

2001 InternetTraffic

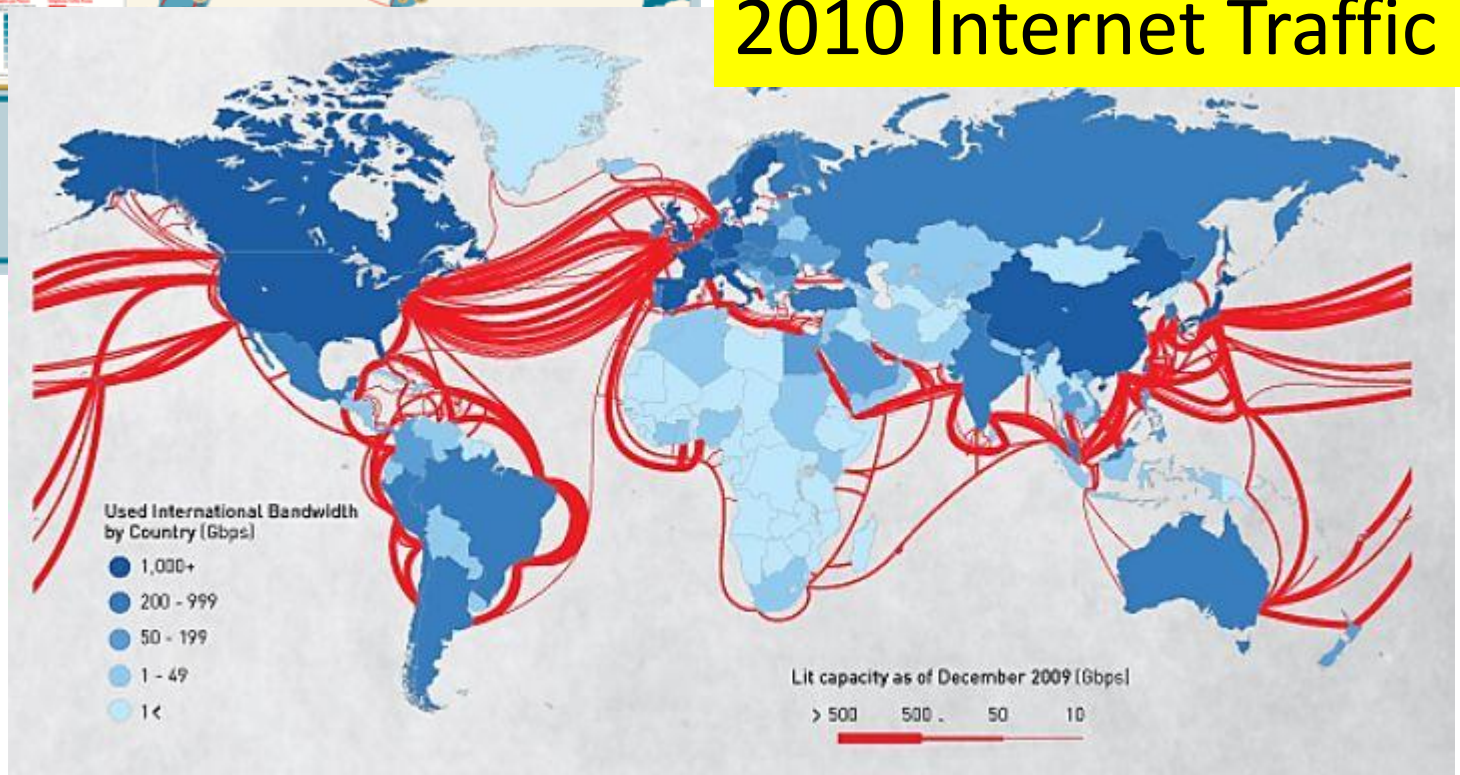
2005 InternetTraffic



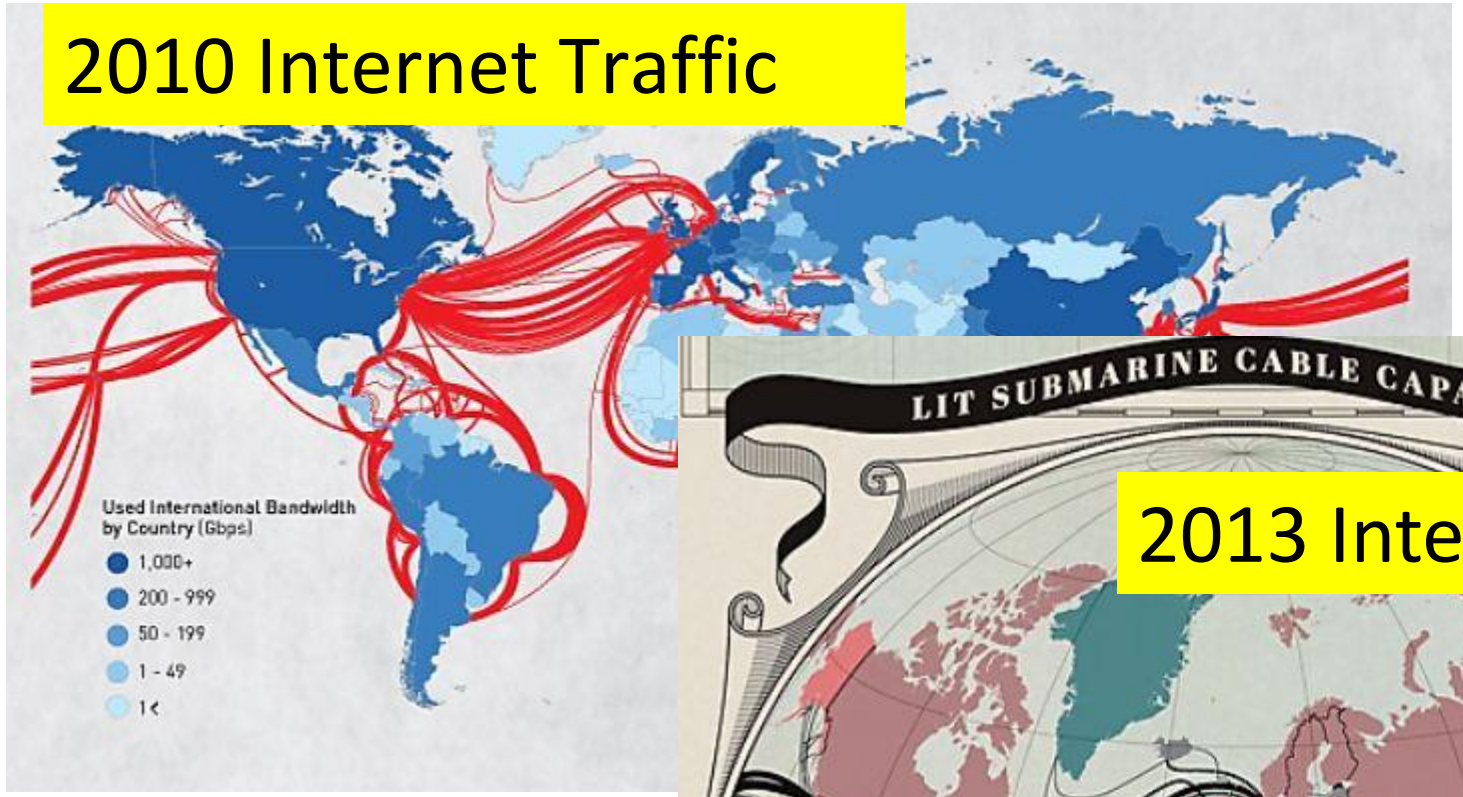
2005 InternetTraffic



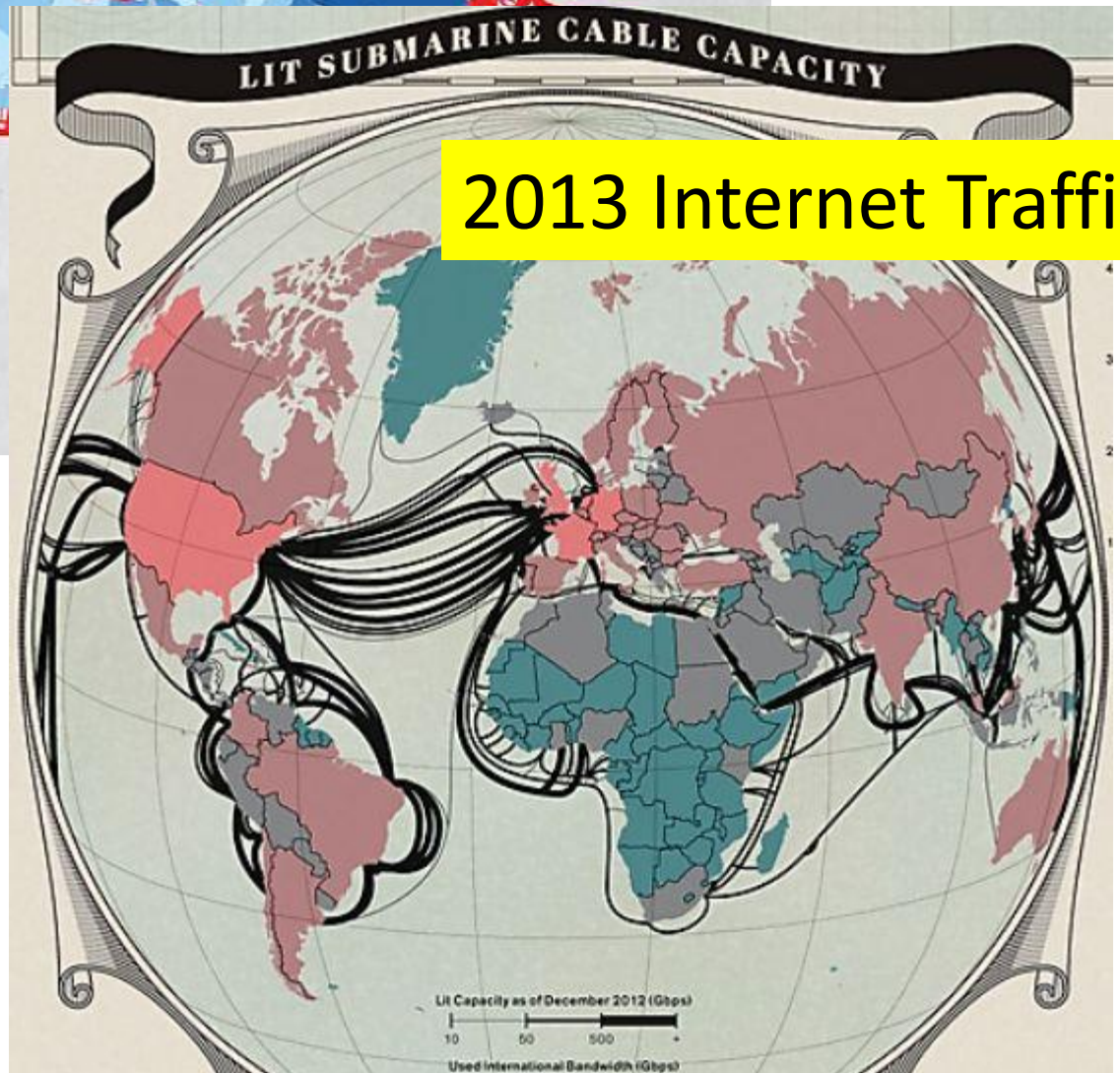
2010 Internet Traffic



2010 Internet Traffic



2013 Internet Traffic



[Submarine Cable Map]

https://www.visualcapitalist.com/wired-world-35-years-of-submarine-cables-in-one-map/