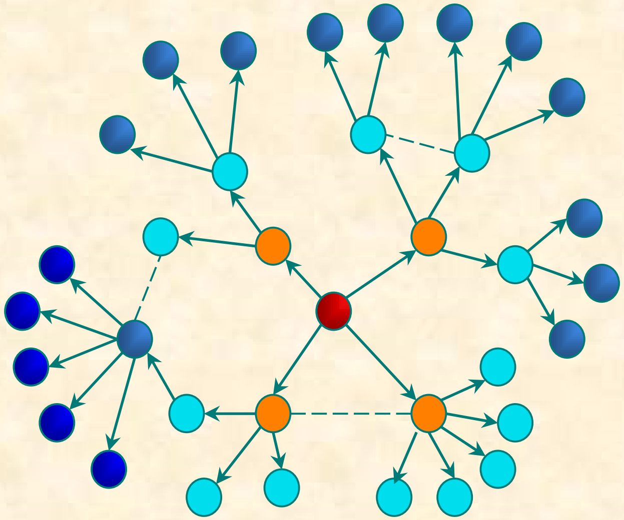
Complex Dynamical Networks:

Lecture 5: Spreading Dynamics

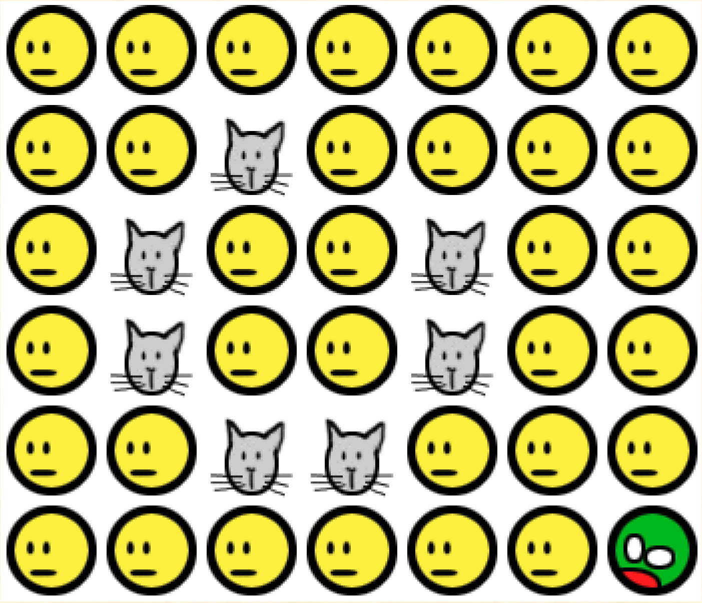
EE 6605

Instructor: G Ron Chen

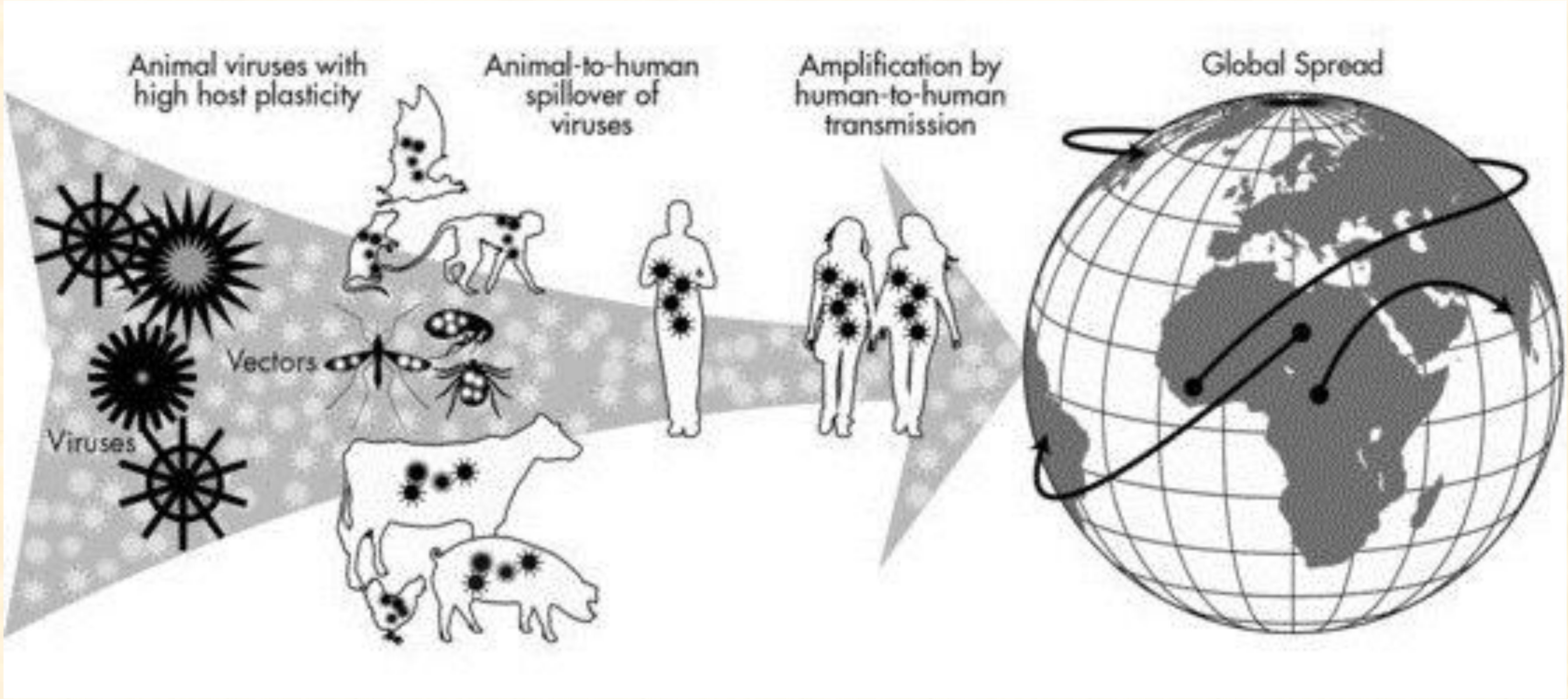
Epidemic Spreading



Typically through contact



Diseases Spreading
In Human Society

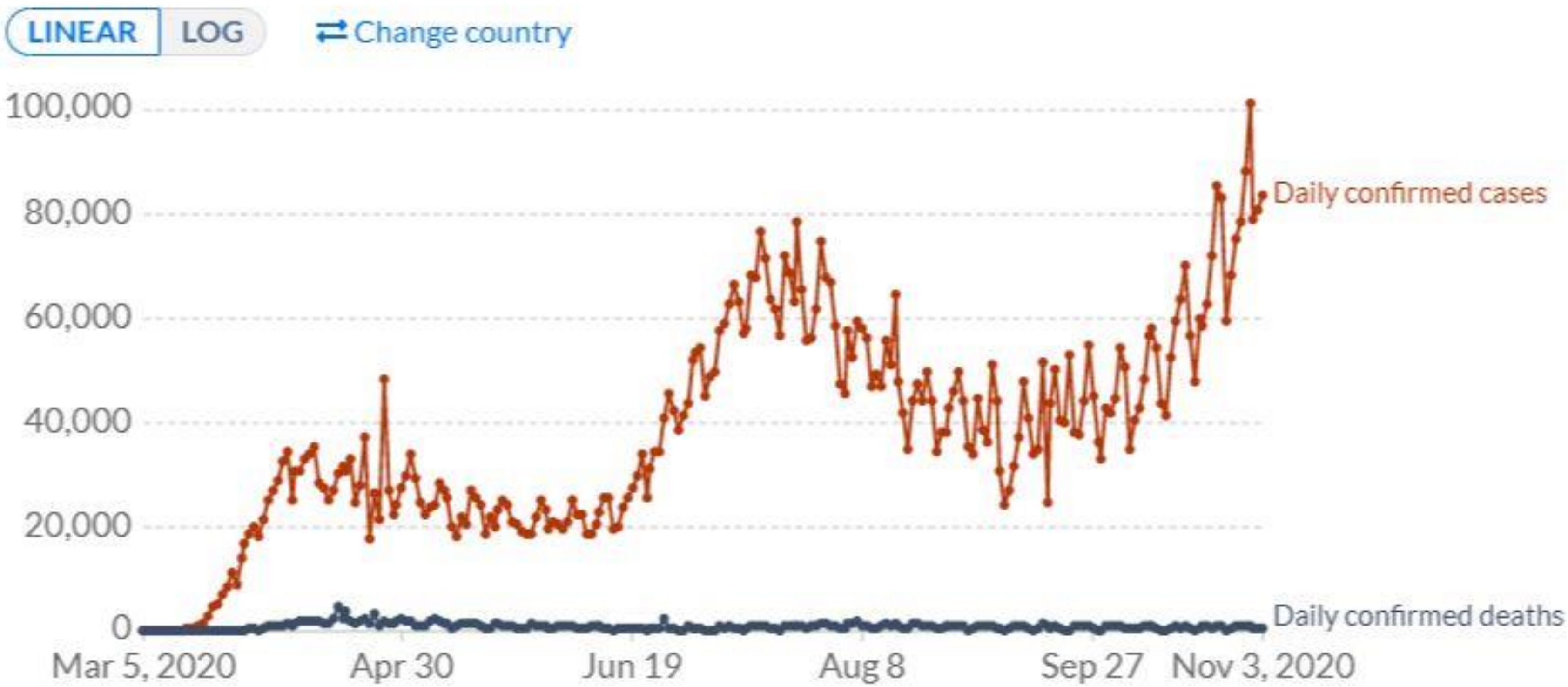



Coronavirus
Disease 2019
(COVID-19)
新冠肺炎
CDC

Daily confirmed COVID-19 cases and deaths, United States

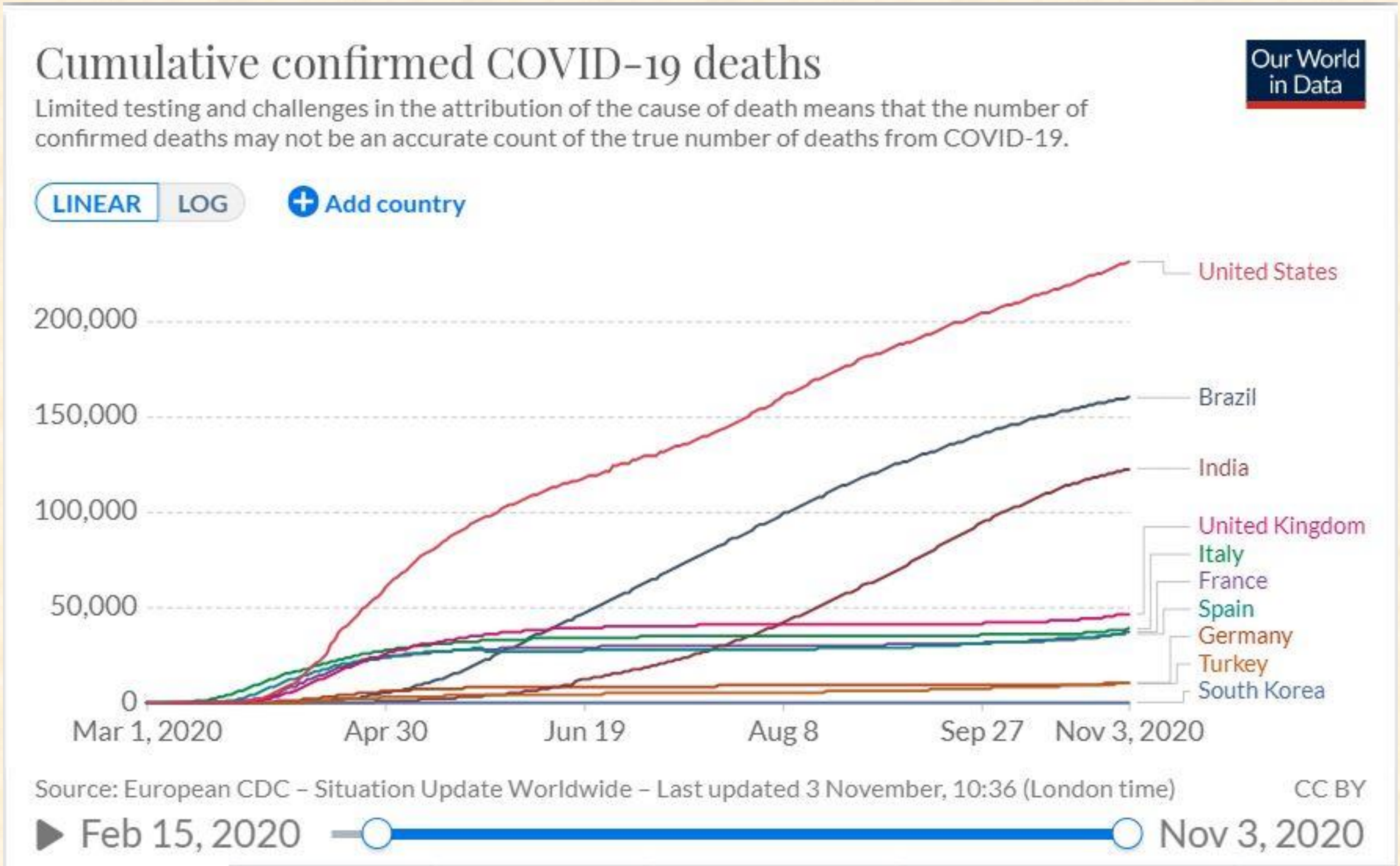
Our World in Data

The confirmed counts shown here are lower than the total counts. The main reason for this is limited testing and challenges in the attribution of the cause of death.



Source: European CDC – Situation Update Worldwide – Last updated 3 November, 10:36 (London time)
OurWorldInData.org/coronavirus •

Dec 31, 2019 Nov 3, 2020



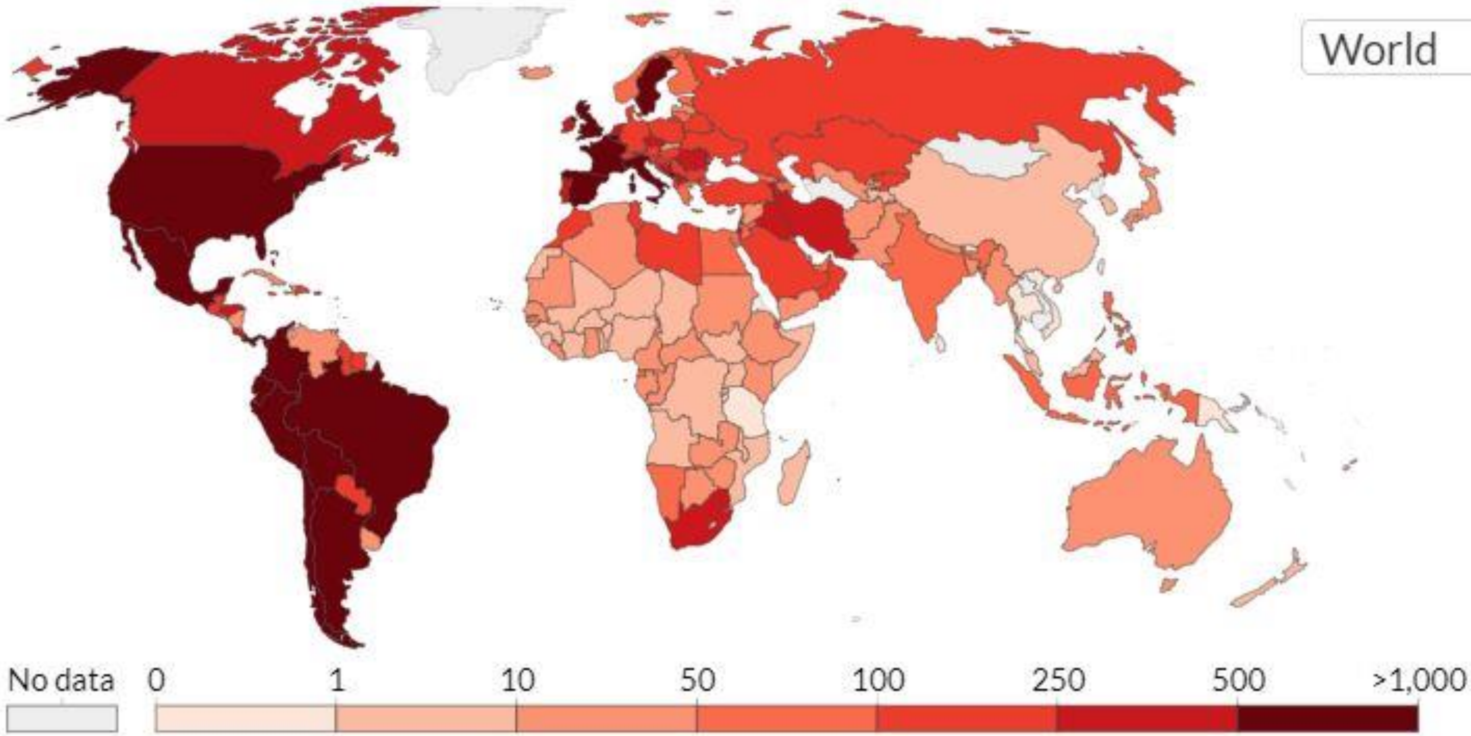
Cumulative confirmed COVID-19 deaths
Limited testing and challenges in the attribution of the cause of death means that the number of confirmed deaths may not be an accurate count of the true number of deaths from COVID-19.
Our World in Data
LINEAR
LOG
Add country
United States
200,000
150,000
100,000
50,000
0
Brazil
India
United Kingdom
Italy
France
Spain
Germany
Turkey
South Korea
Mar 1, 2020
Apr 30
Jun 19
Aug 8
Sep 27
Nov 3, 2020
Source: European CDC – Situation Update Worldwide – Last updated 3 November, 10:36 (London time)
CC BY
Feb 15, 2020
Nov 3, 2020

Cumulative confirmed COVID-19 deaths per million people, Nov 3, 2020

Our World in Data

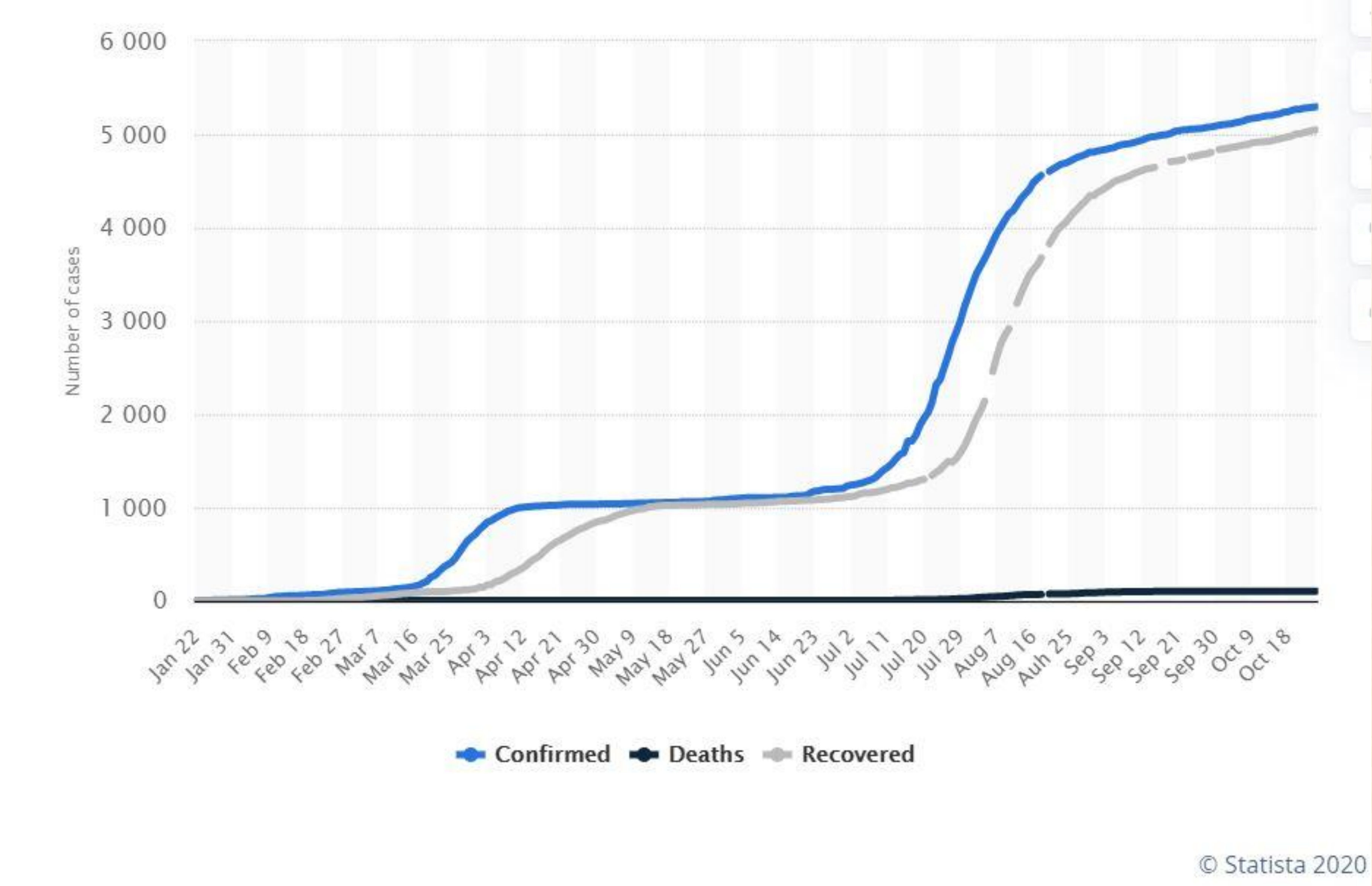
Limited testing and challenges in the attribution of the cause of death means that the number of confirmed deaths may not be an accurate count of the true number of deaths from COVID-19.

World



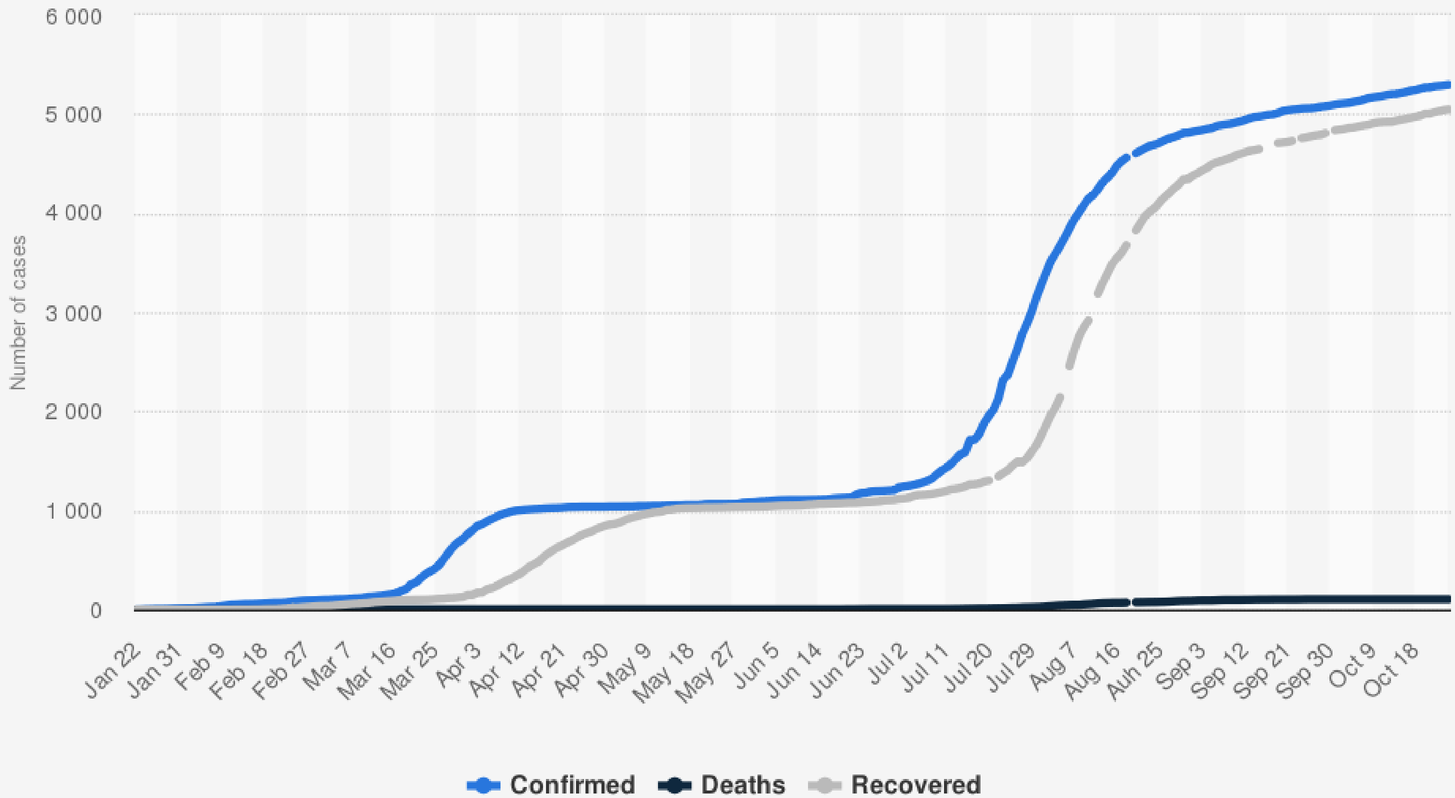
Source: European CDC – Situation Update Worldwide – Last updated 3 November, 10:36 (London time)

Jan 11, 2020 Nov 3, 2020


6 000
5 000
4 000
3 000
2 000
1 000
0
Number of cases
Jan 22
Jan 31
Feb 9
Feb 18
Feb 27
Mar 7
Mar 16
Mar 25
Apr 3
Apr 12
Apr 21
Apr 30
May 9
May 18
May 27
Jun 5
Jun 14
Jun 23
Jul 2
Jul 11
Jul 20
Jul 29
Aug 7
Aug 16
Auh 25
Sep 3
Sep 12
Sep 21
Sep 30
Oct 9
Oct 18
Confirmed
Deaths
Recovered
© Statista 2020

COVID-19 @ Hong Kong

Number of novel coronavirus COVID-19 cumulative confirmed, recovered and death cases in Hong Kong from January 30 to October 25, 2020



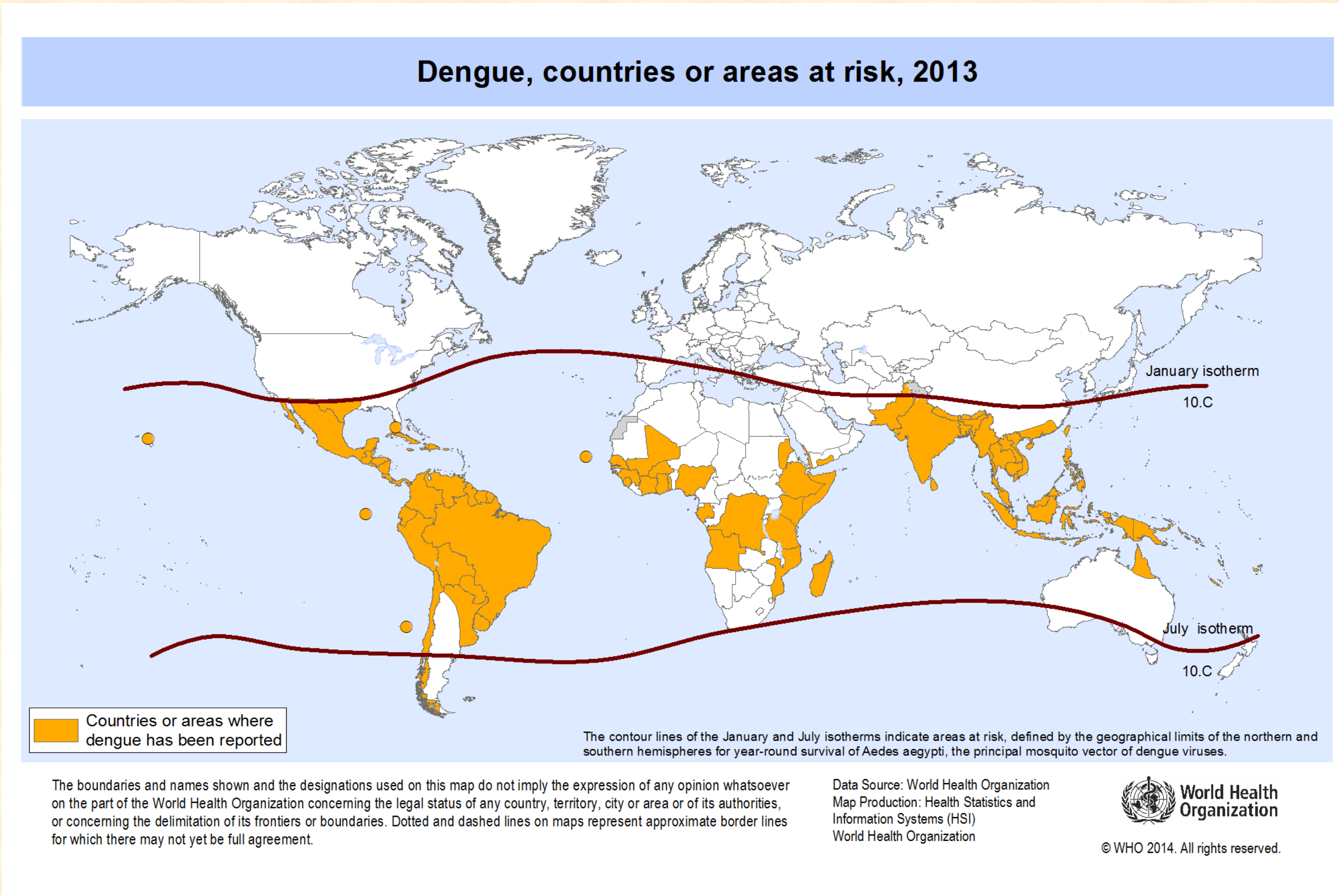
Sources
DXY.cn; Centre for Health Protection

Additional Information:
Hong Kong; DXY.cn; Centre for Health Protection; January 30 to October 25, 2020

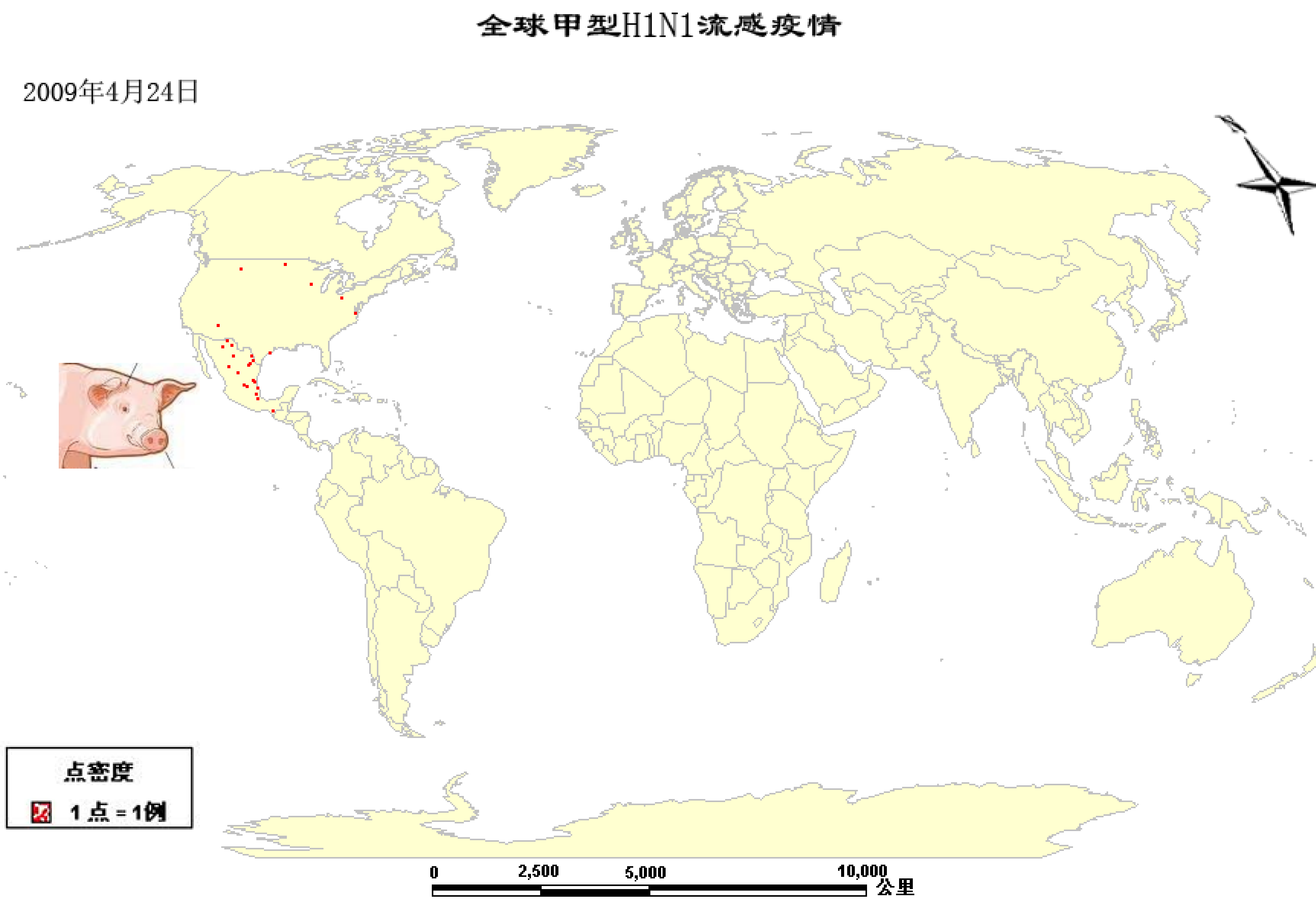
Example

Dengue Fever （登革熱）

Example
Dengue Fever



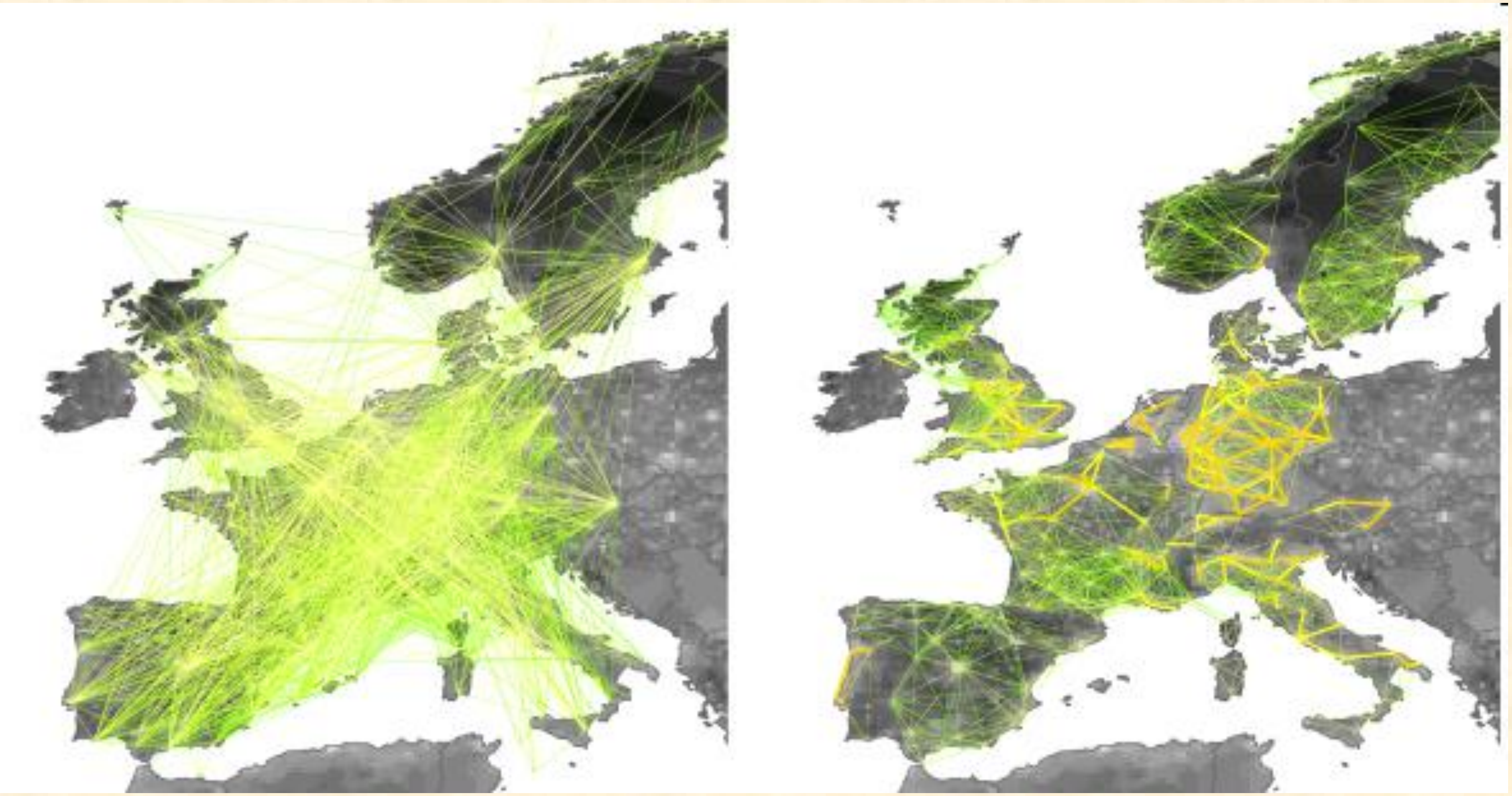
Example: H1N1




THE GLOBAL AVIATION NETWORK
DISEASE CAN SPREAD NEARLY
ANYWHERE WITHIN 24 HOURS


Bird
Flu

H1N1 Flu

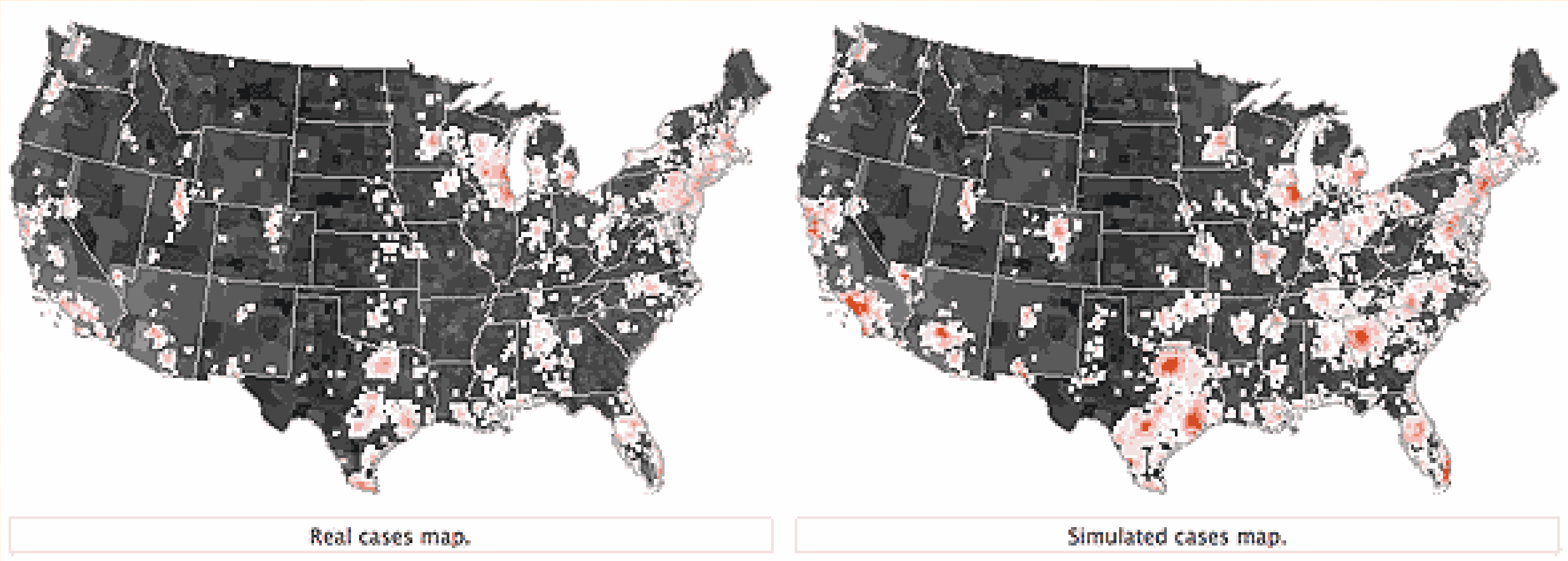


Airport network　　　Commuting network

Human Mobility Networks in Europe

Data

H1N1 Flu



Human Mobility Networks in USA

Data

Spanish Flu

1918 influenza pandemic (Jan. 1918 – Dec. 1920; known as Spanish Flu) was an unusually deadly influenza pandemic, the first of the two pandemics involving H1N1 influenza virus

It infected 500 million people around the world. About 50~100 million (3~5% of world population at the time) died

It was one of the deadliest Epidemics in human history

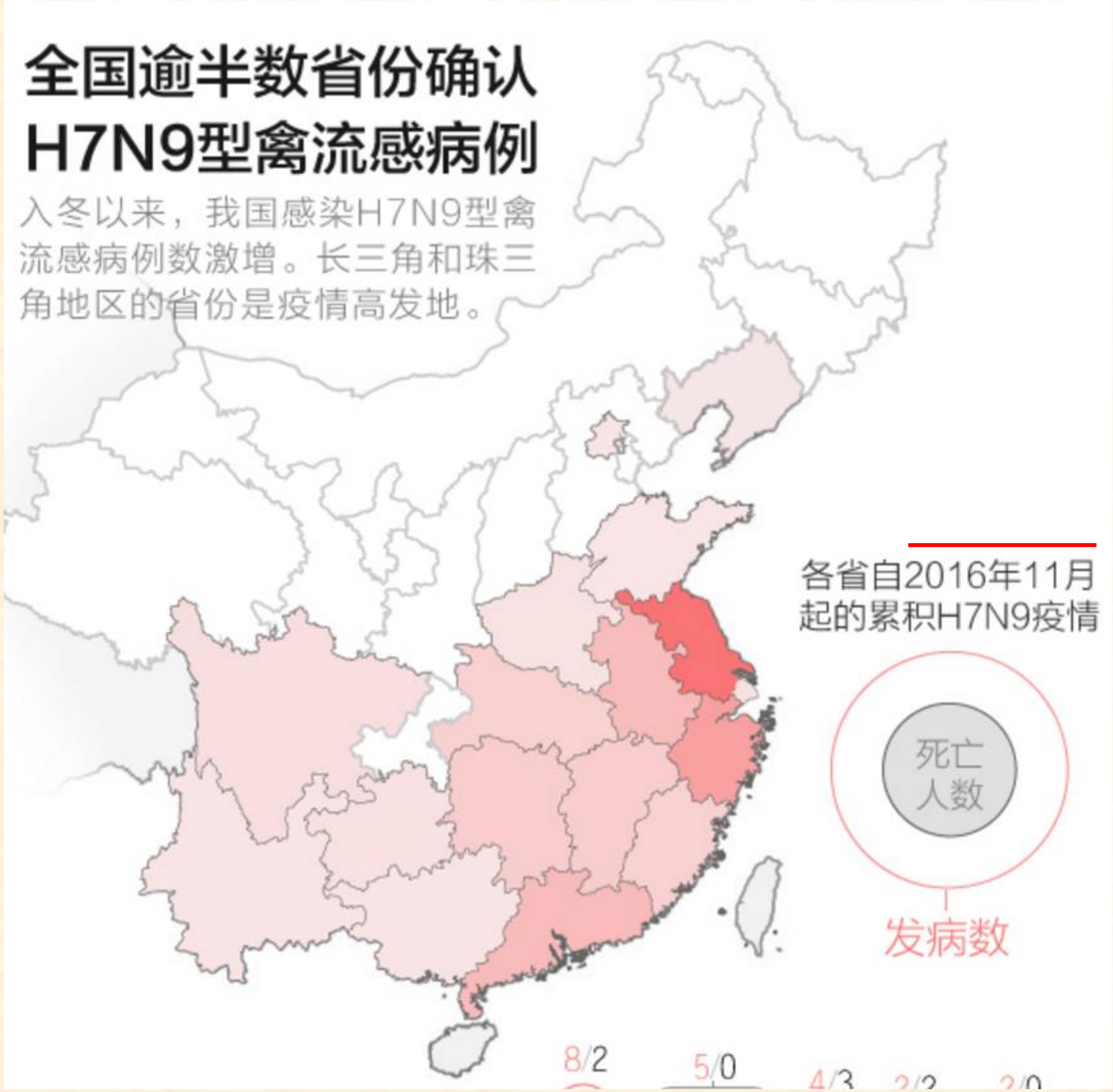
1920: World population
~ 1900 million

100m/1900m ~ 5% died !

Coming Again?

2015 In Hong Kong …

2016 In Mainland



2017 In Hong Kong

香港今夏流感死亡人数升至327人，流感活跃仍会持续数周

卫生署在新闻稿中指出，上述情况已超越2003年SARS时期造成299人死亡的数字。不过，同时强调，不同疾病的死亡人数不宜直接比较，以死亡率参考则较科学和客观。

港台来信 | 1小时前

2018 In India

印度甲型H1N1流感今年致1741人死亡，医生怀疑已变异

印卫生部门官员介绍，印政府已成立应急小组前往马哈拉施特拉邦调查。当地医生怀疑，甲型H1N1流感病毒可能已经变异。这种病毒最初通过动物传播，现在则由人向人传播。

绿政公署 | 2小时前

2019 In India

RAPID SPREAD OF SWINE FLU CLAIMS 226 LIVES IN INDIA

News Home | More from International

Thursday, February 7th, 2019 12:49pm

India has recorded an alarming spike in swine flu cases this year, with 226 people reported dead.

123rf

It has triggered a health alarm with more than 6,700 cases reported across the country.

Most of the cases are reported from the northern Indian states of Rajasthan, Delhi and Haryana.

2019 In Hong Kong …

醒晨快報：流感肆虐 累計死亡人數增至81人

2019-01-25

Like 12 Share

A A A

● 港聞

▸ 踏入冬季流感高峰期後，本港累計感染流感死亡人數增至81人。據最新統計數字，成人嚴重流感個案增加11宗至185宗，當中超過一半屬65歲或以上人士，兒童嚴重流感維持13宗，全部是甲型流感。

表 3　自 2003 年起呈報給世衛 / 國家衛健委的確診人類感染甲型禽流感(H5N1)個案（根據發病日期）[8]

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	總數
個案	4	46	98	115	88	44	73	48	62	32	39	52	145	10	4	0	0	860
死亡	4	32	43	79	59	33	32	24	34	20	25	22	42	3	2	0	0	454
死亡率	100%	69.6%	43.9%	68.7%	67.0%	75.0%	43.8%	50.0%	54.8%	62.5%	64.1%	42.3%	29.0%	30.0%	50.0%	0%	0%	52.8%

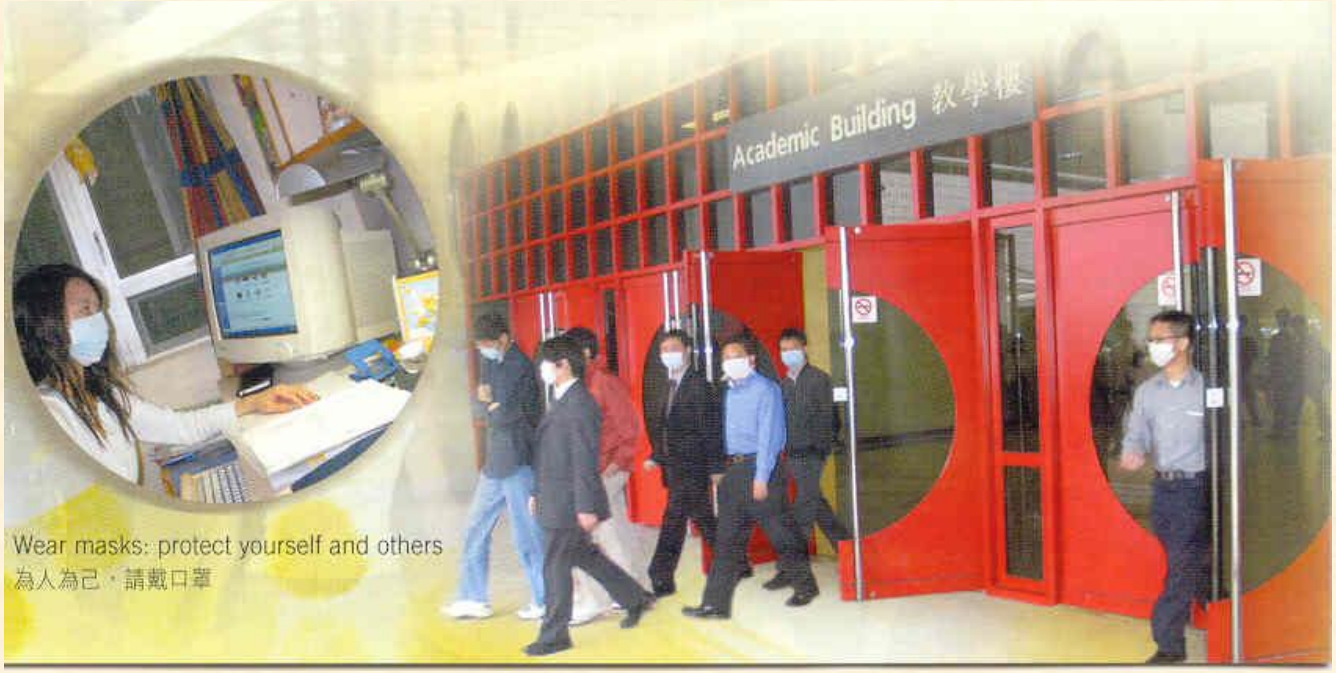
Recall History

Epidemics in Hong Kong

- Bubonic Plague 鼠疫 (1894–1929)
- H1N1 (1918-1919)
- H2N2 (1957-1958)
- H3N2 “Hong Kong flu” (1968-1969)
- H1N1 Influenza (2009)
- SARS (2003)
- COVID-19 (2019-2020)

Recall History

Epidemic Spreading

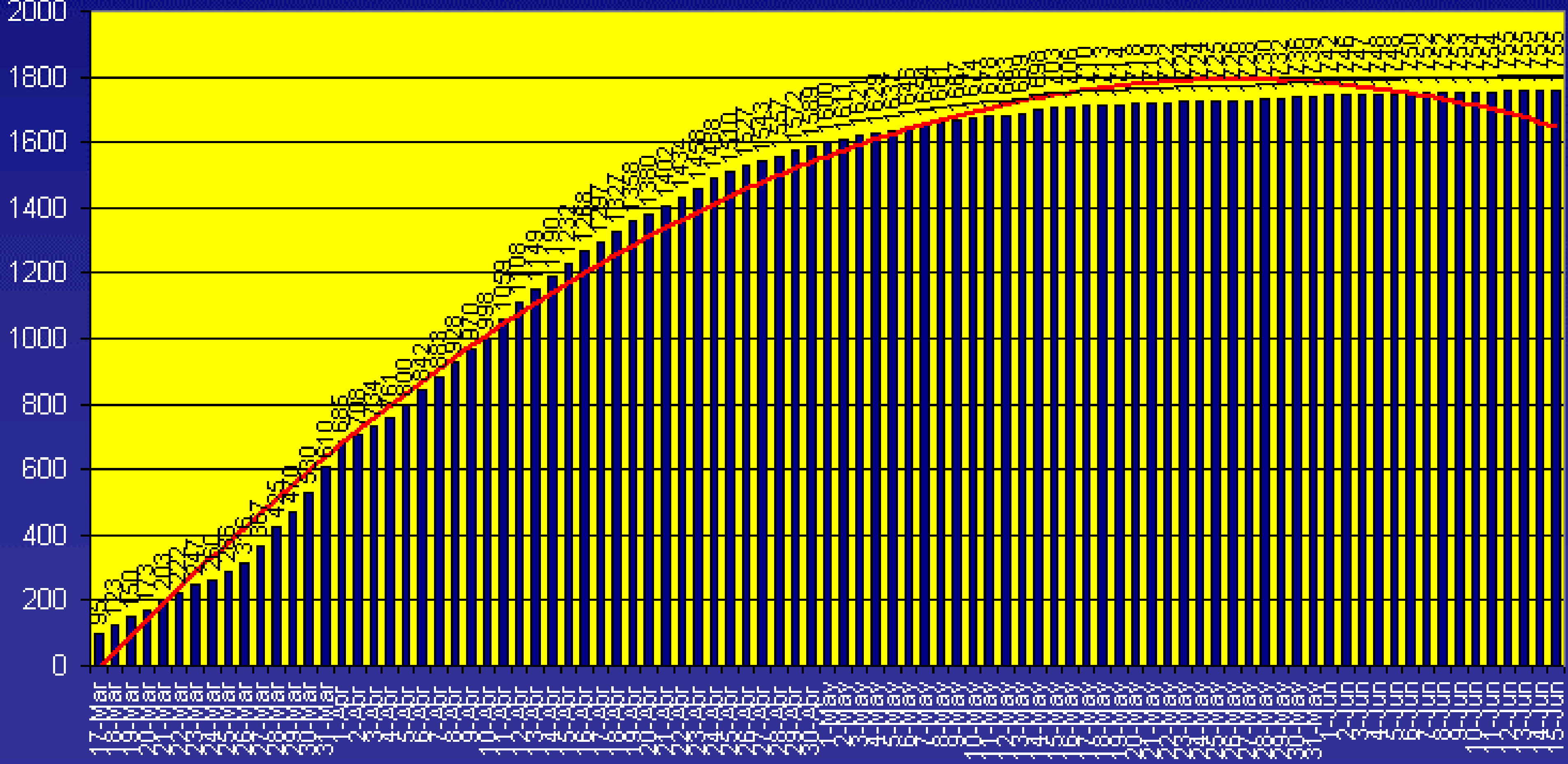


CityU of HK, 2003

SARS — First Major New Infectious Disease of the 21st Century

- Severe Acute Respiratory Syndrome (SARS) is a highly infectious and potentially lethal atypical form of pneumonia that begins with deceiving common flu-like symptoms
- On 16 November 2002, the first known case of SARS was discovered in Guangdong province in southern China
- The number of reported SARS cases has increased exponentially, prompting the World Health Organization (WHO) to issue a global alert on 12 March 2003

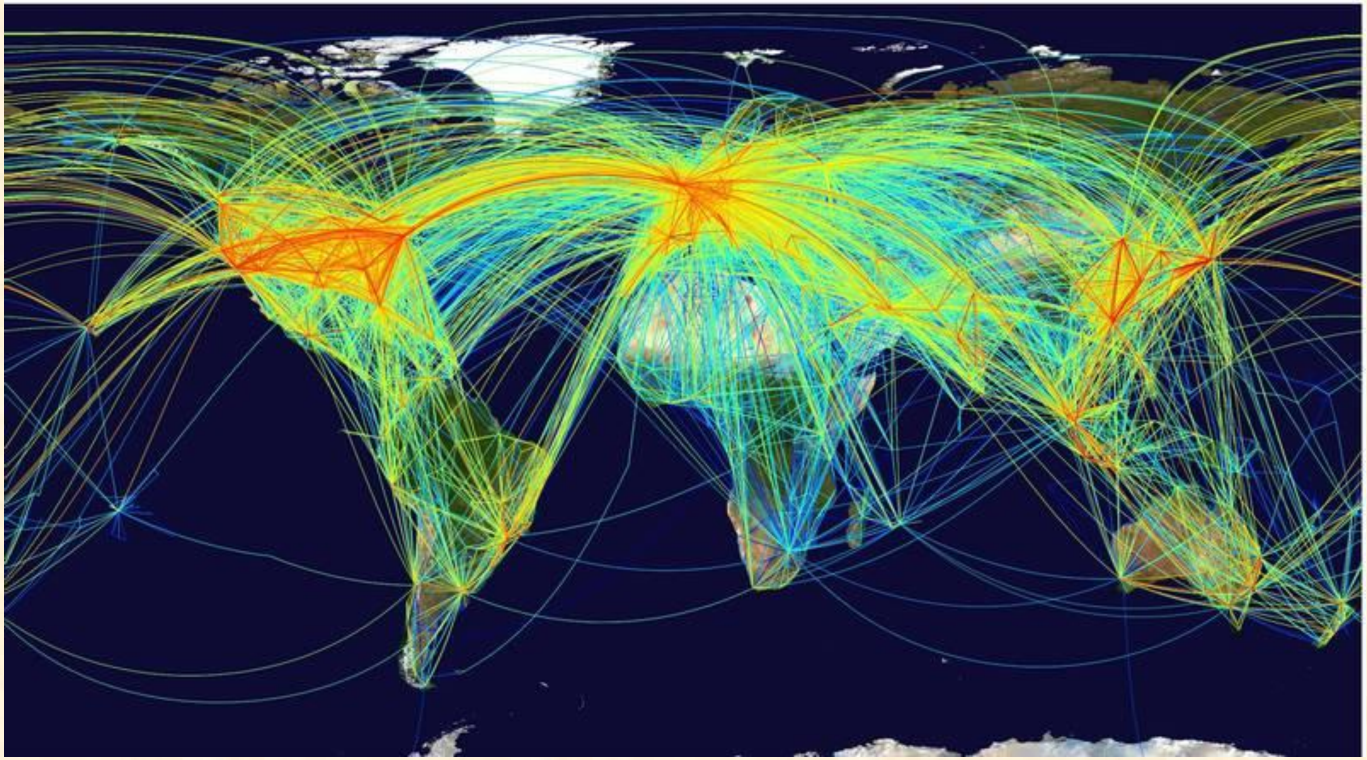
Number of Hospitals Admissions of SARS in Hong Kong Since March 17 (Figures as published by WHO)



Epidemic Spreading

Typically through contact …

Human Travel Map:

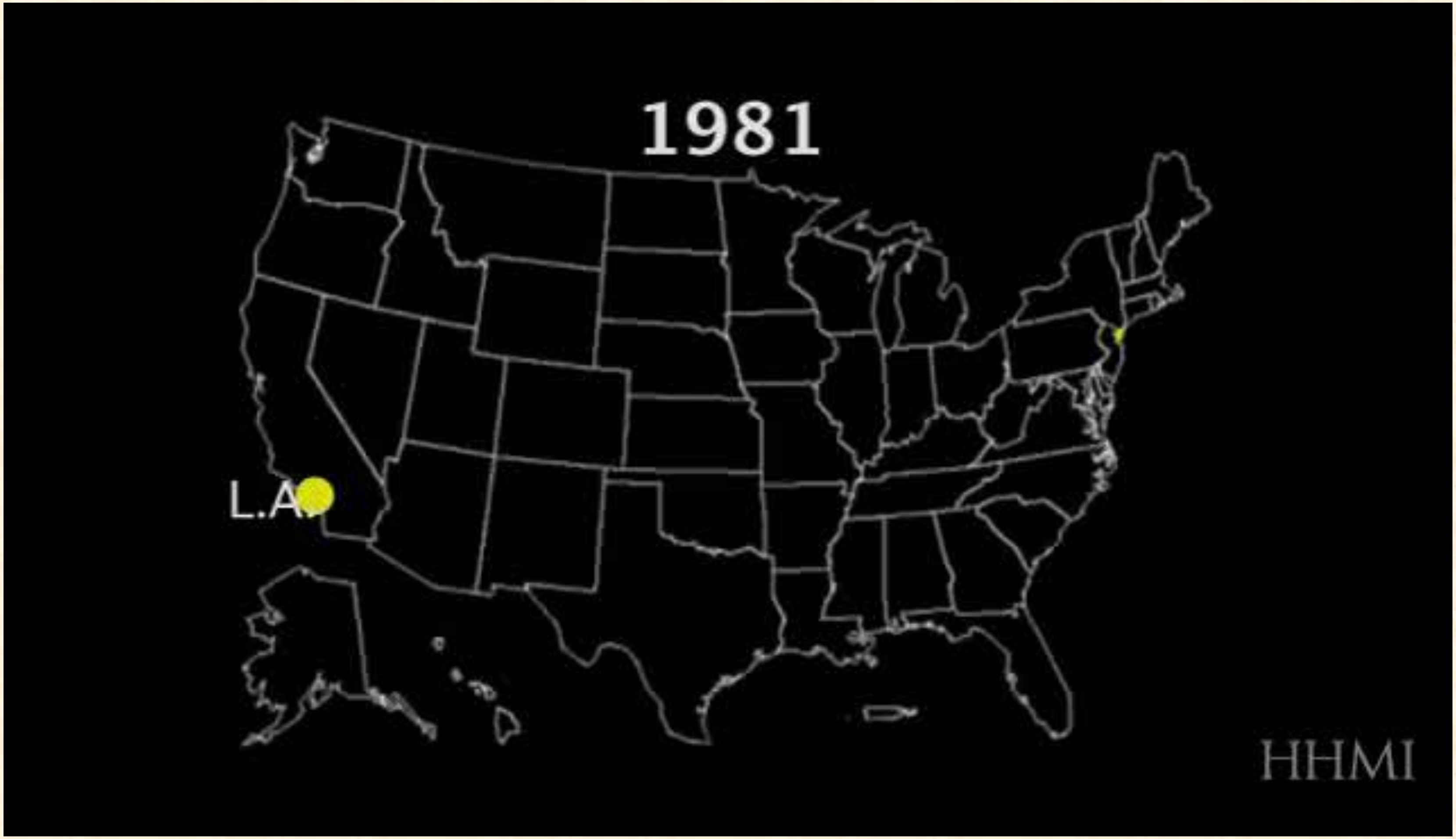


Epidemic Spreading

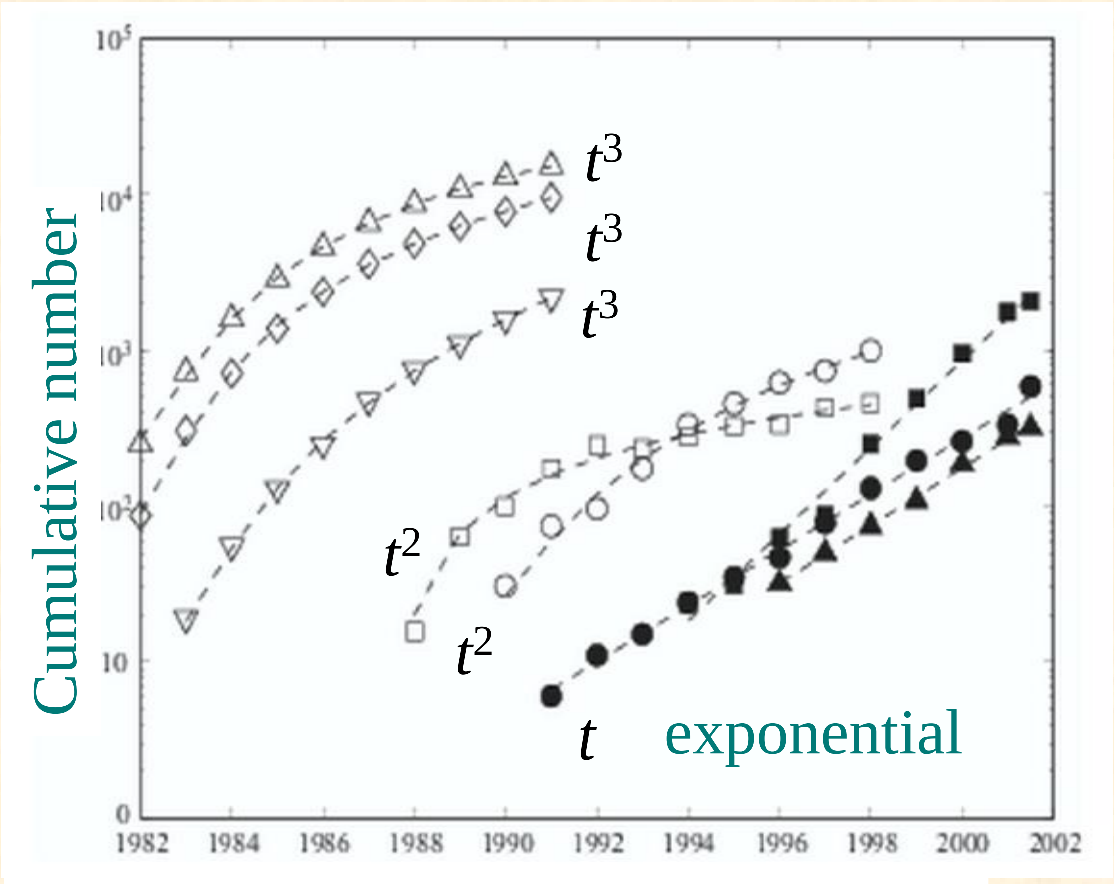
Human Travel Map:

春运

AIDS in USA



Example: AIDS Epidemics



t (years)

△ New York - Hom
▽ New York - Het
◇ San Francisco - Hom

○ South Africa
□ Kenya

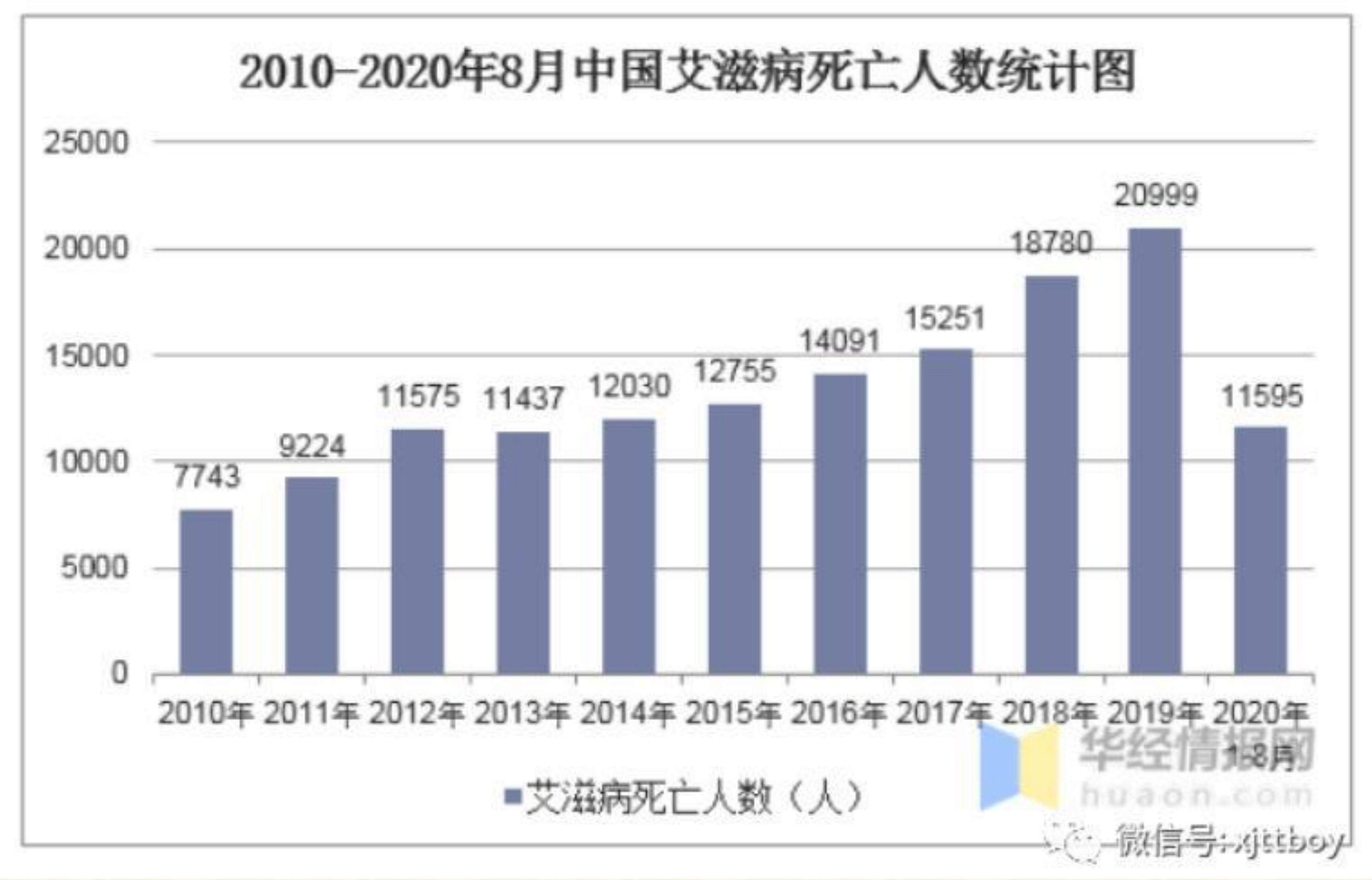
▲ Georgia
■ Latvia
● Lithuania

Szendroi & Czanyi, Proc. Royal Society of London, B 2004

In China ...

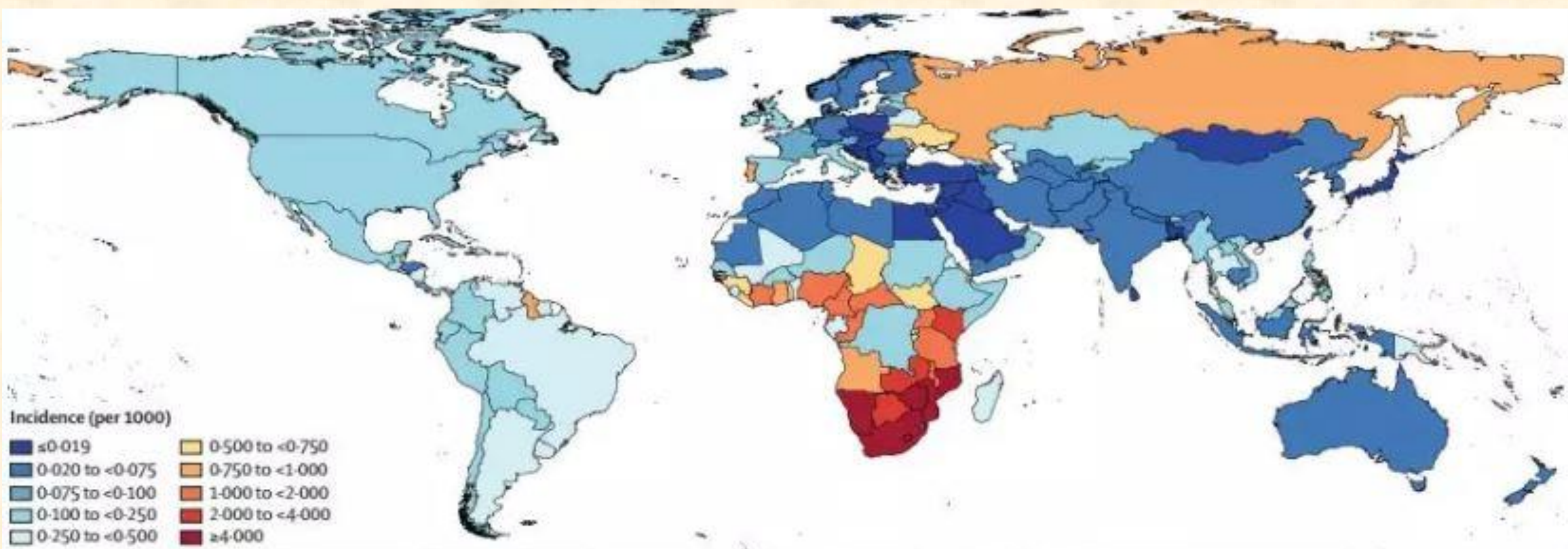

2010-2020年8月中国艾滋病发病数量统计图
80000
70000
60000
50000
40000
30000
20000
10000
0
15982
20450
41929
42286
45145
50330
54360
57194
64170
71204
39349
2010年
2011年
2012年
2013年
2014年
2015年
2016年
2017年
2018年
2019年
2020年
1-8月
艾滋病发病数量（例）
华经情报网
huaon.com
微信号: xjttboy

In China …



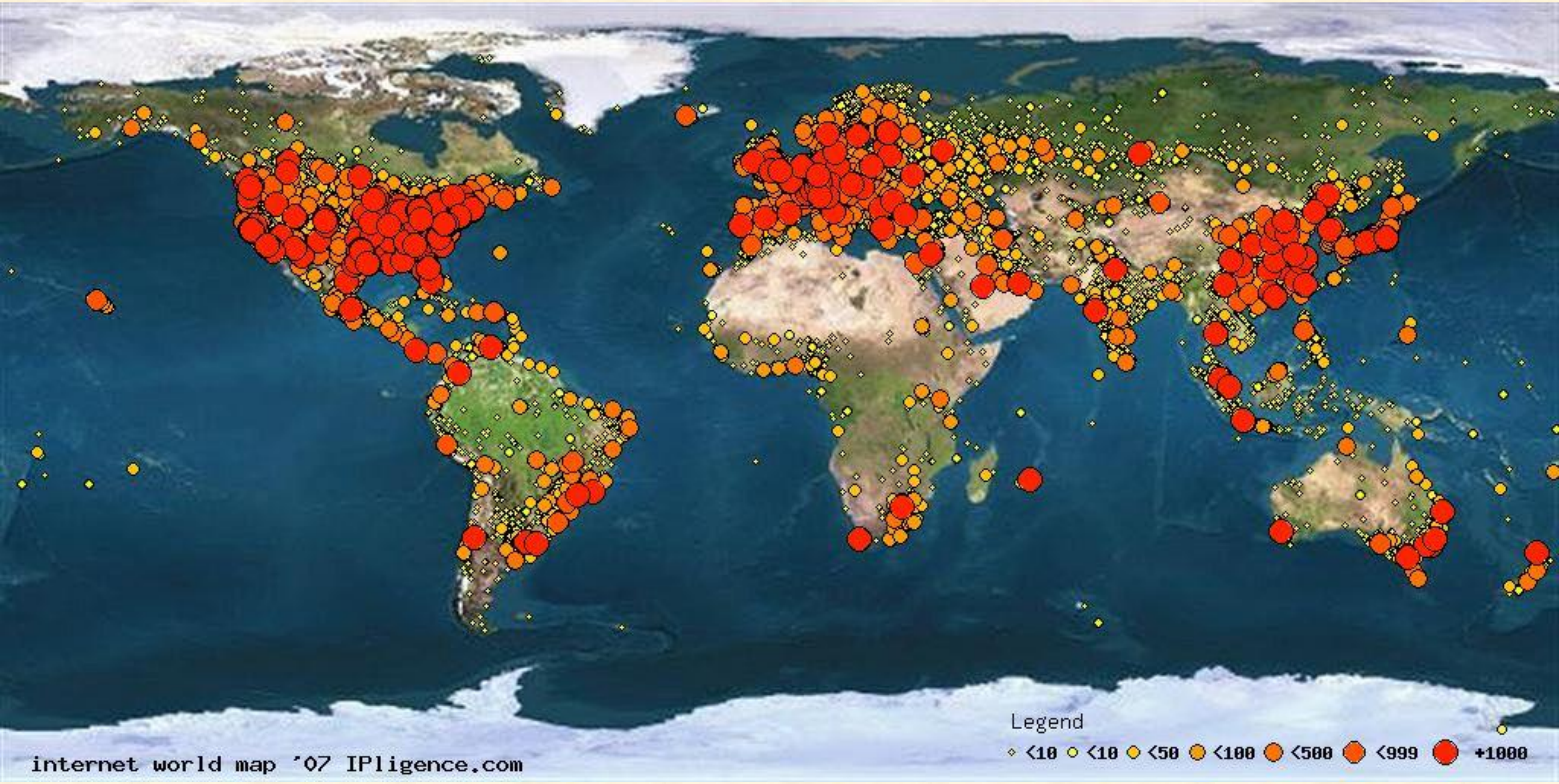
2010-2020年8月中国艾滋病死亡人数统计图
25000
20000
15000
10000
5000
0
7743
9224
11575
11437
12030
12755
14091
15251
18780
20999
11595
2010年
2011年
2012年
2013年
2014年
2015年
2016年
2017年
2018年
2019年
2020年 1-8月
艾滋病死亡人数（人）
华经情报网
huaon.com
微信号: xjttboy

In China … and in the World



Internet

Computer Viruses



Computer Virus Spreading

- The first virus capable of infecting PCs was perhaps the Brain virus developed in Pakistan in 1986.
- I-Love-You bug began in Philippines on May 4, 2000, and spread across the world in one day (traveling through Hong-Kong to Europe then to USA), infecting more than 78 million computers worldwide in just 4 days, i.e., about 10% of all computers connected to the Internet, and causing about US$5.5 billions in damage.
- It was estimated that there were more than 48,000 identified viruses on the Internet worldwide in year 2000 alone.
- In 2000-2001, well-known viruses: Lover Letter, Nimda, and Sircam …
- It was estimated that more than 80% computers were attacked by viruses in China in 2004.
- Also in 2004, the infamous Worm Sasser attacked several hundred thousands of computers over the world within just a couple of weeks.
- In 2009, Conficker (worm) remotely installs software on infected machines.
- …… Many other examples … still today!

Computer Virus Spreading

Hong Kong

腦毒Nimda突襲全球 港中招

接獲近50入侵報告 破壞力更甚「紅碼」

市場突變

繼電腦病毒「紅碼」（Code Red）肆虐全球後，另一網絡病蟲「W32.Nimda.A.@mm」昨日再次廣泛損害全球網絡，本港亦難幸免。綜合各有關機構匯報，昨共有近50個本港企業受襲報告，情況令人關注，電腦界人士稱，Nimda「娜坦」較先前的「紅碼」破壞力更甚，由網絡伺服器以致商業及家用電腦都廣泛受到破壞。

本地一銀行「中毒」

專為30萬中小企提供協助的本港電腦保安事故協調中心（CERT），昨日便接獲12宗求助個案，國際知名互聯網保安機構趨勢科技及Symantec分別亦有逾30個本港機構及最少4名大型機構客戶的網絡「中毒」報告。據Symantec稱，其中一家為本地銀行。

Symantec旗下的安全機制應變中心將該病毒定為危害指數達4級的病蟲。Symantec中國及香港執行總裁鄭裕慶稱，本地不少大型機構均報稱網絡受病毒感染，其中包括銀行、傳媒及跨國企業，雖然接獲求助個案不多，但估計受影響的機構數以百計。目前除蟲措施已積極進行，但截至昨午尚未完全解決。

損伺服器更改權限

該病毒主要利用微軟IE、IIS伺服器及Outlook的漏洞進行入侵及傳播，損害伺服器並開放網絡共享，及更改系統管理者權限。

趨勢科技香港總經理陸仰星表示，單是昨日早上該公司已接獲逾30個本港受影響企業的報告，當中業務性質由電訊及資訊科技企業以至金融及主要投資銀行。他指Nimda致命之處在於其可經多種如電郵、網絡文件夾及IIS網絡伺服器等渠道散播。

該公司已為客戶提供修補程式及病毒最新資料，至今病毒感染已全面修復。

另外，CA保安方案商業經理Ian Hameroff指出，Nimda擁有新增能影響網絡伺服器、商業及家庭電腦用家的能力，這是前所未見。要防範同類的病毒威脅，便要對質素參差的應用程式提高警覺，作出政策評估，以加強互聯網保安方案的防禦。

網絡保安開支不足

鄭裕慶認為，本港的網絡保安意識已較前提高，但基於經濟不景，企業目前仍不太願意投入太多資金於網絡保安上，但預期當經濟好轉，企業必意識到大增保安支出的重要性。

若公司被襲可瀏覽以下有關網址：

相關網址 趨勢科技：www.antivirus.com www.trendmicro.com.hk
生產力局：www.hkpc.org

●本港昨接獲入侵的報告，快加強網絡保

[10 Most Dangerous Computer Viruses of All Time]

More Examples …

In 2008, for example, security software maker “Symantec in Mountain View” in California detected 1.6 million new threats from computer viruses and other malicious software (In 2007, only 600,000 or so)

Such attacks will become more common and more sophisticated in the future

Statistically, unsolicited junk e-mails (‘spams’) accounts for about 90–95% of all e-mails sent

Such trash will become more common and more annoying in the future [Computer Viruses]

Computer Viruses and Worms

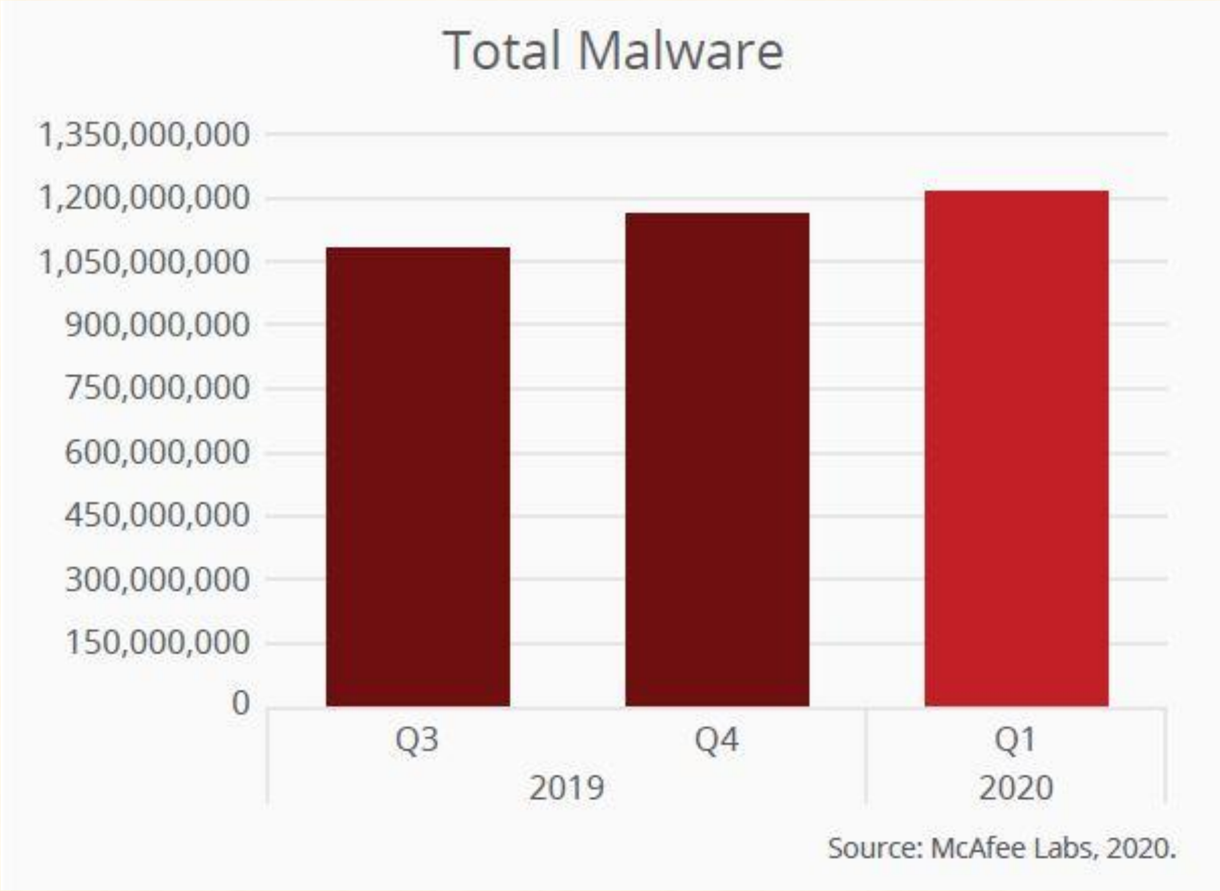
- Computer viruses are usually referred to as some small computer programs that can reproduce themselves by infecting other programs and computers, which continuously grow and spread out.
- When a virus is active inside a computer, it is able to copy itself in many different ways into the codes of some programs of the computer.
- When the infected computer program is run into another computer, typically the code of the virus is executed first thus continues to infect other programs in the new computer.
- This process repeats endlessly, leading to the collapse of a local or even global network of computers eventually, causing tremendous technological and economical disasters.

Computer Viruses and Worms

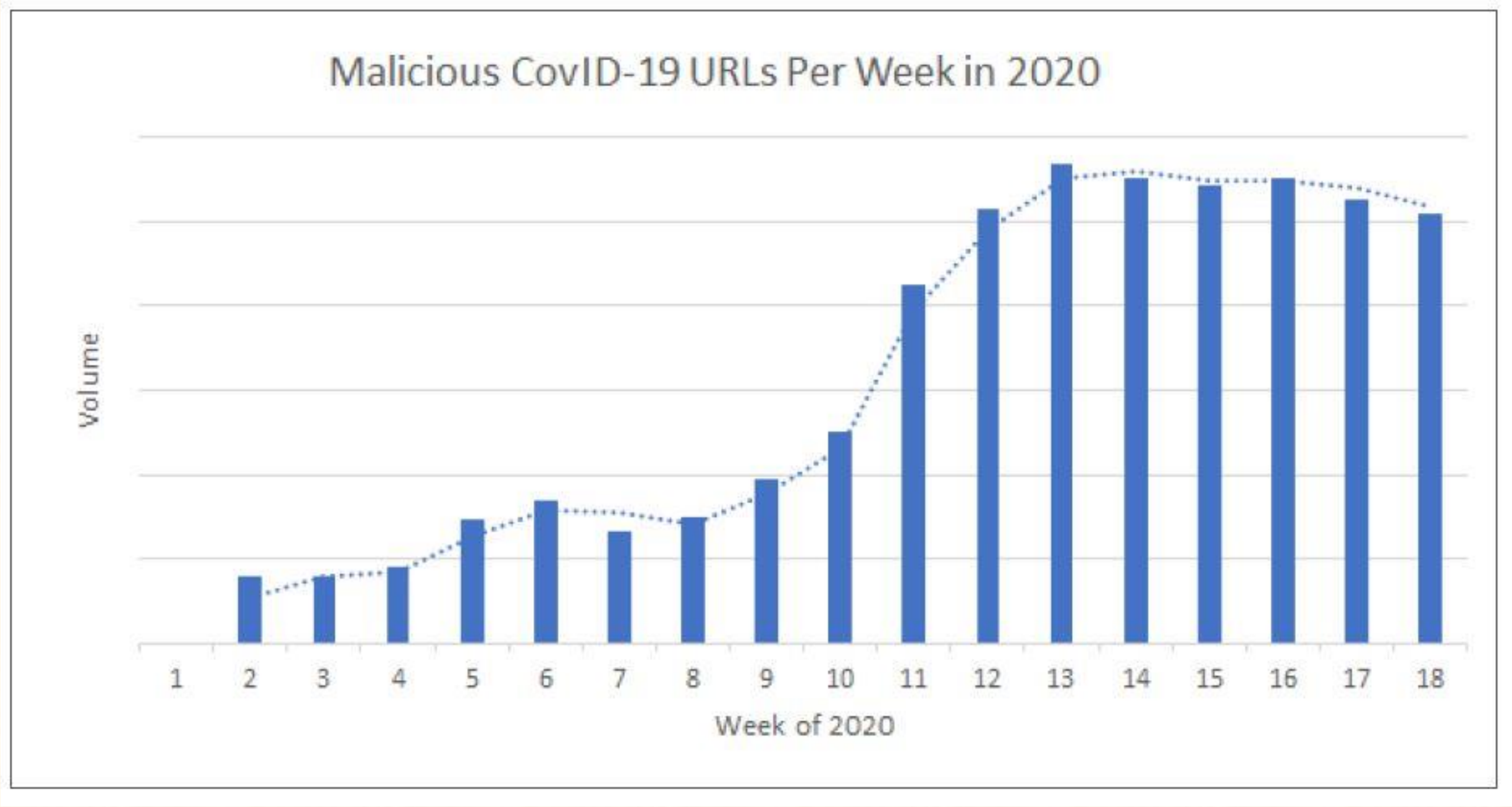
Major computer viruses may be roughly classified into:

- Boot-sector viruses, which infect the boot sectors of floppies and hardware devices
- File viruses, which infect application programs
- Macro viruses, which infect data files directly
- Hybrid types of viruses, in a certain combination of the above basic ones, which infect some special technologies or applications such as Java, ActiveX, and HTML, etc.
- Trojan horses are malicious file or program, which can make copies of themselves, steal information, or harm their host computer systems

Computer Viruses



Malicious Emails and URLs referring to CODVID-19



Data: McAfee Labs report

作者：张建新 来源：新华网 发布时间：2014-3-2 12:13:33 选择字号：小 中 大

Trojan

可利用DOS命令进行自我删除的恶意木马变种被发现

国家计算机病毒应急处理中心通过对互联网的监测发现，近期出现一种恶意木马程序变种Ｔｒｏｊａｎ＿Ｓｗｉｓｙｎ．ＣＦＤ。该变种在对操作系统进行入侵感染破坏后，利用ＤＯＳ命令进行自我删除，阻止防病毒软件对其进行查杀。

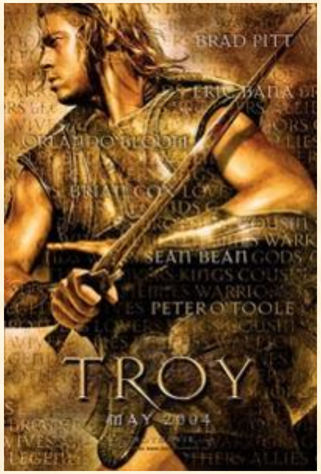
该变种运行后，会自身复制到受感染操作系统指定文件夹下，重命名为可执行文件，设置其属性为“只读”、“隐藏”。与此同时，该变种会创建进程快照，查找受感染操作系统中指定文件名进程，如发现该文件进程正在运行，则弹出对话框，显示防病毒软件正在升级的虚假提示信息。

另外，该变种会迫使受感染操作系统主动访问指定的恶意Ｗｅｂ网址，最终变种可以获取受感染操作系统的本机信息（诸如：计算机名、操作系统版本、处理器类型、内存大小等），随即发送到恶意攻击者指定的Ｗｅｂ服务器上，致使受感染操作系统接受远程恶意代码指令。

针对已经感染该恶意木马程序变种的计算机用户，专家建议立即升级系统中的防病毒软件，进行全面杀毒。对未感染的用户建议打开系统中防病毒软件的“系统监控”功能，从注册表、系统进程、内存、网络等多方面对各种操作进行主动防御。

“Achilles' Heel”

Corfu, Greece



2004 film: TROY

特洛伊

Trojan Horse

木马

Story

Robustness and Fragility of Scale-Free Networks

"Achilles' heel"

R. Albert, H. Jeong, A. L. Barabasi, Nature, 406, 387-482 (2000)

In Greek mythology, when Achilles was a baby, his mother Thetis took him to the River Styx, which was supposed to offer powers of invulnerability, and dipped his body into the water. But as mother held Achilles by the heel, his heel was not washed over by the water of the magical river. Achilles grew up to be a man of war who survived many great battles. On one day, a poisonous arrow shot at him was lodged in his heel, killing him shortly after.

Computer Viruses and Worms

- The first computer worm was created in 1988 by the now-infamous Robert Tappan Morris
- On November 2, 1988, Robert Morris, Jr., a graduate student in Computer Science at Cornell, wrote an experimental, self-replicating, self-propagating program called a *worm* and injected it into the Internet.
- Computer worms are most aggressive cyber-organisms (larger and more sophisticated programs) with much more powerful abilities to attack computers.
- They shut down the Internet e-mail systems that got clogged with infected e-mails propagating from the worm.
- A worm is capable of sending itself to all e-mail addresses in the e-mail address book of the computer, which received an infected e-mail. This makes worms very effective in spreading over the Internet.

Incidents on Facebook

<< See all Yahoo! Tech News

Koobface, Other Worms Target Facebook Friends (NewsFactor)

Posted on Thu Mar 5, 2009 11:31AM EST

Add articles about technology to your My Yahoo! MY Y!

- As Facebook works to make itself more relevant and timely for its growing member base with a profile page makeover, attackers seem to be working overtime to steal the identities of the friends, fans and brands that connect though the social-networking site.

Indeed, Facebook has seen five different security threats in the past week. According to Trend Micro, four new hoax applications are attempting to trick members into divulging their usernames and passwords. And a new variant of the Koobface worm is running wild on the site, installing malware on the computers of victims who click on a link to a fake YouTube video.

The Koobface worm is dangerous. It can be dropped by other malware and downloaded unknowingly by a user when visiting malicious Web sites, Trend Micro reports. When attackers execute the malware, it searches for cookies created by online social networks. The latest variant is targeting Facebook, but earlier variants have also plagued MySpace.

Facebook Malware

Malware Worm Spreading on Facebook – 45,000 Passwords Stolen So Far

January 5, 2012

in Internet Safety & Privacy

Like 7,597 people like this.

Seculert issued a warning today that the Ramnit worm, which has traditionally targeted financial login credentials, is now targeting Facebook users. At the time

Incidents on Facebook

May 29, 2015 — Leave a comment 0

Warning: New virus attacks routers, steals Facebook passwords

By Komando Staff, Komando.com

5,000 cyber-attacks were attempted against one Irish hospital in just 24 hours

The HSE decided to cut external communications, including emails and server connections, on Friday.

7 hours ago 14,817 Views 17 Comments Share 17 Tweet Email 1

THE HSE SAYS it has found 5,000 cyber-attack attempts on one major Irish hospital between Friday and Saturday.

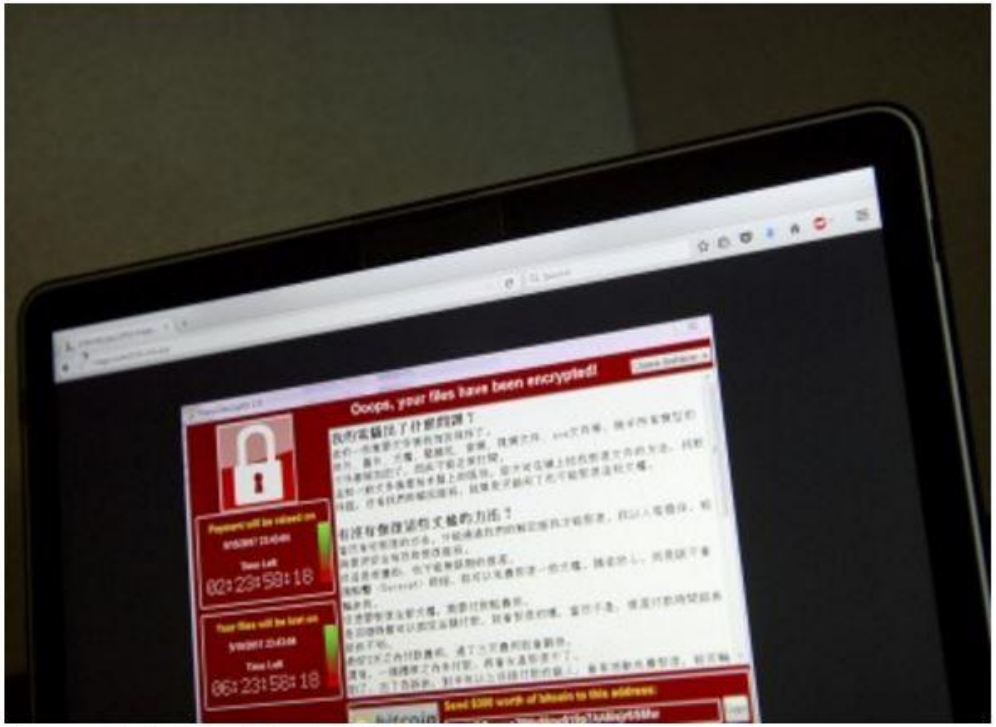


Image: Mark Schiefelbein/PA images

The executive says it is on course to re-connect services to the outside world following a four-day-long disconnection due to the WannaCry ransomware virus.

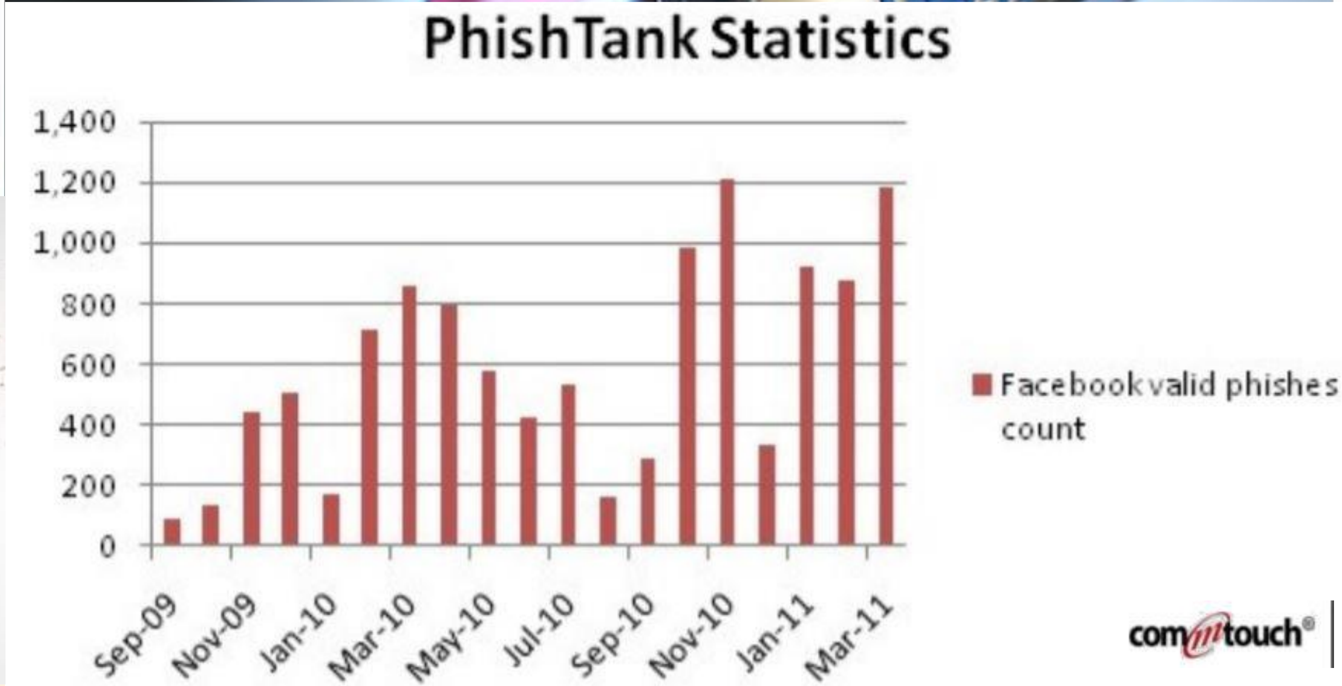
While the HSE said that medical services were minimally disrupted, it said that a number of computers had the potential to be held to ransom.

threatpost

Years-Long 'SilentFade' Attack Drained Facebook Victims of $4M

Author:
Lindsey O'Donnell

October 2, 2020
/ 11:17 am



网络安全问题

2016 年10月21日，美国东海岸出现了大面积互联网断网事件，大半个美国的网络服务瘫痪。

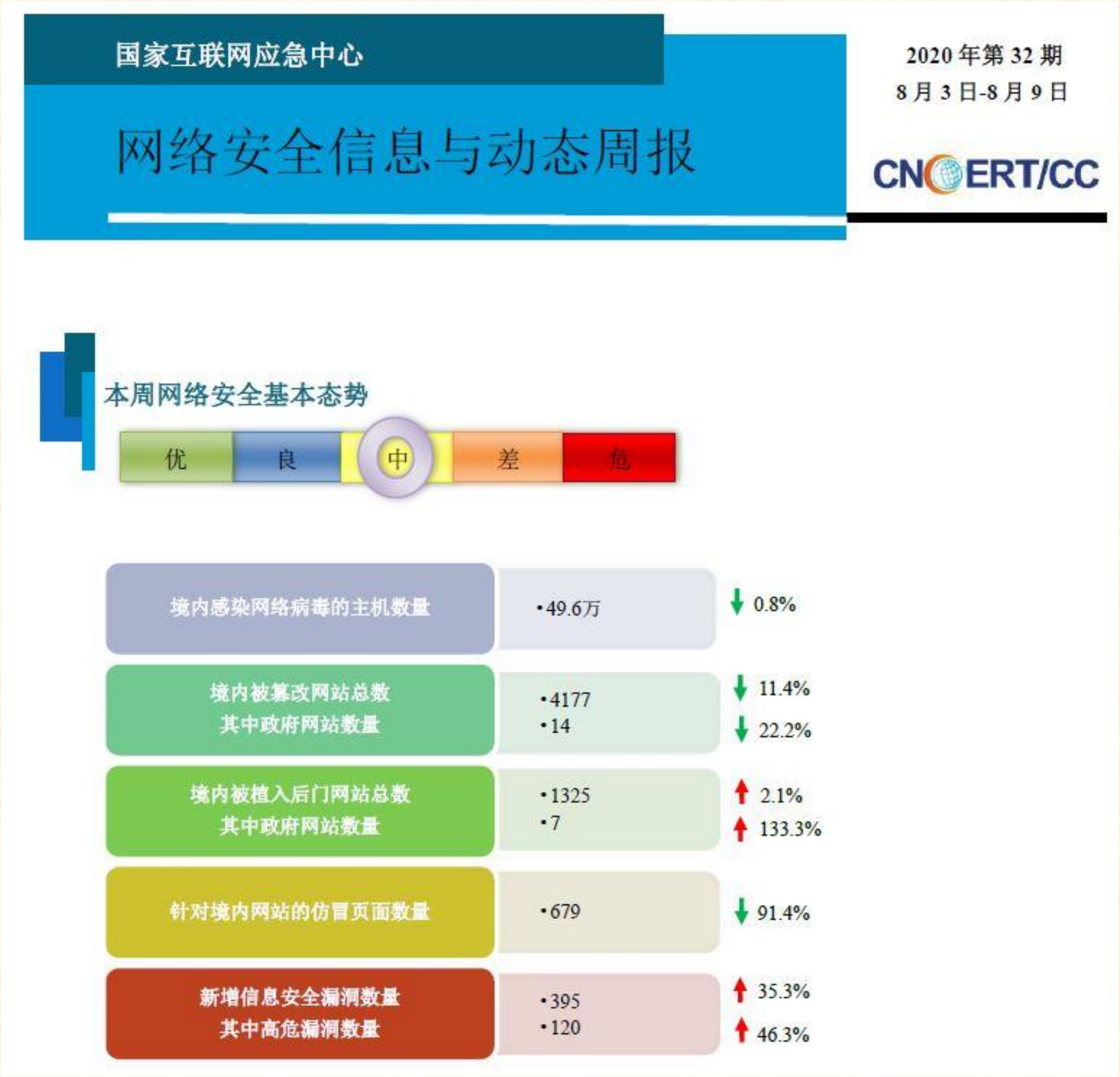
据360全球网络攻击实时监测预警系统的跟踪监测显示：导致这场灾难的原因是黑客入侵，控制了全世界十多万台智能硬件设备，组成了僵尸网络，对美国互联网域名解析服务商DYN进行DDoS攻击。

十多万台设备被控制发起的攻击已经让半个美国的互联网瘫痪，数十亿设备如果被控制则足以让全球互联网瘫痪。

October 21, 2016, USA:

> 100000 computers hacked → ½ Internet down

In China …



国家互联网应急中心

网络安全信息与动态周报

2020 年第 32 期
8 月 3 日-8 月 9 日

CNCERT/CC

本周网络安全基本态势

优 良 中 差 危

境内感染网络病毒的主机数量	•49.6万	↓ 0.8%
境内被篡改网站总数 其中政府网站数量	•4177 •14	↓ 11.4% ↓ 22.2%
境内被植入后门网站总数 其中政府网站数量	•1325 •7	↑ 2.1% ↑ 133.3%
针对境内网站的仿冒页面数量	•679	↓ 91.4%
新增信息安全漏洞数量 其中高危漏洞数量	•395 •120	↑ 35.3% ↑ 46.3%

In China …

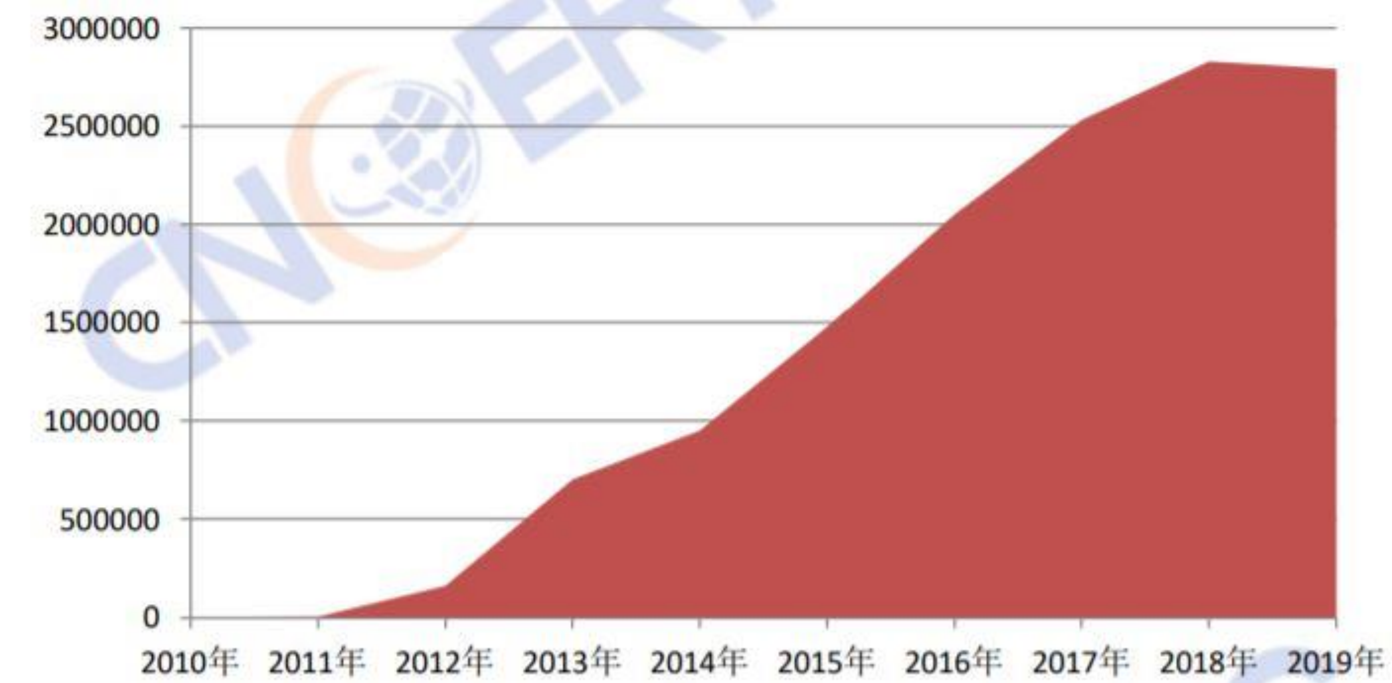


图 8 2010 年至 2019 年移动互联网恶意程序捕获数量走势

[安全报告]

In China …

图 8-1 2019 年 CNCERT/CC 网络安全事件接收数量月度统计（来源：CNCERT/CC）

安全报告

18岁高中生的非法“数据帝国”：有1亿条公民个人信息

2019-09-09 18:34 来源：澎湃新闻·澎湃号·政务

字号

中央政法委长安剑 | + 关注

自学软件编程技术，研发黑客软件，利用网站注册漏洞疯狂盗取公民个人信息上亿条，在境内外网络上公开售卖，刚满18岁的高中生竟构想出一个非法“数据帝国”梦。近日，江苏省无锡市惠山区检察院依法以涉嫌侵犯公民个人信息罪对刘某提起公诉。

City University of Hong Kong

CityU Announcement Portal (CAP)

In CityU

There was an incident before

Archive

Posting Detail

Title :	Zero-day malware新形電腦病毒
Body :	

Zero-day malware

Dear colleagues and students,

On 22 January, CityU found that a new computer virus (zero-day malware) invaded the University's email system and hacked the login names and passwords of some faculty and staff. The malware was successfully removed before it could spread further. There is no evidence that any sensitive information was compromised.

Upon learning about the incident, the University immediately contacted the police, informed the Office of the Privacy Commissioner for Personal Data, and asked all affected faculty and staff to change their passwords.

To further bolster the security of our computer systems, experts from our vendor have been engaged to review our email infrastructure and management processes. In addition, all faculty, staff and students are required to change their passwords regularly, and are reminded to encrypt their files when sending sensitive information through emails.

Office of the Chief Information Officer
28 January 2014

新形電腦病毒

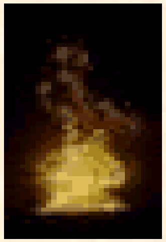
各位同事、同學：

城大在1月22日發現電郵系統被一種新形的電腦病毒（zero-day malware）入侵，盜取了一些教職員的登入名稱及密碼。大學在病毒進一步入侵系統或其他敏感資料外洩之前，已成功將之移除。

校方得悉事件後已即時向警方報案及知會個人資料私隱專員公署，並隨即通知所有受影響的用戶更改密碼。城大非常重視大學電腦系統的安全，已要求服務供應商檢討電郵系統的架構及管理程序，進一步加強保安的措施，全校教職員及學生必須定時更改密碼，並在使用電郵傳送敏感資料時須為檔案加密。

資訊總監辦公室
2014年1月28日

Another Example



Flame (malware)

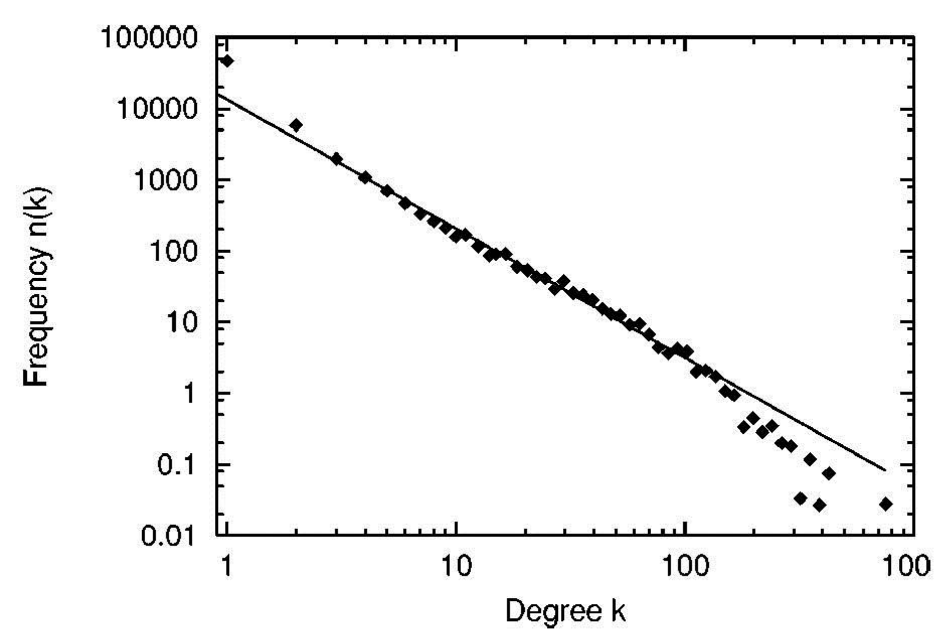
Flame, also known as Flamer, sKyWIper, or Skywiper, is modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system.

Reportedly, the program is being used for targeted cyber espionage (spy) in some middle eastern countries.

June 19, 2012, Washington Post published an article that Flame was jointly developed by U.S. National Security Agency, CIA and Israel's military at least five years ago as part of a classified effort code-named Operation Olympic Games to collect intelligence in preparation for cyber-sabotage aimed at slowing Iranian nuclear efforts.

Spreading of Email Viruses

- **Typical examples:**
- Milessa (1999)
- I-Love-You (2000)
- Nimda (2001)
- Win32/Sircam (2001)
- Chinese versions:
- Worm.Klez.cn.b (2002)
- Worm.SoBig.c (2003)
- Worm.Mimail.C (2003)
- SCO bomb (2004)
- ……



Node-degree distribution of the email network in Kiel University, Germany, 2002

$N = 59812 \quad \langle k \rangle = 2.88 \quad \gamma = -1.81$

Ebel et al (2002)

Computer Viruses seem to be Decreasing

For many good reasons:

- Modern software has embedded virus protection modules
- Operating systems have stronger ability to resist viruses
- Antivirus software becomes much more powerful
- **… …**

Epidemic Models

Epidemic Models

Consider a network of population N individuals (nodes)

$S(t)$ – percntage of susceptible (healthy) individuals at time $t \geq 0$

$I(t)$ – percentage of infected (sick) individuals at time $t \geq 0$

$R(t)$ – percentage of recovered (healthy) individuals at time $t \geq 0$

→ $S(t) + I(t) + R(t) = 1$ (100%) at time $t \geq 0$

Assume:

Infective rate (from susceptible to infected) is $\lambda \in [0,1]$

Recover rate (from sick to become healthy) is $\delta \in [0,1]$

(recovered individuals are permanently immune)

SI Model

Consider the situation where $R(t) \equiv 0$ for all $t \geq 0$. Thus, the increased number of infected individual from time t to time $t + \Delta t$ is

$$N[I(t+\Delta t) - I(t)] = \alpha \, NI(t)\, \Delta t$$

where $I(t)$ is the percentage of infected individuals in the population, and $\alpha = [\lambda S(t)]$ is the proportional coefficient at time t, so

$$\frac{I(t+\Delta t) - I(t)}{\Delta t} = [\lambda S(t)] I(t)$$

As $\Delta t \to 0$, it becomes $\frac{dI(t)}{dt} = \lambda S(t) I(t)$. Since $S(t) = 1 - I(t)$, it gives

$$\frac{dI(t)}{dt} = \lambda[1 - I(t)]I(t)$$

This is called the Logistic equation.

Continuous: $\dot{x} = \lambda(1-x)x$ Discrete: $x_{k+1} = \lambda(1-x_k)x_k$

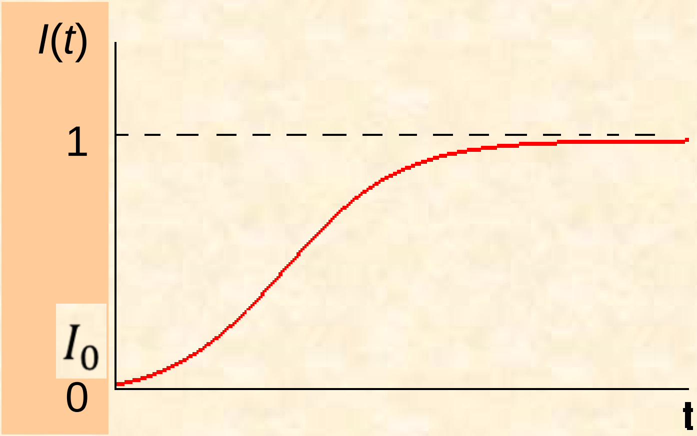
Logistic Equation

$$\frac{dI(t)}{dt} = \lambda[1 - I(t)]I(t), \quad I(0) = I_0$$

The Logistic equation has a solution

$$I(t) = \frac{1}{1 + (I_0^{-1} - 1)e^{-\lambda t}}$$

As $t \to \infty$, $I \to 1$, so the whole population is infected.



SIS Model

S → I → S → I → S → ···

Infective rate (from susceptible to infected) is $\lambda \in [0,1]$

Recover rate (from sick to become healthy) is $\delta \in [0,1]$

Consider, again, the case of $R(t) = 0$, but with $\delta > 0$. Then

$$\frac{dI(t)}{dt} = \lambda[1 - I(t)]I(t) - \delta I(t)$$

which has a solution

$$I(t) = \begin{cases} \left\{ \dfrac{1}{1 - \frac{\delta}{\lambda}} + \left(I_0^{-1} - \dfrac{1}{1 - \frac{\delta}{\lambda}} \right) e^{-\left(1 - \frac{\delta}{\lambda}\right)\lambda t} \right\}^{-1}, & \delta \neq \lambda \\ \dfrac{1}{I_0^{-1} + \lambda t}, & \delta = \lambda \end{cases}$$

SIS Model

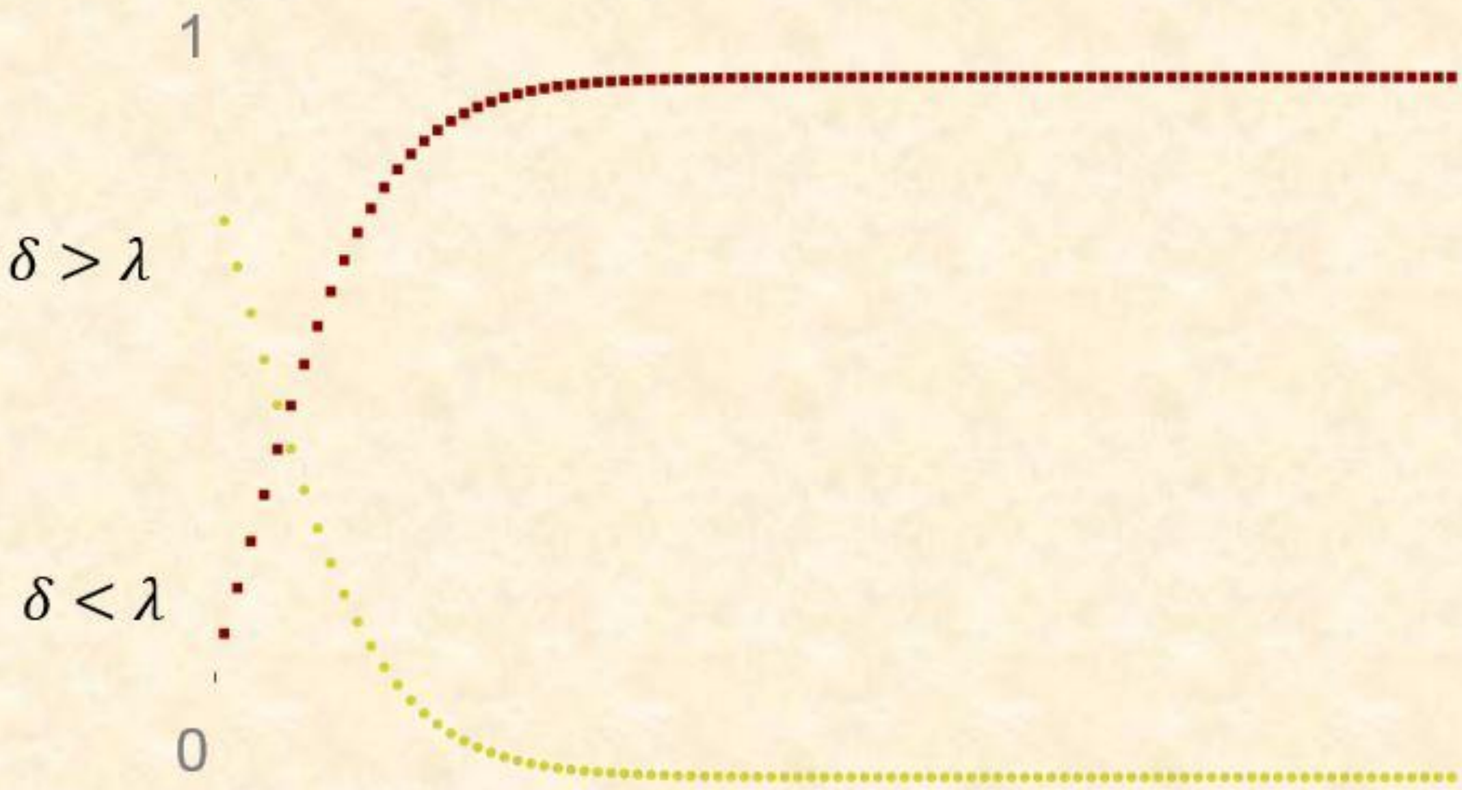
$$
I(t) = \begin{cases} \left\{ \dfrac{1}{1-\frac{\delta}{\lambda}} + \left(I_0^{-1} - \dfrac{1}{1-\frac{\delta}{\lambda}} \right) e^{-\left(1-\frac{\delta}{\lambda}\right)\lambda\, t} \right\}^{-1}, & \delta \neq \lambda \\ \dfrac{1}{I_0^{-1} + \lambda\, t}, \qquad \delta = \lambda & \end{cases}
$$

Three cases:

- $\delta > \lambda$: Recovering is faster than infecting.
  $I(t) \to 0$ exponenentially fast as $t \to \infty$
- $\delta = \lambda$: Threshold case. $I(t) \to 0$ recipically fast as $t \to \infty$
- $\delta < \lambda$: Recovering is slower than infecting. $I(t) \to \left(1 - \frac{\delta}{\lambda}\right)$ as $t \to \infty$

  If $\delta \ll \lambda$, then $I(t) \sim 1$ as $t \to \infty$, all will be infected eventually

SIS Model



SIR Model

Now, suppose $R(t) > 0$. Then

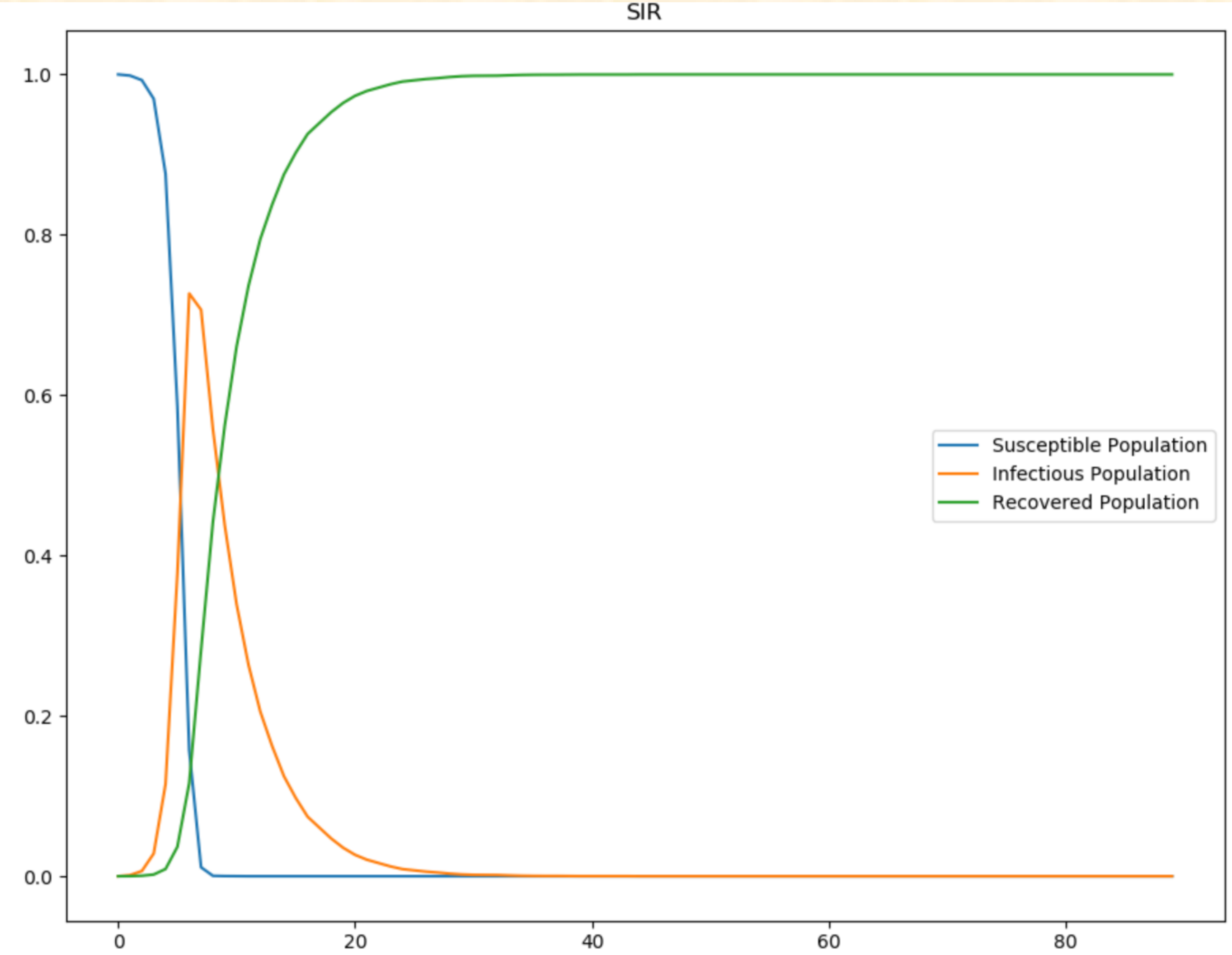
$$\begin{cases} \frac{dI(t)}{dt} = [\lambda S(t)]I(t) - \delta I(t) \\ \frac{dS(t)}{dt} = -[\lambda I(t)]S(t) \\ \frac{dR(t)}{dt} = \delta I(t) \end{cases}$$

with $S(0) = S_0, I(0) = I_0, \; R(0) = 0$

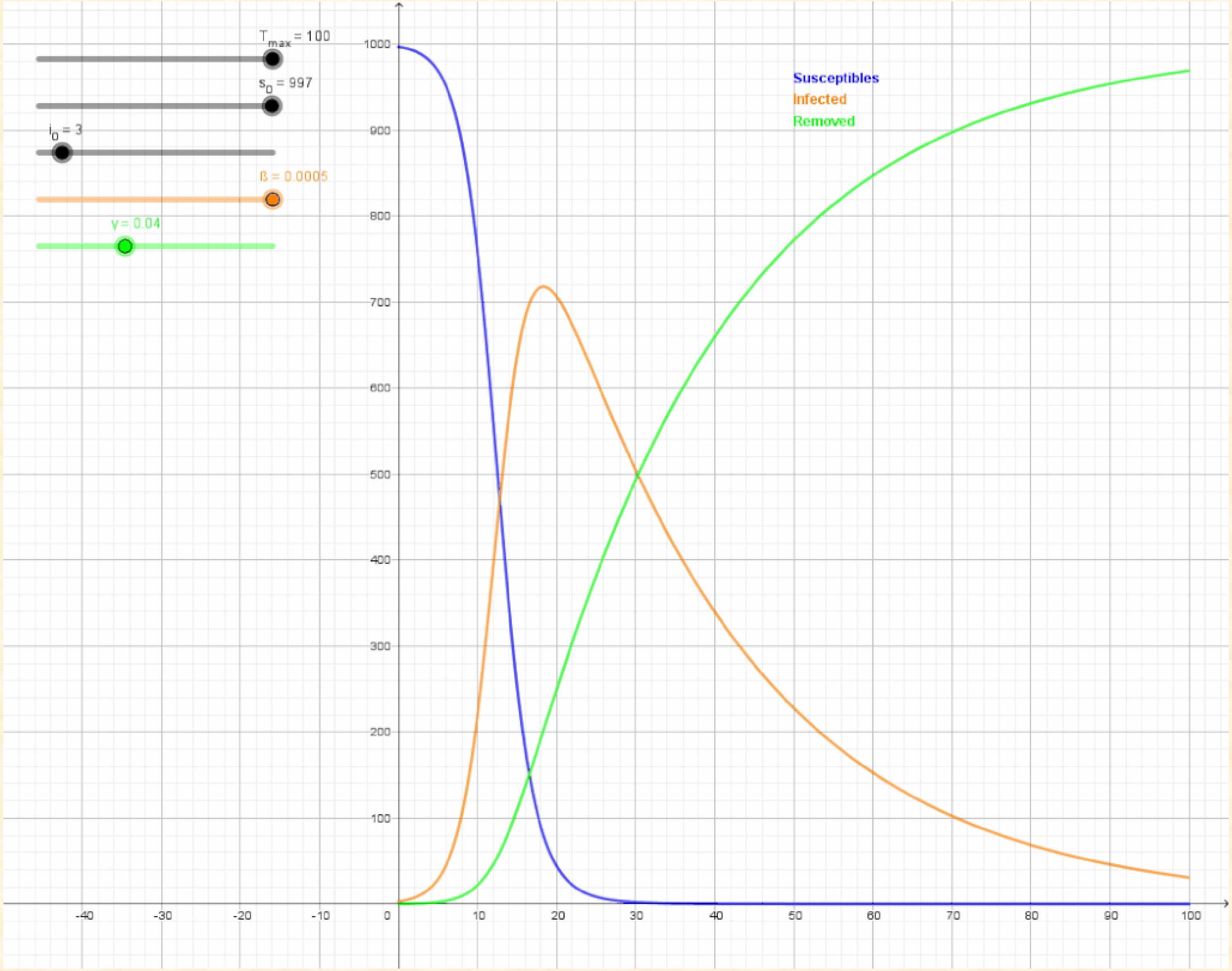
Two case:

- $S_0 > \frac{\delta}{\lambda}$: Virus will spread for some time, but eventually die out
- $S_0 < \frac{\delta}{\lambda}$: Virus will die out quickly

SIR Model



SIR
1.0
0.8
0.6
0.4
0.2
0.0
0
20
40
60
80
Susceptible Population
Infectious Population
Recovered Population



T_{max} = 100
s_0 = 997
i_0 = 3
ß = 0.0005
γ = 0.04
Susceptibles
Infected
Removed
1000
900
800
700
600
500
400
300
200
100
0
-40
-30
-20
-10
10
20
30
40
50
60
70
80
90
100

SEIR Model

Consider a network of population N individuals (nodes)

$S(t)$ – percntage of susceptible (healthy) individuals at time $t \geq 0$

$I(t)$ – percentage of infected (sick) individuals at time $t \geq 0$

$R(t)$ – percentage of recovered (healthy) individuals at time $t \geq 0$

$E(t)$ – percentage of exposed individuals at time $t \geq 0$

$$S(t) + E(t) + I(t) + R(t) = 1 \quad \text{for all} \quad t \geq 0$$

$$\Uparrow$$

S → E (with latency) → I

more models

$$\frac{dS(t)}{dt} = \mu - \beta S(t)I(t) - \mu S(t)$$

$$\frac{dE(t)}{dt} = \beta S(t)I(t) - (\mu + \alpha)E(t)$$

$$\frac{dI(t)}{dt} = \alpha E(t) - (\mu + \gamma)I(t)$$

$R(t) = 1 - S(t) - E(t) - I(t)$ for all $t \geq 0$

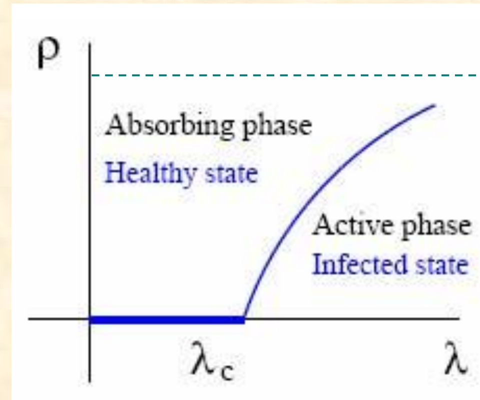
μ – birth rate = death rate

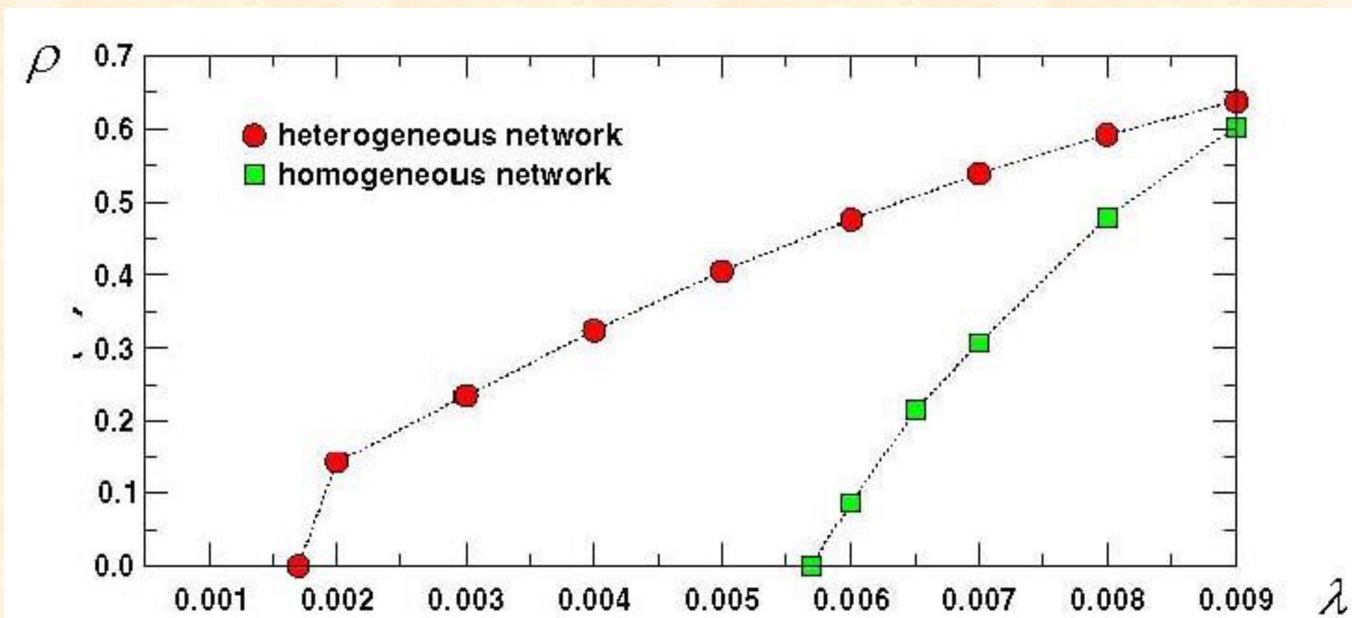
β – scaling constant

1 / α – average latent period

1 / γ – average infectious period

Virus Spreading Threshold





Epidemic Threshold on Homogenous Networks

- Consider the SIS model: S → I → S → I → S → ⋯

$$\frac{dI(t)}{dt} = \nu[1 - I(t)]I(t) - \delta I(t)$$

- Suppose that the probability of a node becoming "infected" from being "susceptible" is ν, and the probability of a node being cured and becomes "susceptible" again is δ . Define the virus effective spreading rate as before:

$$\lambda = \frac{\nu}{\delta}$$

- Let the density of infected population at time t be $\rho(t)$, with $\rho(t) \to \rho$ ($t \to \infty$)

$$k_i \approx \langle k \rangle$$

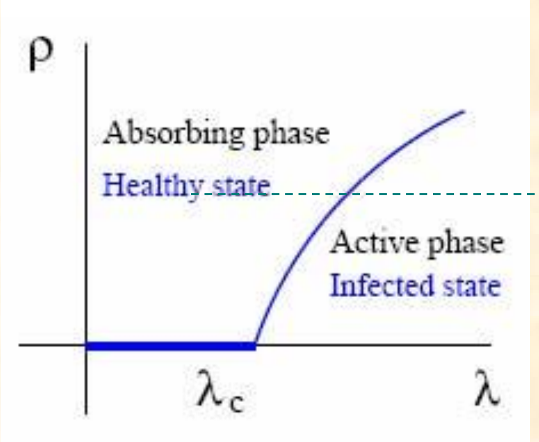
Epidemic Threshold on Homogenous Networks

Then, the epidemic spreading equation is:

$$\frac{d\rho(t)}{dt} = \langle k \rangle \lambda [1 - \rho(t)] \rho(t) - \rho(t)$$

It yields, as $t \to \infty$

$$\rho = \begin{cases} 0 & \lambda < \lambda_c \\ \dfrac{\lambda - \lambda_c}{\lambda} & \lambda \geq \lambda_c \end{cases}$$



with the spreading threshold

$$\lambda_c = \frac{1}{\langle k \rangle}$$

M. Boguna, R. Pastor-Satorras, A. Vespignani (2003):
"Epidemic spreading in complex networks with degree correlations".

Epidemic Threshold on Scale-Free Networks

The virus spreading equation

$$\frac{d\rho(t)}{dt} = \langle k \rangle \lambda [1 - \rho(t)] \rho(t) - \rho(t)$$

is modified to:

$$\frac{d\rho_k(t)}{dt} = k \lambda [1 - \rho_k(t)] \Theta(\rho_k(t)) - \rho_k(t)$$

Here, $\Theta(\rho_k(t))$ is the probability of an edge connecting to an infected degree-k node.

Solution: $\rho_k = \dfrac{k\lambda\Theta(\lambda)}{1 + k\lambda\Theta(\lambda)}$ Threshold: $\lambda_c = \dfrac{\langle k \rangle}{\langle k^2 \rangle}$

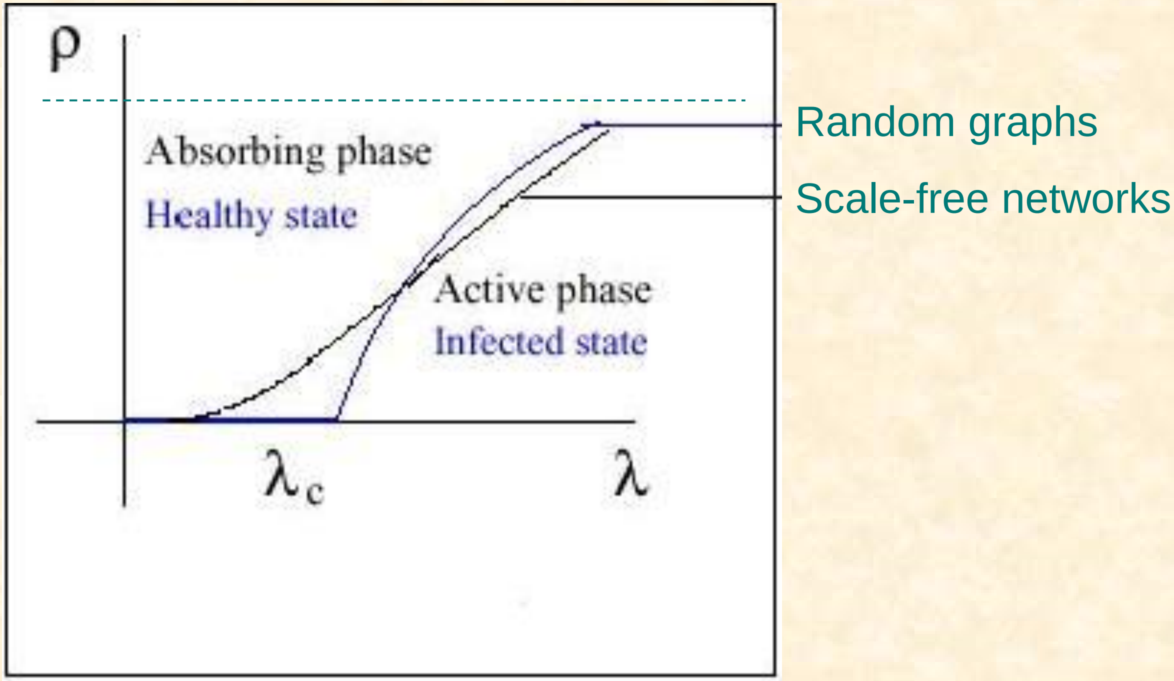
Higher-degree nodes have higher probabilities to be infected

as $N \to \infty$ → $k \to \infty$

→ $\lambda_c \to 0$

M. Boguna, R. Pastor-Satorras, A. Vespignani (2003):
"Epidemic spreading in complex networks with degree correlations".

Epidemic Threshold on Scale-Free Networks



λ is the spreading rate
λ_c is the threshold

- Classical theory: $\lambda_c > 0$
- Scale-free network: $\lambda_c = 0$

(Pastor-Satorras, 2001)

Immunization on Scale-Free Networks

❖ Since scale-free networks are fragile to virus attacks, causing wide and serious outbreak, immunization becomes especially important for this type of networks

❖ There are three effective immunization strategies:

➢ Random Immunization (or, Uniform Immunization)

➢ Targeted Immunization (or, Selective Immunization)

➢ Acquaintance Immunization

Random Immunization

Let the immunity (density of immunized nodes) be denoted by g

Random immunization strategy: the immunization threshold is

$$g_c = 1 - \frac{\lambda_c}{\lambda}$$

where $\lambda_c = \frac{\langle k \rangle}{\langle k^2 \rangle}$ is the effective epidemic threshold, giving

$$g_c = 1 - \frac{1}{\lambda} \frac{\langle k \rangle}{\langle k^2 \rangle}$$

Clearly, $N \to \infty$ → $\langle k^2 \rangle \to \infty$ → $\lambda_c \to 0$ → $g_c \to 1$

→ in order to immune a scale-free network, almost every node has to be immunized

→ random immunization for scale-free networks is inefficient and expensive

Satorras and Vespignani (2003)

Targeted Immunization

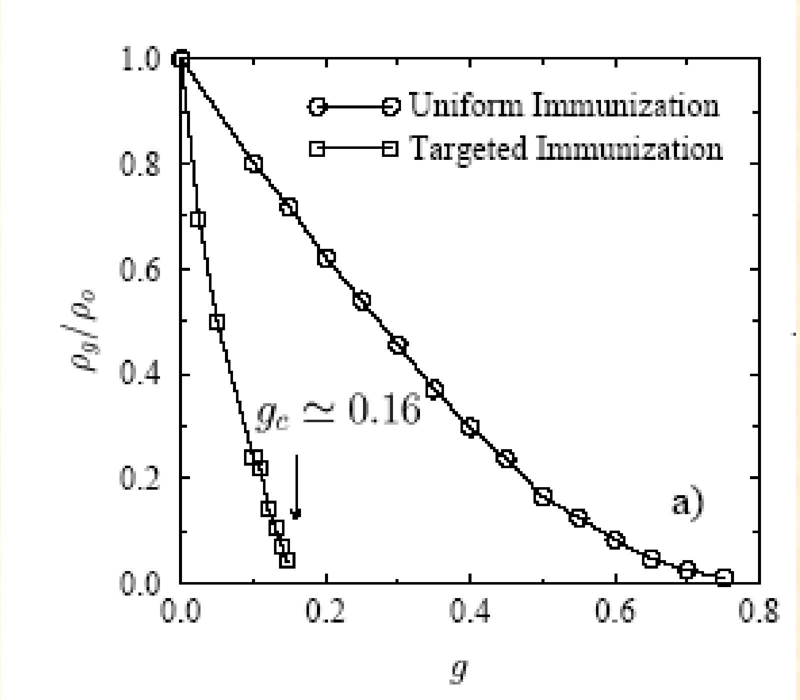
Targeted immunization strategy: to immune the most highly connected nodes, thereby reducing or completely blocking virus spreading

For BA scale-free networks, the immunization threshold is

$$g_c \sim e^{-\frac{2}{m\lambda}}$$

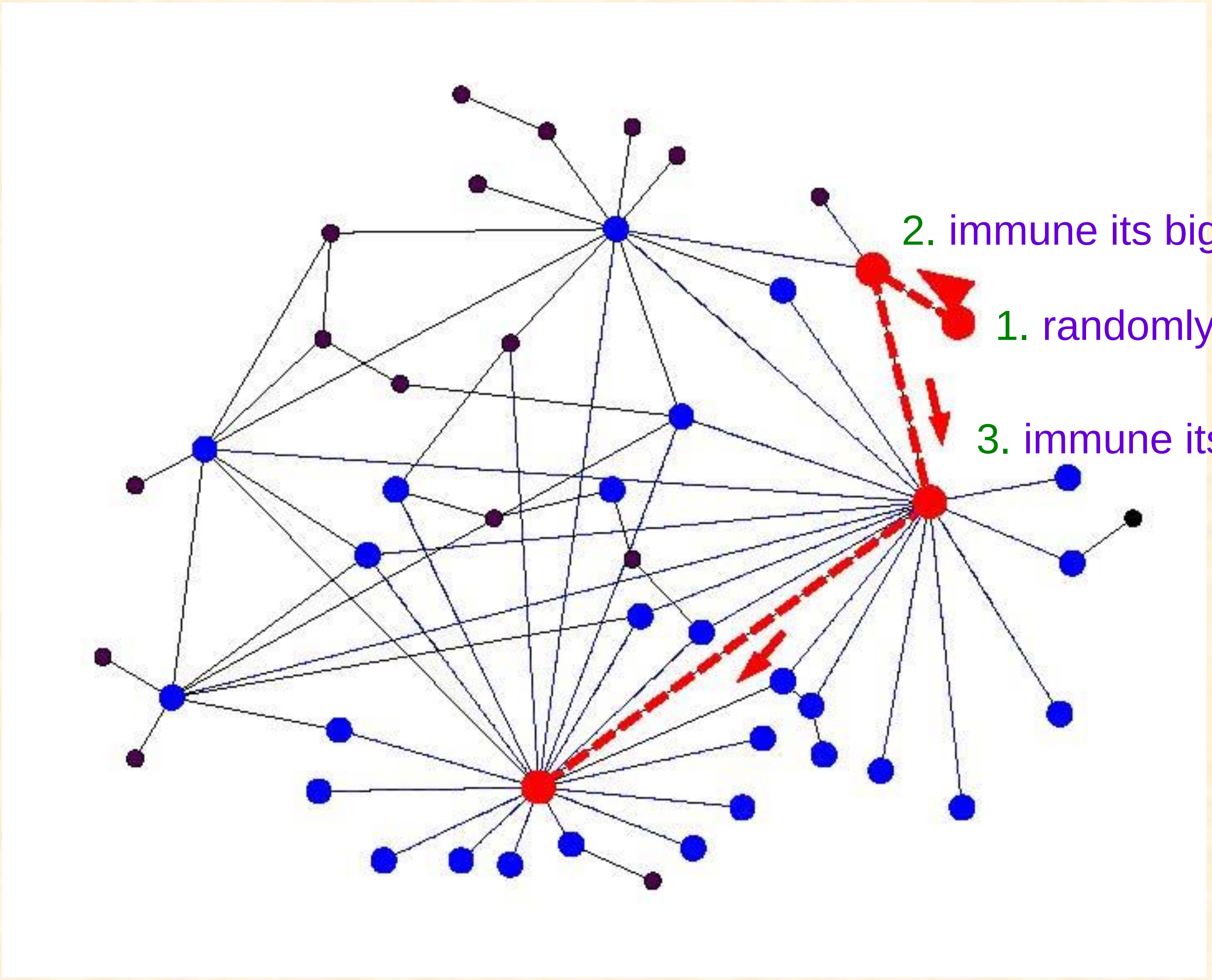
→ a very small immunization threshold can be obtained for a very large range of effective spreading rate λ

→ for scale-free networks, targeted immunization has a much smaller immunization threshold than random immunization, hence is more effective



Satorras and Vespignani (2003)

Acquaintance Immunization

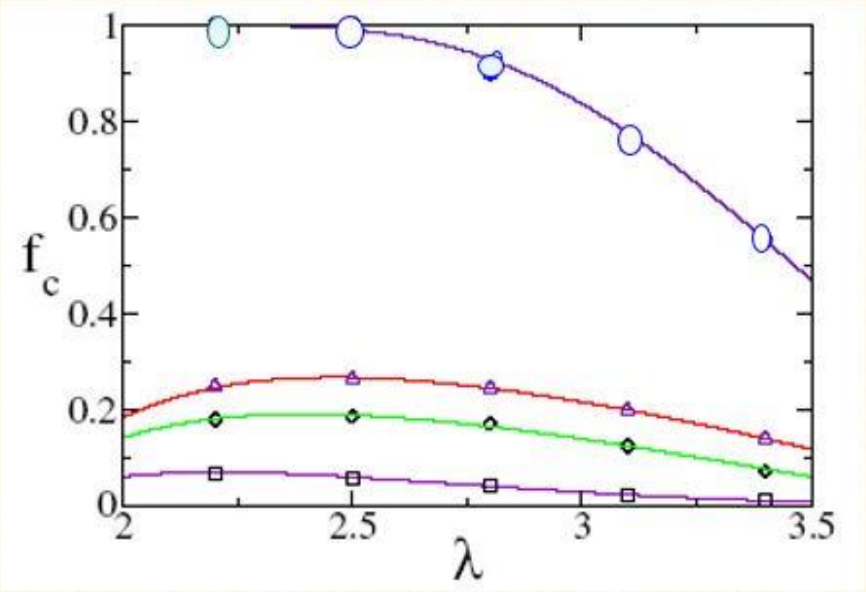


Idea:

1. → 2. → 3. → ......

Immunization on Scale-Free Networks

Acquaintance immunization strategy:
To randomly select a fraction of nodes from the population, and for each node in the fraction select a biggest one of its neighbors for immunization



empty circles – random

empty triangles – acquaintance

empty diamonds – two-acquaintance

empty squares – targeted

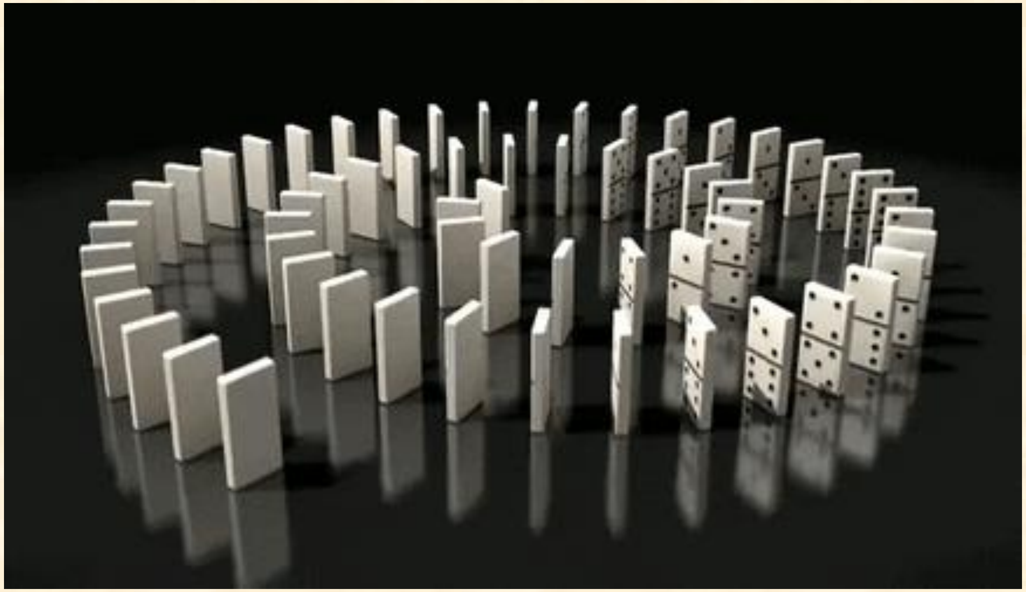
BREAK

10 minutes

Power Networks Black Out

Cascading Failures …

Domino Effect



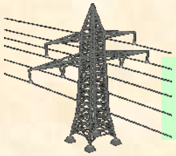
DEMO

Cascading Reactions and Failures

	Epidemics	Power Grids
Similarities	cascading reactions and spreading	cascading reactions and spreading
Differences	• contacting nearest neighbors • due to body immunity systems • individual death → failure • failure curve S-shape	• not through nearest neighbors • by electric circuit laws and impedance values • disconnection → failure • failure curve not S-shape, case-dependent

Real Examples of Cascading Failures


Internet


Power grid

October 1986:
the first documented
Internet collapse
due to congestion

↓

Drop in speed
of a factor 100

August 1996:
sag of just one
electric line in
Oregon USA

↓

Blackout affected 4
million people in 9
different states

August 2003:
local failure
in Ohio USA

↓

Largest blackout
in the US history

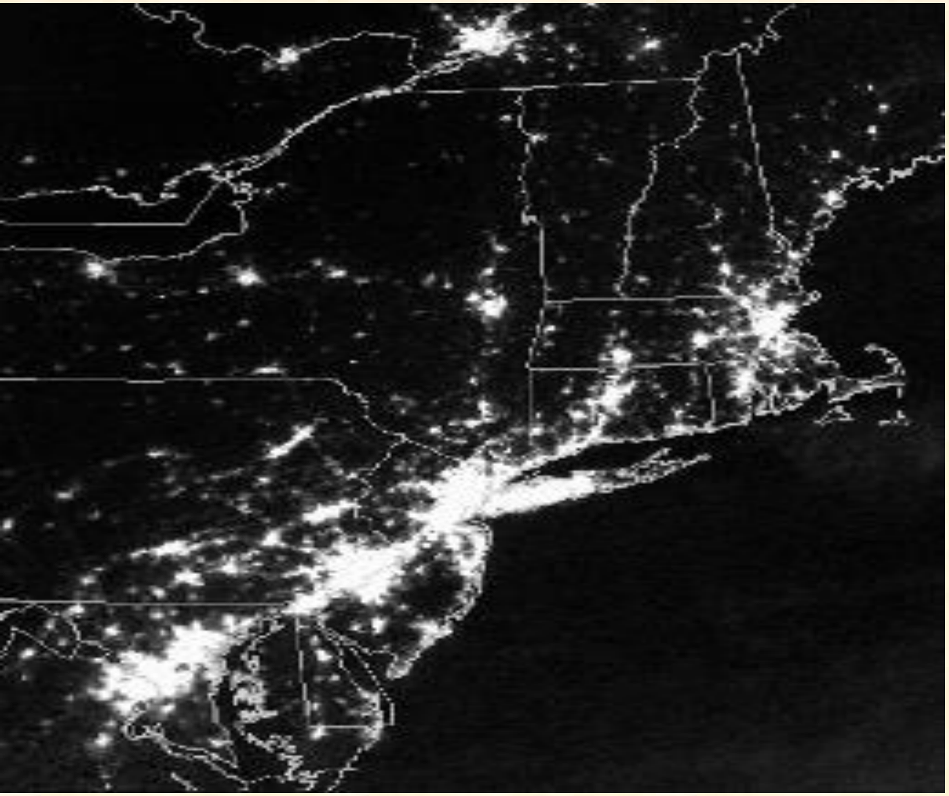
Some Typical Incidents of Power Blackouts

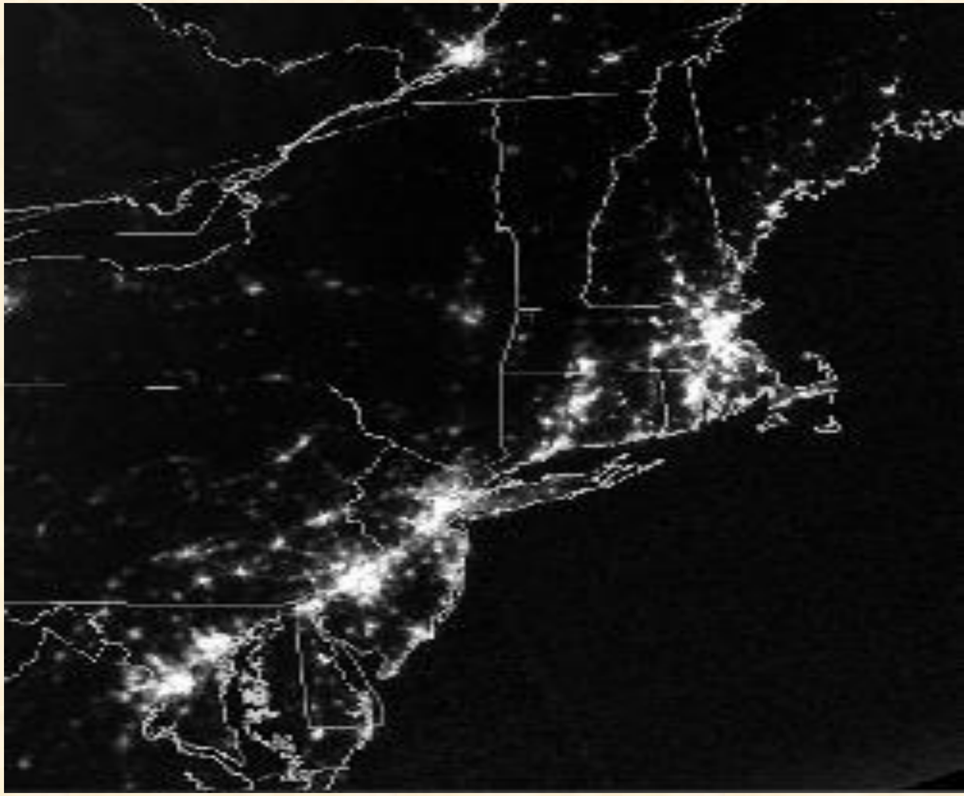
Data Source

Article	People affected (millions)	Location	Date
2012 India blackouts	620	India	July 30–31, 2012
2001 India blackout	230	India	January 2, 2001
2014 Bangladesh blackout	150	Bangladesh	November 1, 2014
2015 Pakistan blackout	140	Pakistan	January 26, 2015
2019 Java blackout	120	Indonesia	August 4–5, 2019
2005 Java–Bali blackout	100	Indonesia	August 18, 2005
1999 Southern Brazil blackout	97	Brazil	March 11–June 22, 1999
2015 Turkey blackout	70	Turkey	March 31, 2015

12 Biggest Power Blackouts in History

Snapshot: 15 August 2003 Power Blackout





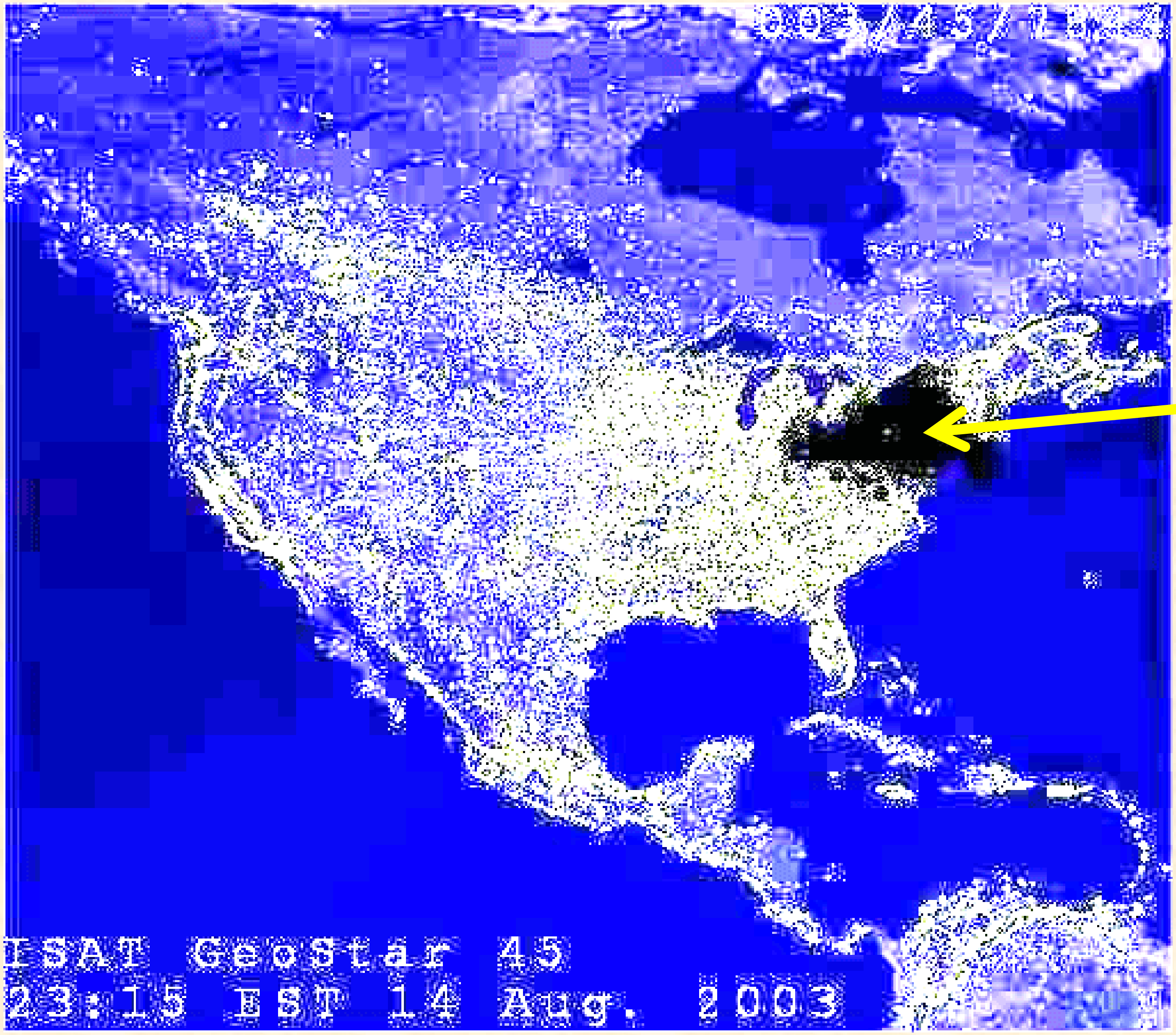
Satellite images

Before blackout

During blackout

Reference

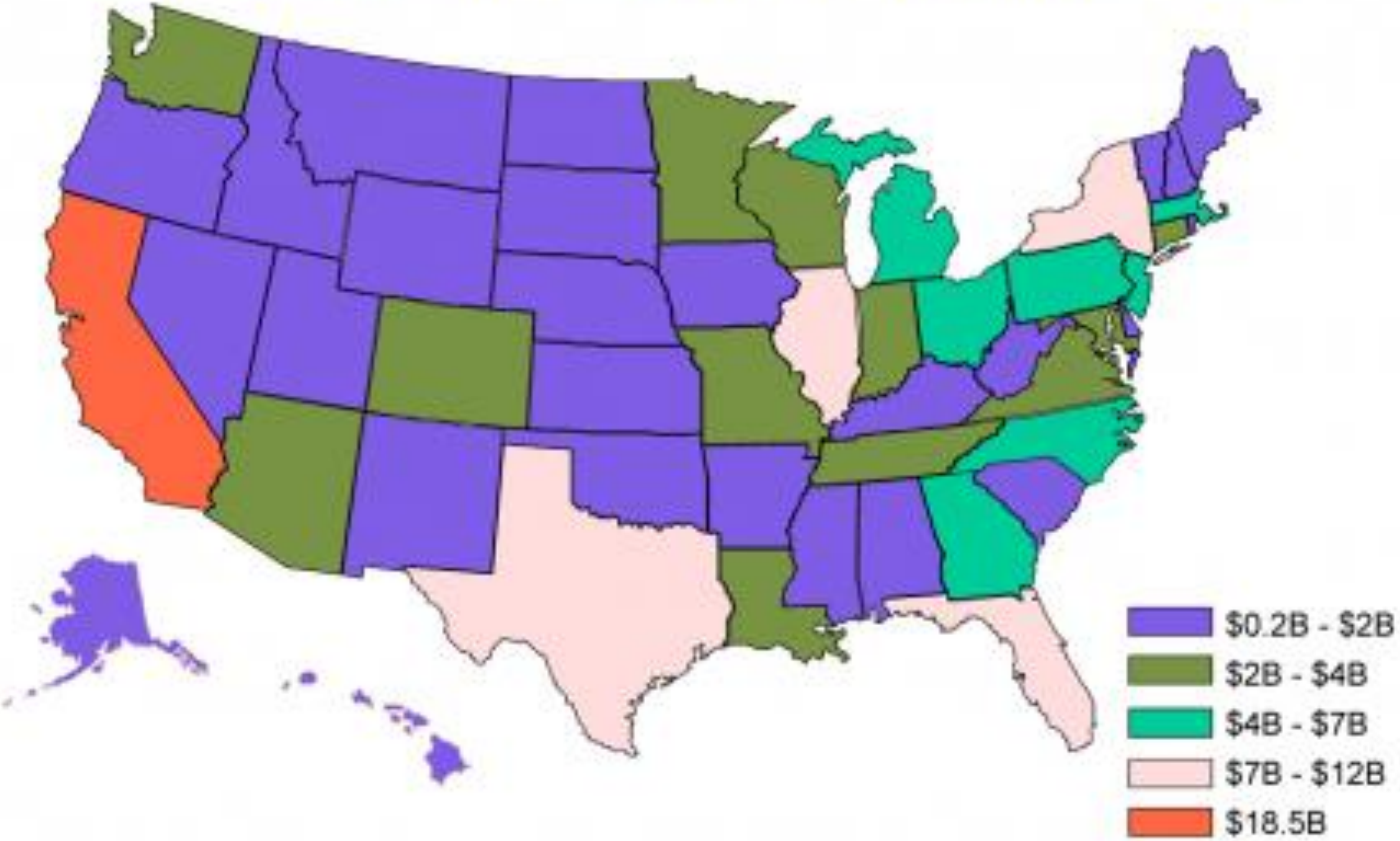
A detailed map



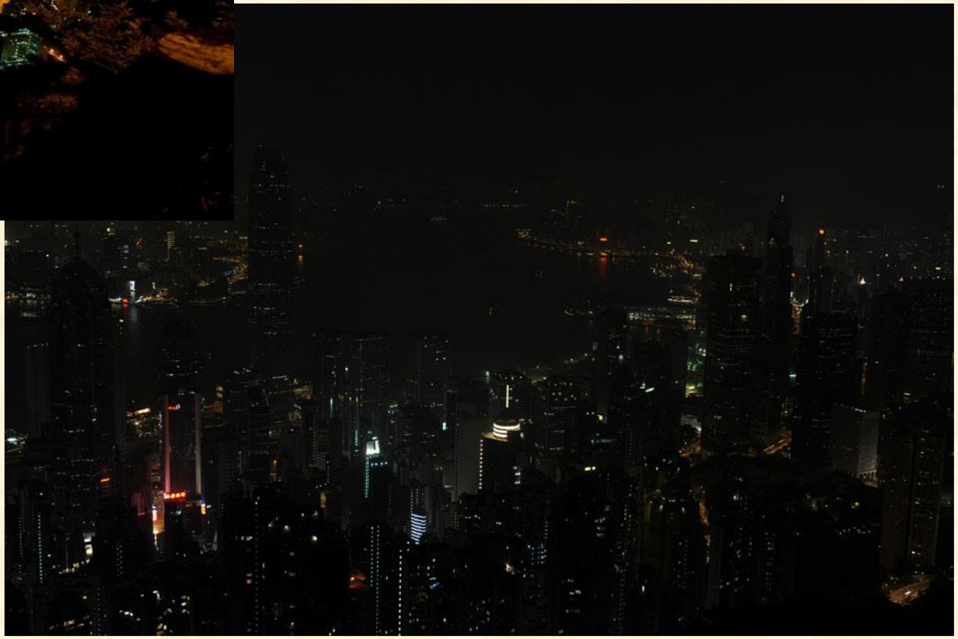
black out

Annual Business Losses from Grid Problems

Primen Study: $150B annually for power outages and quality issues



Hong Kong ?



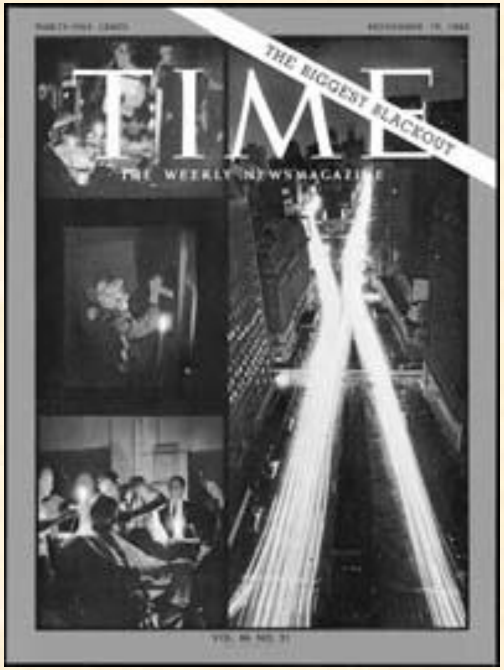
EARTH HOUR
28 MAR 2020

28Mar2020 —— 20:30

地球一小時

EARTHHOUR.HK

Will It Happen Again ?



… 1959, 1961, 1965, 1977, 2003, … … 2019, 2020, 2021 ?

Major Power Blackout Records

Unfortunately, the answer is YES

凤凰网 财经 finance.ifeng.com　凤凰网财经 > 财经资讯 > 环球财经 > 正文　梦之蓝 特约

印度再断电半数地区瘫痪 国民指因腐败政客贪婪所致

2012年08月01日 07:44
来源：财经网 作者：张阳　1人参与 0条评论　打印　转发　字号:TT

2012 India

7月31日，印度乘客在焦急地等火车。因为断电，印度的很多铁路陷入瘫痪。

7月31日，印度的断电危机更加严重。印度电力部门一名高级官员表示，周二又有多个地区的电网出现故障，导致全国一半地区没有电力供应，其中包括首都新德里和加尔各答等众多大城市，受影响人口达6亿。

据印度《经济时报》31日报道，当天下午，印度全国有一半的地区没有电力供应，这被称为印度史上最大的断电危机。目前，所有连接北部、东部和东北部地区的发电站均已关闭。在首都及多个邦，地铁服务均暂停，铁路系统一名发言人说，全国有多达500列火车因断电陷入困境。

August 01, 2012　RECORDER REPORT　0 Comments

BUSINESS RECORDER

Hundreds of millions of people across India were left without power on Tuesday in one of the world's worst blackouts, trapping miners, stranding train travellers and plunging hospitals into darkness when grids collapsed for the second time in two days.

Stretching from Assam, near China, to the Himalayas and the north-western deserts of Rajasthan, the outage covered states where half of India's 1.2 billion people live and embarrassed the government, which has failed to build up enough power capacity to meet soaring demand. "Even before we could figure out the reason for yesterday's failure, we had more grid failures today," said R. N. Nayak, chairman of the state-run Power Grid Corporation.

Prime Minister Manmohan Singh had vowed to fast-track stalled power and infrastructure projects as well as introduce free market reforms aimed at reviving India's flagging economy. But he has drawn fire for dragging his feet. By nightfall, power was back up in the humid capital, New Delhi and much of the north, but a senior official said only a third was restored in the rural state of Uttar Pradesh, itself home to more people than Brazil.

Power blackout caused traffic jam

Pakistan

Massive power failure plunges 80% of Pakistan into darkness

- Rebels blamed for breakdown of power transmission line on Sunday
- Huge blackout is latest reminder of the country's chronic problems

Agence France-Presse

Sunday 25 January 2015 07.10 GMT

A shopkeeper uses a gas lamp during a power outage in Pakistan where blackouts are common. Photograph: Arshad Arbab/EPA

Pakistan was plunged into darkness after a power transmission line broke down early on Sunday in an incident blamed on a rebel attack.

The power failure, one of the worst Pakistan has experienced, caused electricity to be cut in 80% of the country, including major cities and the capital Islamabad.

2015
Pakistan

2019 Venezuela

央视新闻客户端

【委内瑞拉全国大面积停电】政府抢修电网 又遭新一轮网络攻击

2019-03-10 09:40 央视新闻客户端 A+

从当地时间7日下午开始，包括首都加拉加斯在内的委内瑞拉全国发生大规模停电，直到8日傍晚，供电部分恢复。当地时间9日，委内瑞拉总统马杜罗在参加集会时说，全国受停电影响地区本来已经恢复大约70%的供电，但当天中午电力系统又受到新一轮网络攻击，导致再次崩溃。目前，电力系统工作人员仍在积极抢修中。

2019 New York

New York

Heart of New York goes dark as Manhattan suffers power outage

Governor calls failure 'unacceptable' as 73,000 people lose electricity for three hours

Associated Press in New York

Sun 14 Jul 2019 11.42 BST

503

Manhattan transformer fire knocks out power to thousands in Midtown, Upper West Side

据美国福克斯新闻频道报道，当地时间7月13日晚，美国纽约曼哈顿上城西区数万人停电，**停电原因为变压器起火造成。**

2019 New York

另据美国《纽约邮报》网站报道，当地时间7月13日晚，纽约曼哈顿中心地带的时代广场、地铁站、电影院、百货公司等因停电原因陷入一片漆黑。

英国高峰时段发电机故障大停电，致交通大乱影响近100万人

中新网

2019-08-10 13:24

2019 London

字号

当地时间2019年8月9日，英国伦敦，包括伦敦在内的英格兰东南部地区发生大规模停电事故，造成当地交通瘫痪。视觉中国 图

阿根廷全国大停电

头条君 国家电网报 6/17

2019 Argentina

据《纽约时报》6月16日报道，阿根廷和乌拉圭16日发生全国大停电，社交媒体用户称，巴西部分地区、巴拉圭和智利也受到波及。

当地时间16日7点50分，阿根廷电力公司Edesur Argentina在推特表示，“由于电力互联系统大规模故障，导致阿根廷和乌拉圭全境停电。”

Argentina and Uruguay Without Power After ‘Massive’ Failure

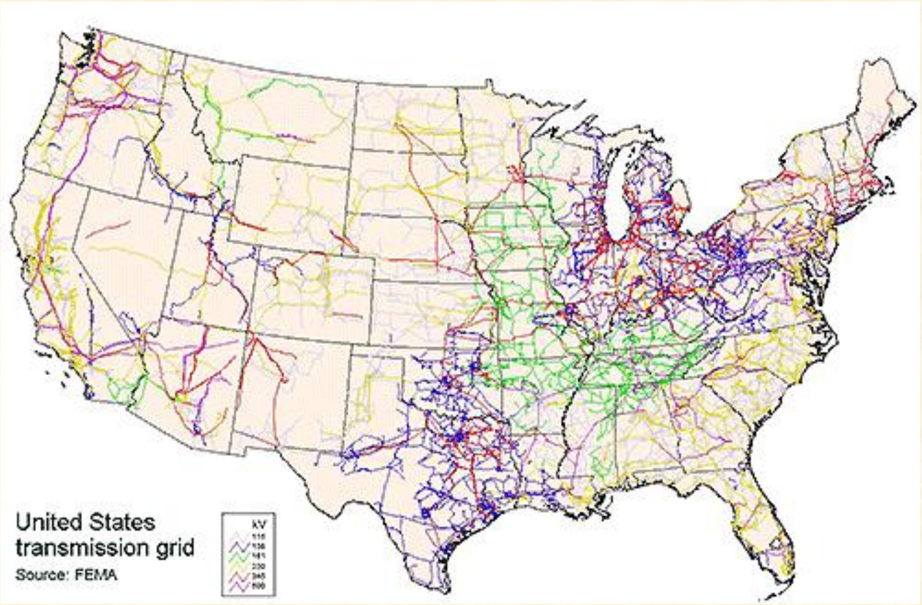
报道截图

乌拉圭乌特电力公司表示，“阿根廷电网的一个故障影响了相连接的系统，导致整个国家以及邻国几个省份无法供电，该系统于当地时间早上7点06分发生故障。”

阿根廷能源国务秘书处发布公告称，目前约有4800万人受到停电影响，预计需要数小时的时间才能全面恢复供电。阿根廷民防副国务秘书处官员表示，目前阿根廷南部已有部分地区正在恢复供电。

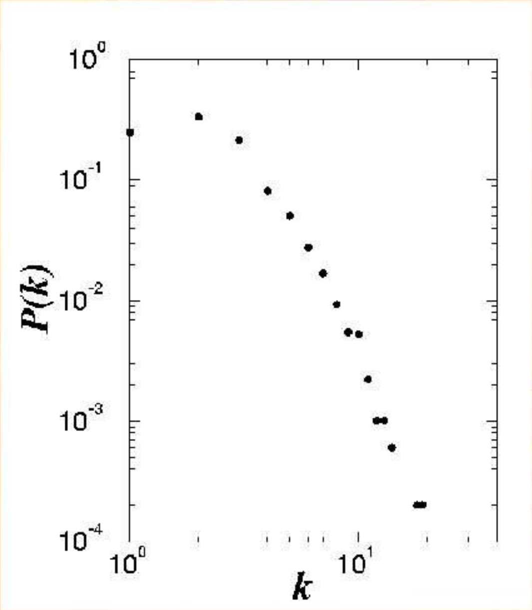
Why?

Cascading Failures on Scale-Free networks



ELECTRICAL POWERGRID

nodes: generators, transformers
edges: transmission lines



The electrical power grid of the western United States

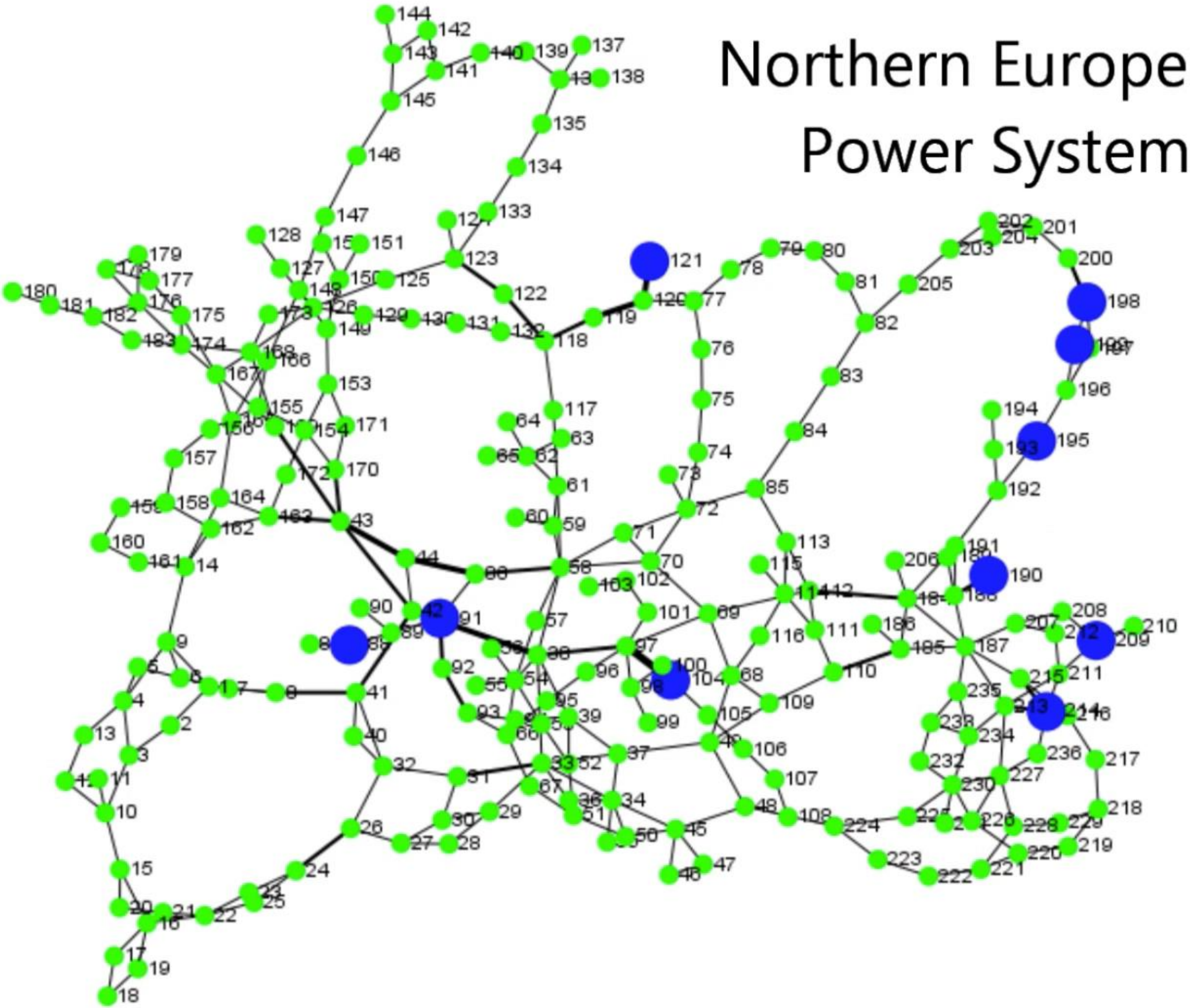
$\gamma \cong 4$

Power-Law Exponents in some Real Networks

$$\boxed{P(k) \sim k^{-\gamma}}$$

SOURCE	EXPONENT	CASCADE
Power grid (North America)	2.0	Power
Power grid (Sweden)	1.6	Energy
Power grid (Norway)	1.7	Power
Power grid (New Zealand)	1.6	Energy
Power grid (China)	1.8	Energy
Twitter Cascades	1.75	Retweets
Earthquakes	1.67	Seismic Wave

Northern European Power System



Demo: California

Black – normal   Red – crash   Blue – failure

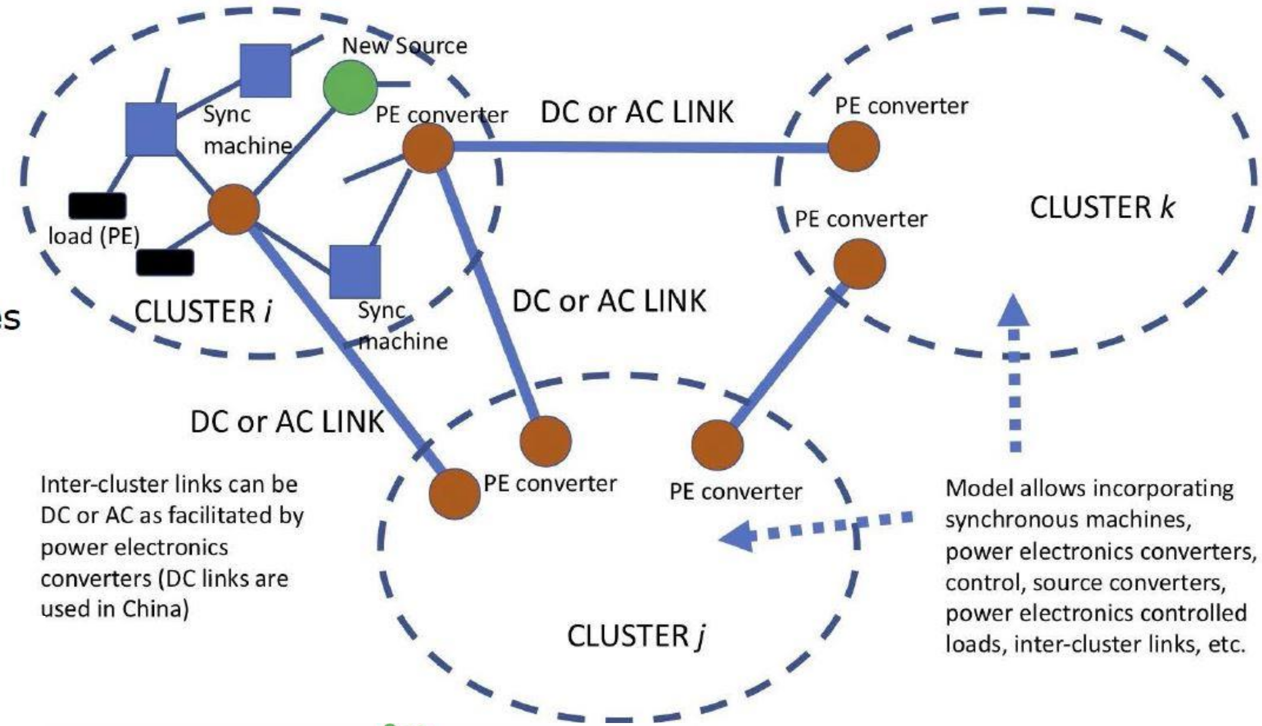
Power Network Cascade Modeling

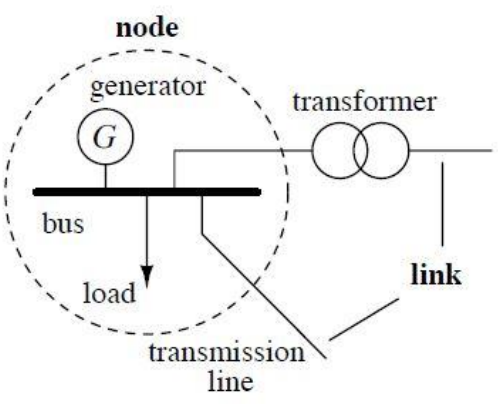
Features

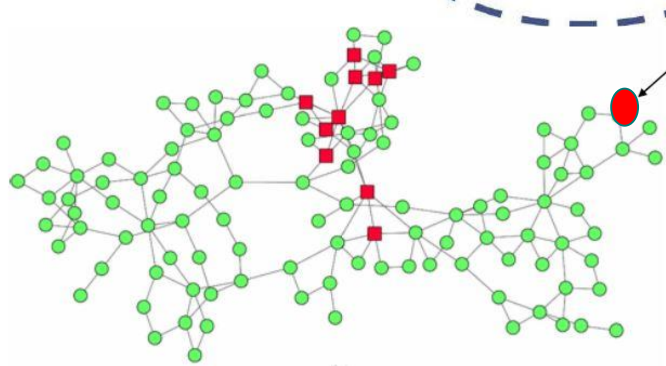
Clustering
  Intercluster connections

Generators
  Sync power generators
  Renewable power sources

Loads
  Conventional loads
  Active regulated loads







First failed node

→

It load will be shared by other

→

Newly overloaded nodes fail

Cascading Failures: Models and Analysis

Models Based on Node Dynamics

Fiber-Bundle Model (FBM):

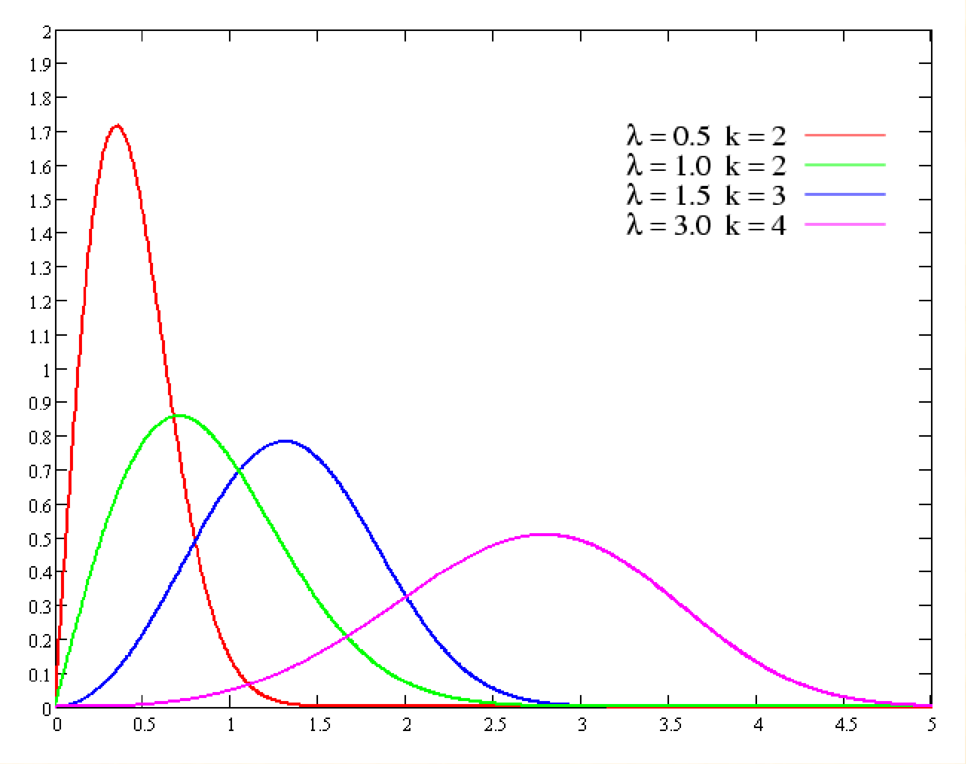
- On a lattice with many squares
- Randomly assign nodes/clusters ("fiber-bundles") into squares
- Connect nodes in a certain (e.g., scale-free) topology
- Assign "loads" to all nodes, $\sigma_i > 0$, by a Weibull distribution:

$$P(\sigma_i) = 1 - e^{-(\sigma_i)^c} \qquad (c > 0)$$

- Now: Suppose that one node/cluster is overloaded: $\sigma > \sigma_i$
- This node/cluster failed, and its load is evenly shared by all others, which causes some other nodes/clusters to fail
- The above cascading process repeats, until network is broken

Recall: Weibull distribution

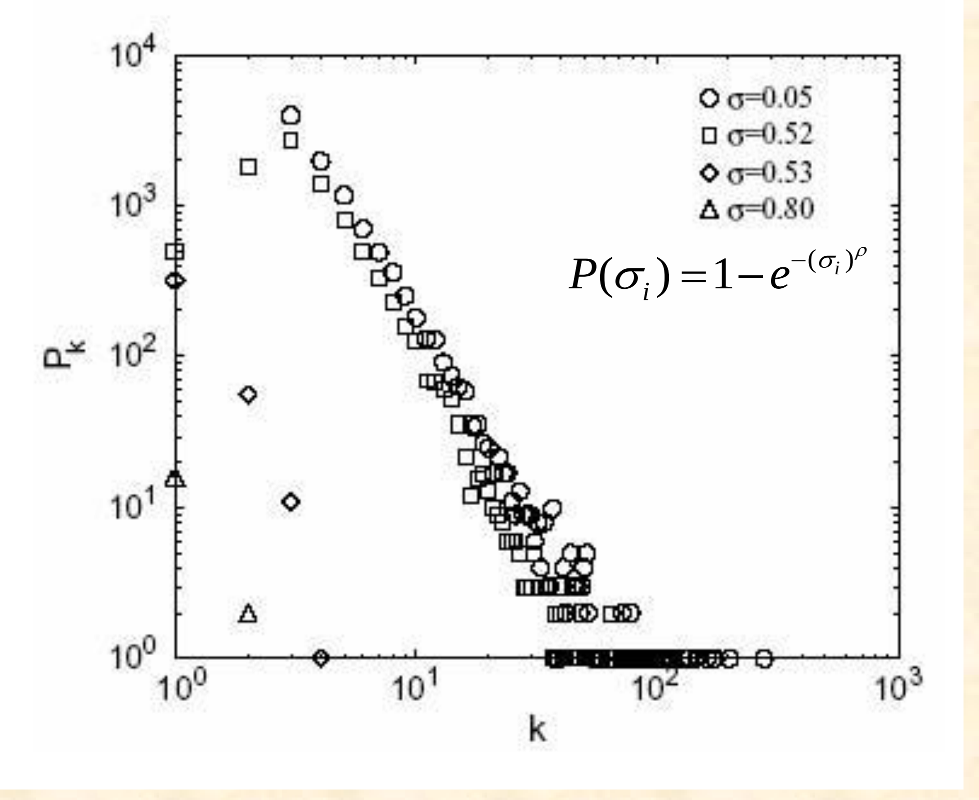
$$f_k(x) = \frac{k}{\lambda}\left(\frac{x}{\lambda}\right)^{k-1} e^{-(x/\lambda)^k}$$



k and λ are constant parameters

Cumulative distribution function: $1 - e^{-(x/\lambda)^k}$

Fiber-Bundle Model Built on a BA Network

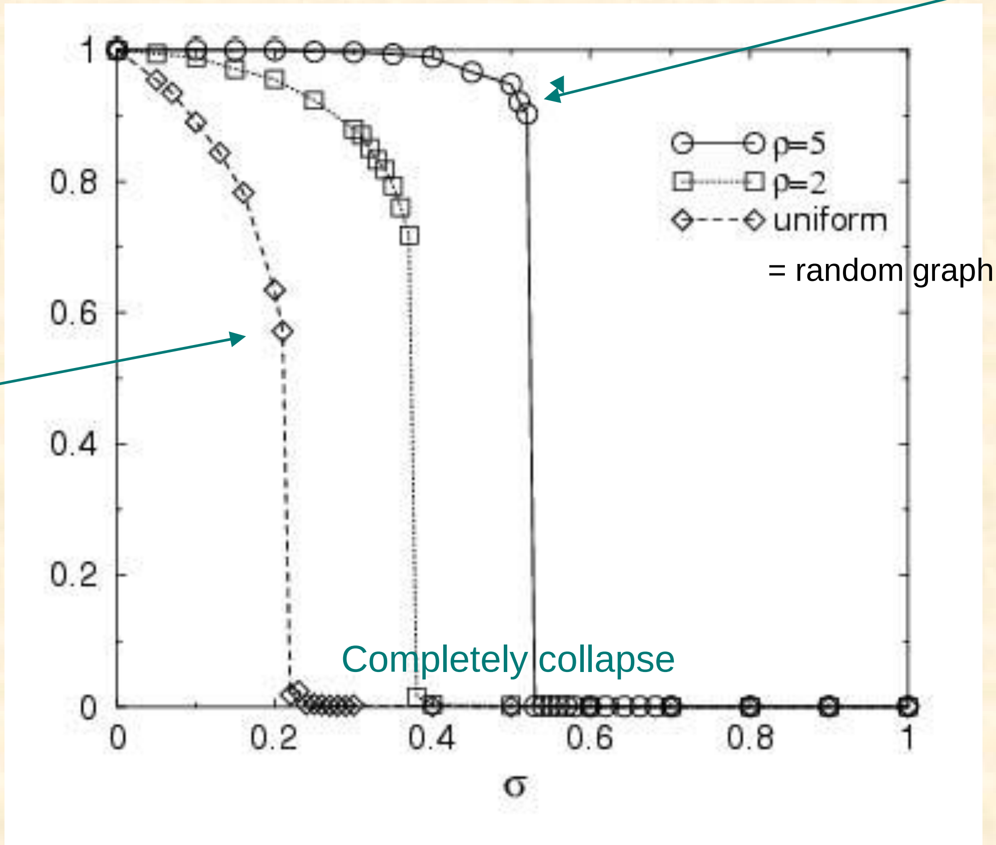


Power-law distributions of degree-k nodes for small σ

Moreno et al. (2002)

Fiber-Bundle Model

Fraction of connected sub-nets



more severe

(whole network collapses even when only 10% nodes are disconnected)

less severe

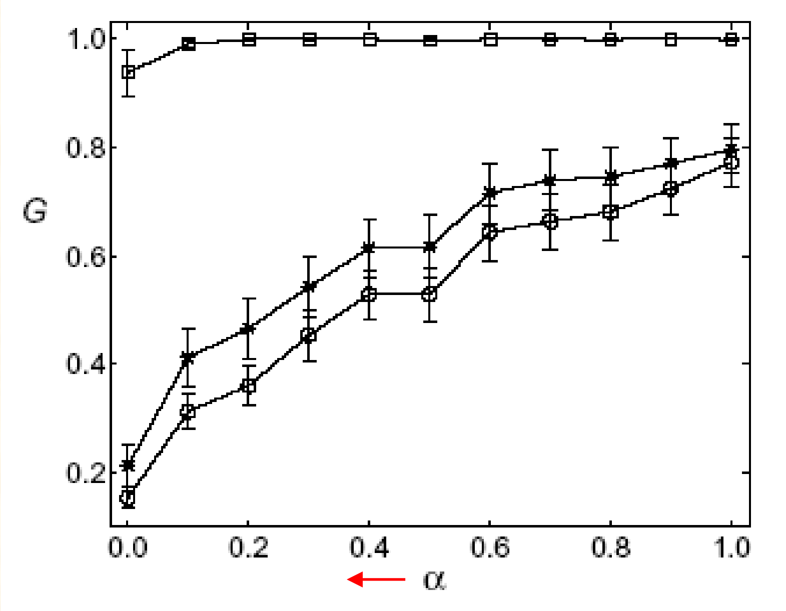
(network not collapses unless 40% nodes are disconnected)

BA scale-free network: $N = 10{,}000$ $\quad P(\sigma_i) = 1 - e^{-(\sigma_i)^{\rho}}$

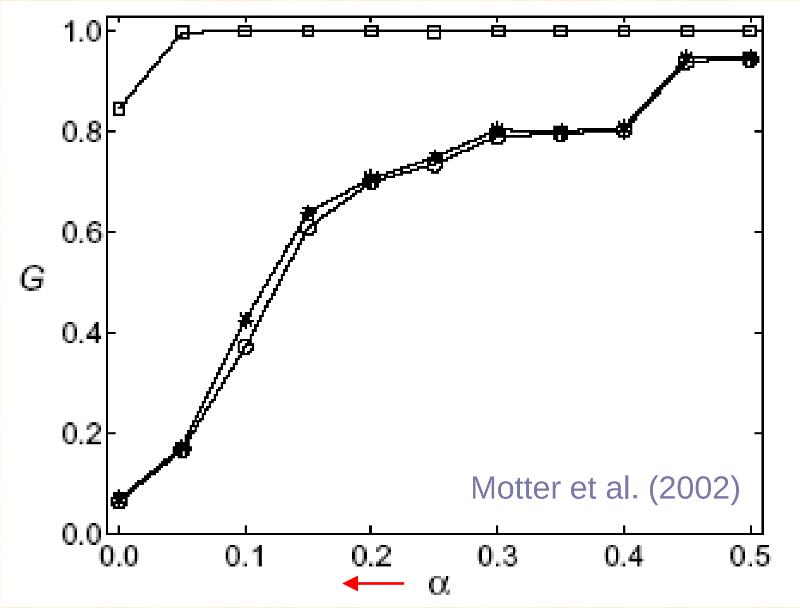
Moreno et al. (2002)

Node-Betweenness Model

Replace “load capacity” by “node-betweenness”



Scale-free network model



AS-level real Internet

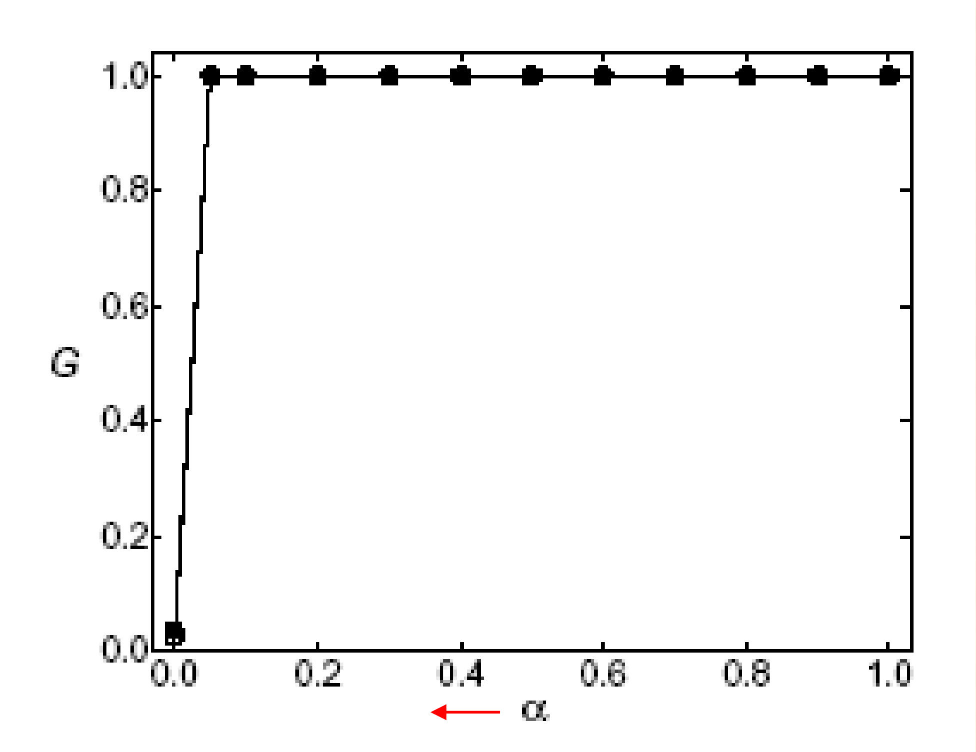
G is the fraction of remaining connected sub-nets over the whole network

[square curves correspond to random node failures, star curves to largest-degree node failures, and circle curves to biggest-betweenness node failures]

Observation 1: smaller tolerance → more severe failure

Observation 2: largest-degree/betweenness failures is more severe than random failures

Node-Betweenness Model



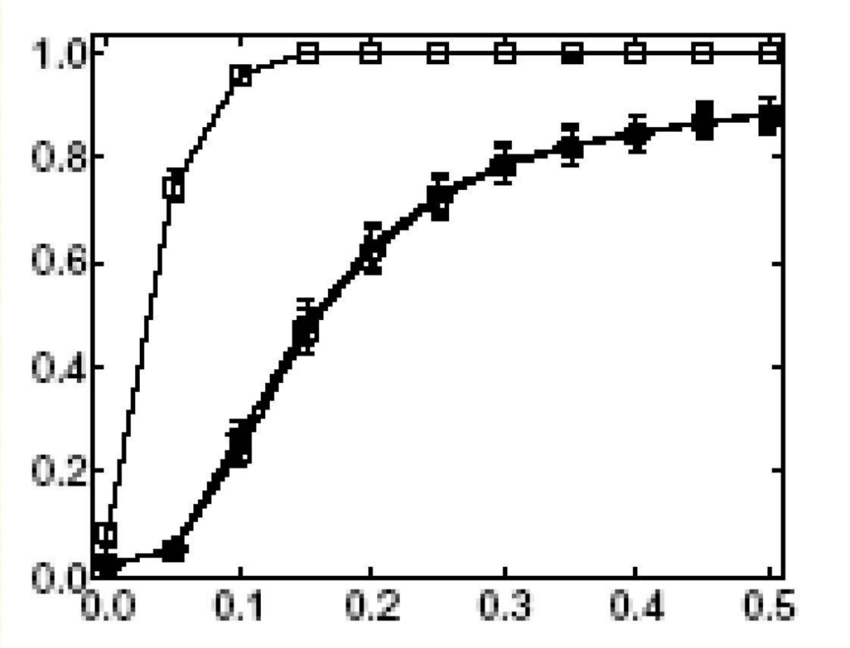
Motter et al. (2002)

Comparison of cascading failures on random networks

square – random attack, circles – intentional attack. $N = 5{,}000$ $\langle k \rangle \approx 3$

Observation 1: For random graphs, both random and intentional attacks perform similarly

Node-Betweenness Model



Motter et al. (2002)

Comparison of cascading failures on scale-free networks

square – random attack, circles – intentional attack. $N = 5{,}000$ $\langle k \rangle \approx 3$

Observation 2: For scale-free networks, intentional attacks are more severe than random attacks

Cascading Failures: Models and Analysis

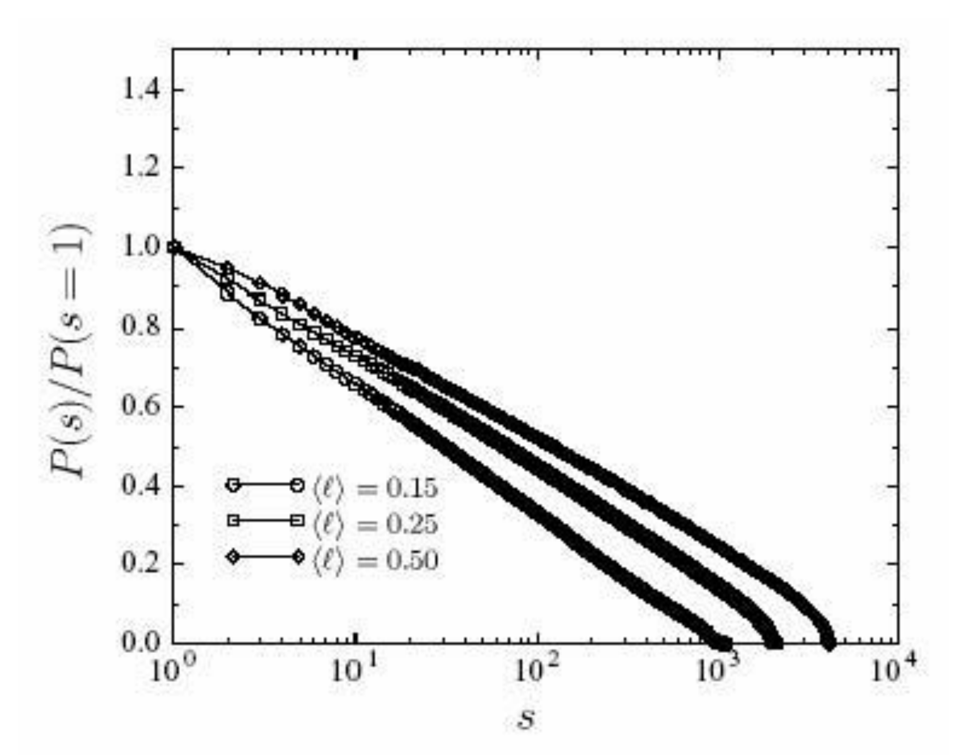
Models Based on Edge Dynamics

Consider loads on edges

Let s be the number of overloaded edges

Let $P(s)$ be the cumulated failures (normalized)

Let $\langle \ell \rangle$ be the average edge loading over the whole network



Moreno et al. (2003)

Cascading Failures

A model based on both node and edge dynamics

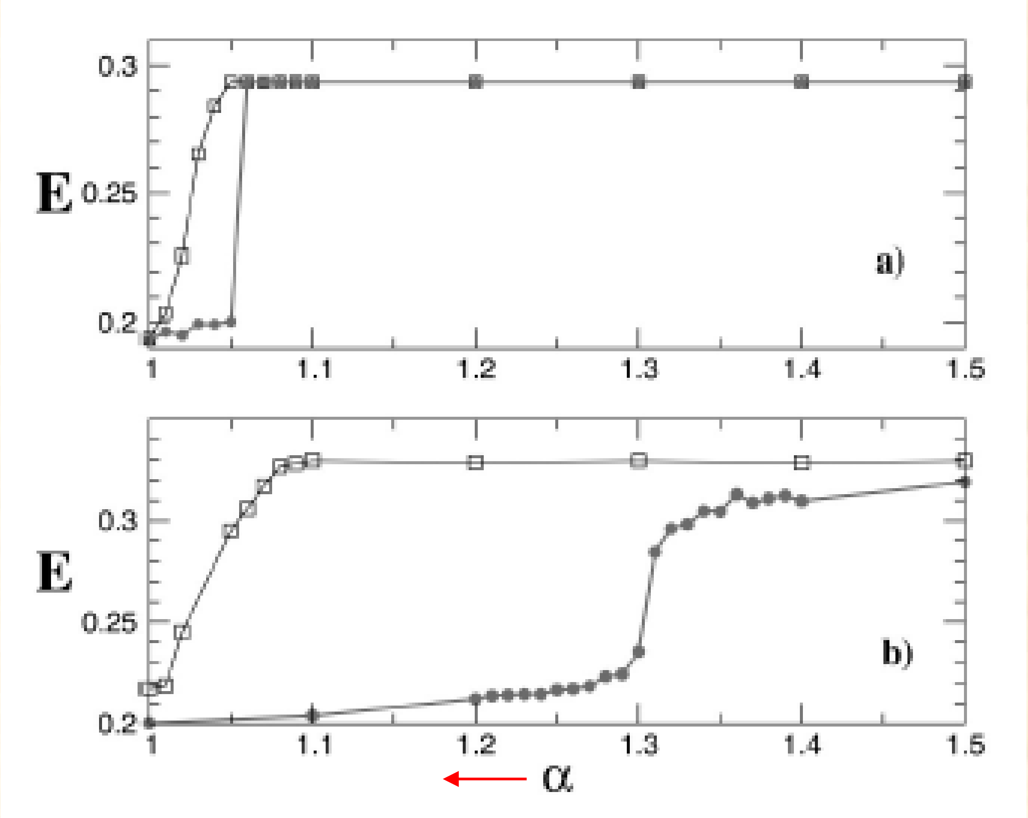
$e_{ij} \in [0,1]$ – efficiency of edge (i,j), e.g., bandwidth

E – average efficiency:

$$E(G) = \frac{1}{N(N-1)} \sum_{i \neq j} e_{ij}$$

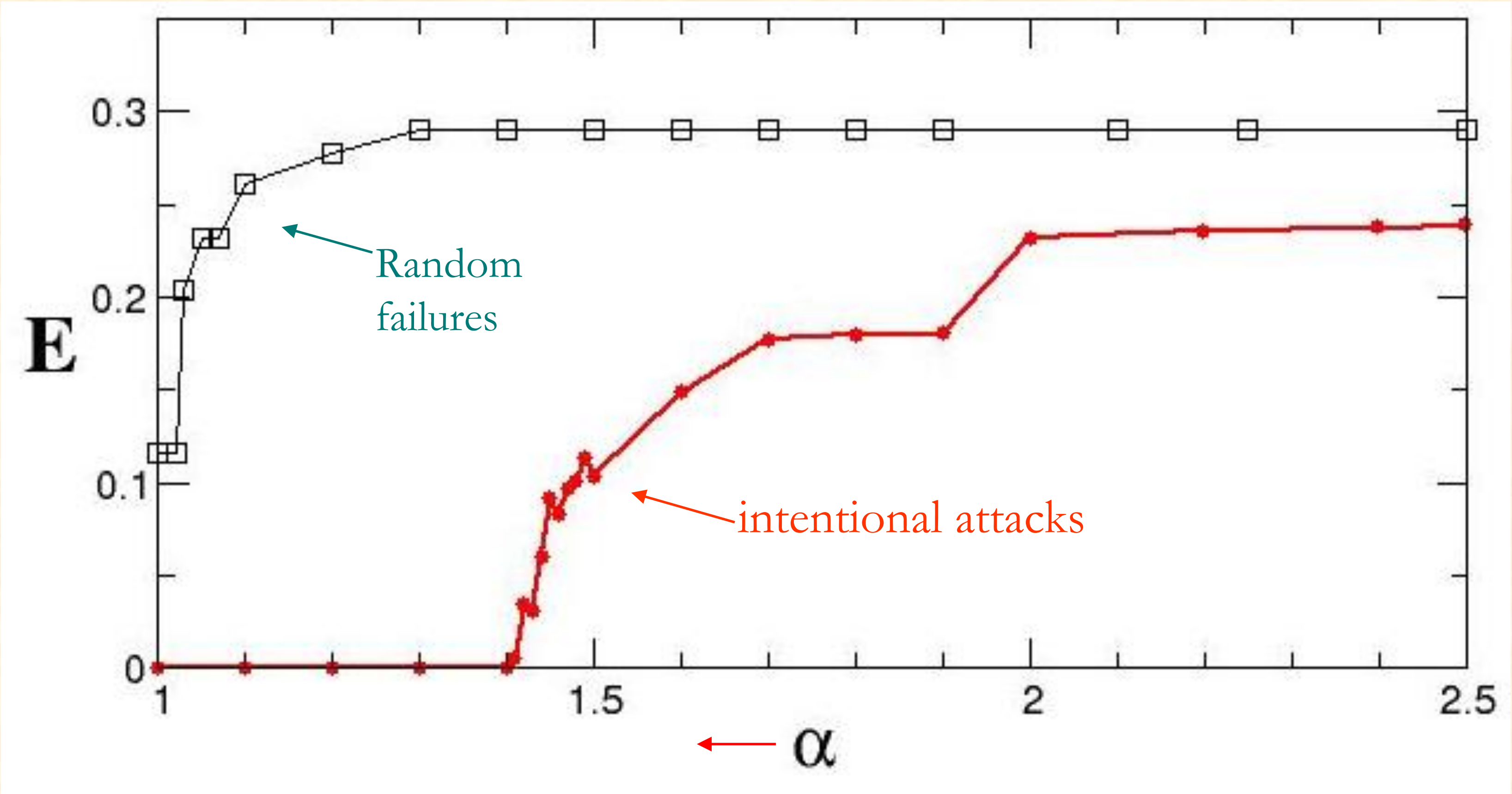
$L_i(t)$ -- loading
$C_i = \alpha \cdot L_i(0)$ -- capacity
$\alpha \geq 1$ -- tolerance

Crucitti et al. (2004)



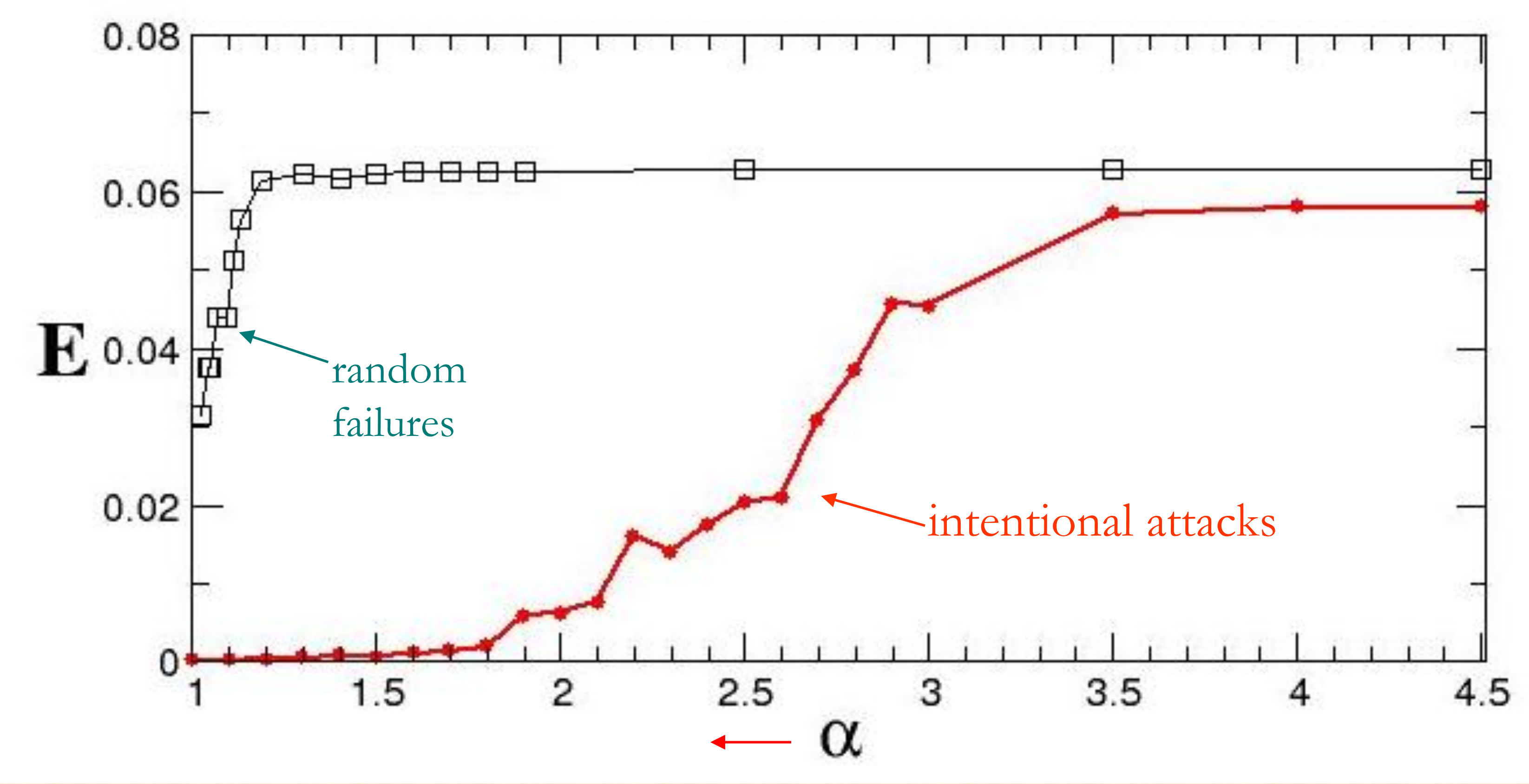
a) ER network, b) BA network. [squares -- random node failures, circles -- biggest node failures]

AS-level Internet (Real Data)



Crucitti et al. (2004)

US Power Grid (Real Data)



Crucitti et al. (2004)

Interdependent Networks

SCIENTIFIC AMERICAN™

Winner of the 2011 National Magazine Award for General Excellence

Search ScientificAmerican.com

News & Features | Blogs | Multimedia | Education | Citizen Science | Topics

Home » Scientific American Magazine » July 2011

Feature Articles | Technology

12 Like

Hacking the Lights Out: The Computer Virus Threat to the Electrical Grid

Computer viruses have taken out hardened industrial control systems. The electrical power grid may be next

By David M. Nicol | June 20, 2011

Interdependent Networks

Network of Networks in the real world

Example: human mobility networks

short-range interconnected flows by cars, trains, ferries, etc.

long-range commuting flows like air-flights

communication network flows (phones and the Internet).

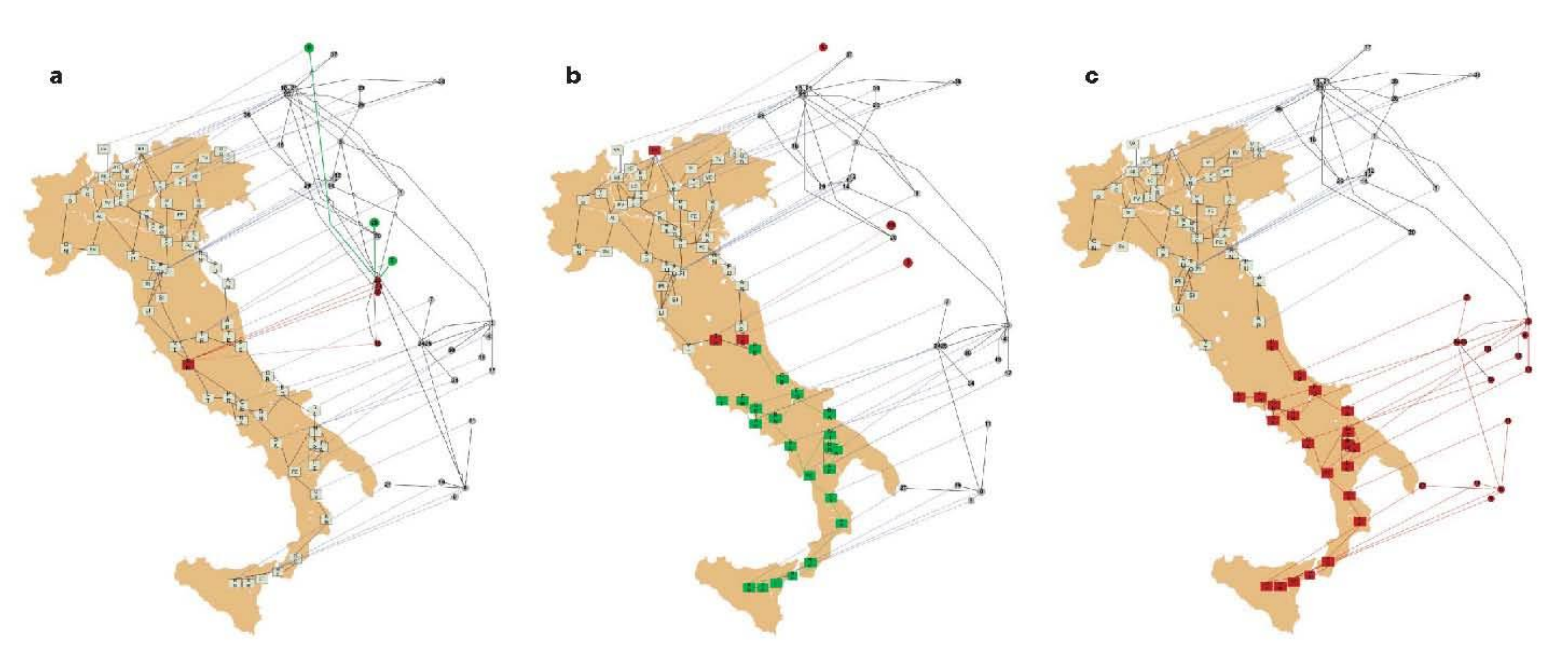
Interdependent Networks of human mobility in the North America

blue – short-range

brown – long-range

Vespignani, Nature (2010) 464: 984-985

A Real-World Example: Italy Blackout in 2003



a One power station failed (red) → a few associated Internet servers failed (red), and some Internet servers are isolated (green)

b The above failed Internet servers (red) and associated edges are removed → related power stations failed (red), and some power stations became isolated (green)

c The above failed power stations (red) and Internet servers (red) are removed → both networks failed (both red) → system collapsed

Buldyrev et al. Nature (2010) 464: 1025-1028

Cyber-attack to Power Grids

CBC news | Technology & Science

Home | World | Canada | Politics | Business | Health | Arts & Entertainment | Technology & Science | Trending | Video

Technology & Science | Quirks & Quarks Blog | Spark | Photo Galleries

Cyberattack that crippled Ukrainian power grid was highly coordinated

1st power outage caused by cyberattack suggests similar attacks possible around the globe

Thomson Reuters Posted: Jan 11, 2016 11:52 AM ET | Last Updated: Jan 11, 2016 12:17 PM ET

(Getty Images)

324 shares

Facebook

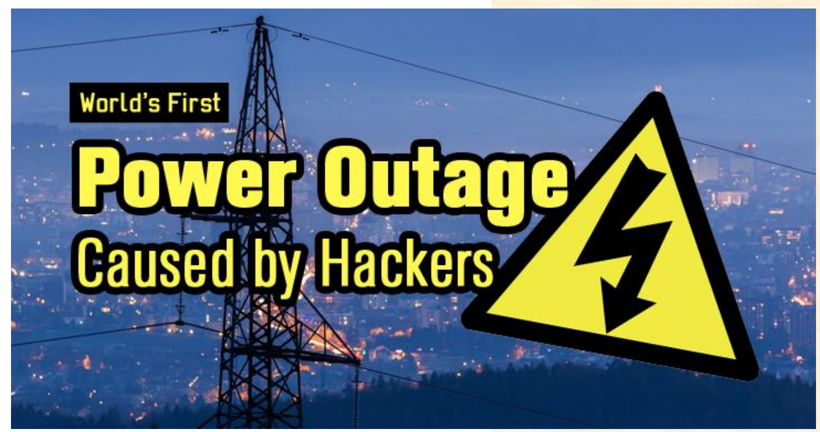
Hackers likely caused a Dec. 23 electricity outage in Ukraine by remotely switching breakers to cut power, after installing malware to prevent technicians from detecting the attack, according to a report analyzing how the incident unfolded.

Stay Connected with CBC News

Mobile Facebook Podcasts Twitter Alerts Newsletter

Top News Headlines

▪ Murray Sinclair, Chantal



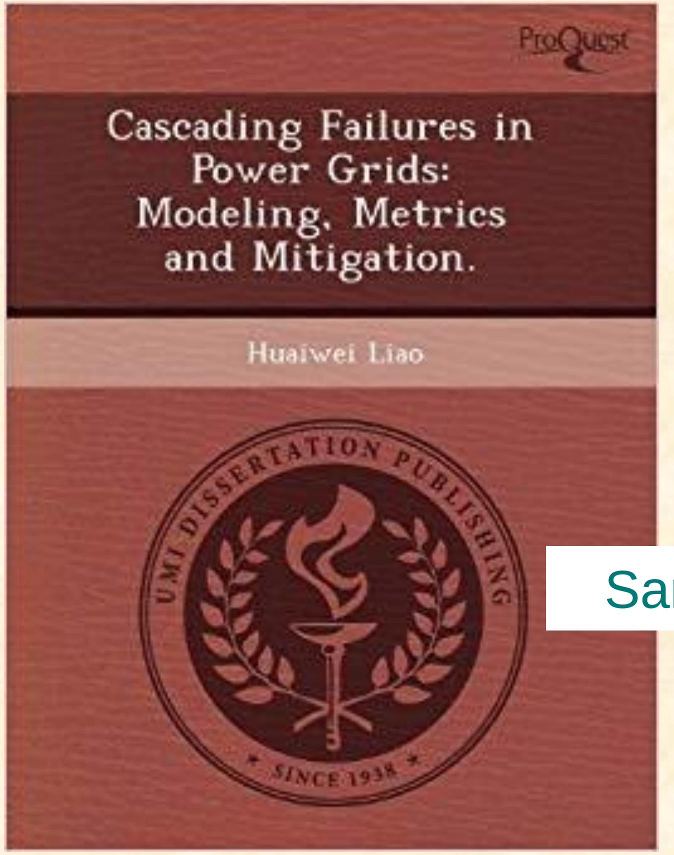
On 23 December 2015

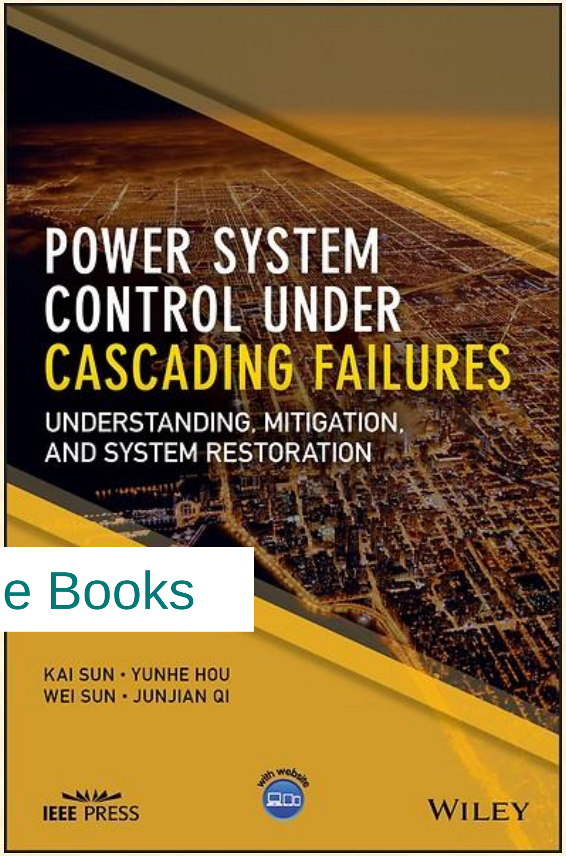
Cyber-attack to Power Grids

2015 年 12 月 23 日，乌克兰电网遭遇突发停电事故，据媒体报道，本次停电事故由 7 个变电站开关动作引起，导致 80 000 个用户停电，停电时间为 3～6 h 不等。事故后，调查机构在电力调度通信网络中获取部分恶意软件的样本，结合停电过程的特征及影响，信息安全组织 SANS ICS 于 2016 年 1 月 9 日明确宣称，本次事件确定为“网络协同攻击”造成的乌克兰电网停电事故（https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid）。

Power Grid Cascading Failures

Models, Analysis → Prevention, Control





Sample Books

End