

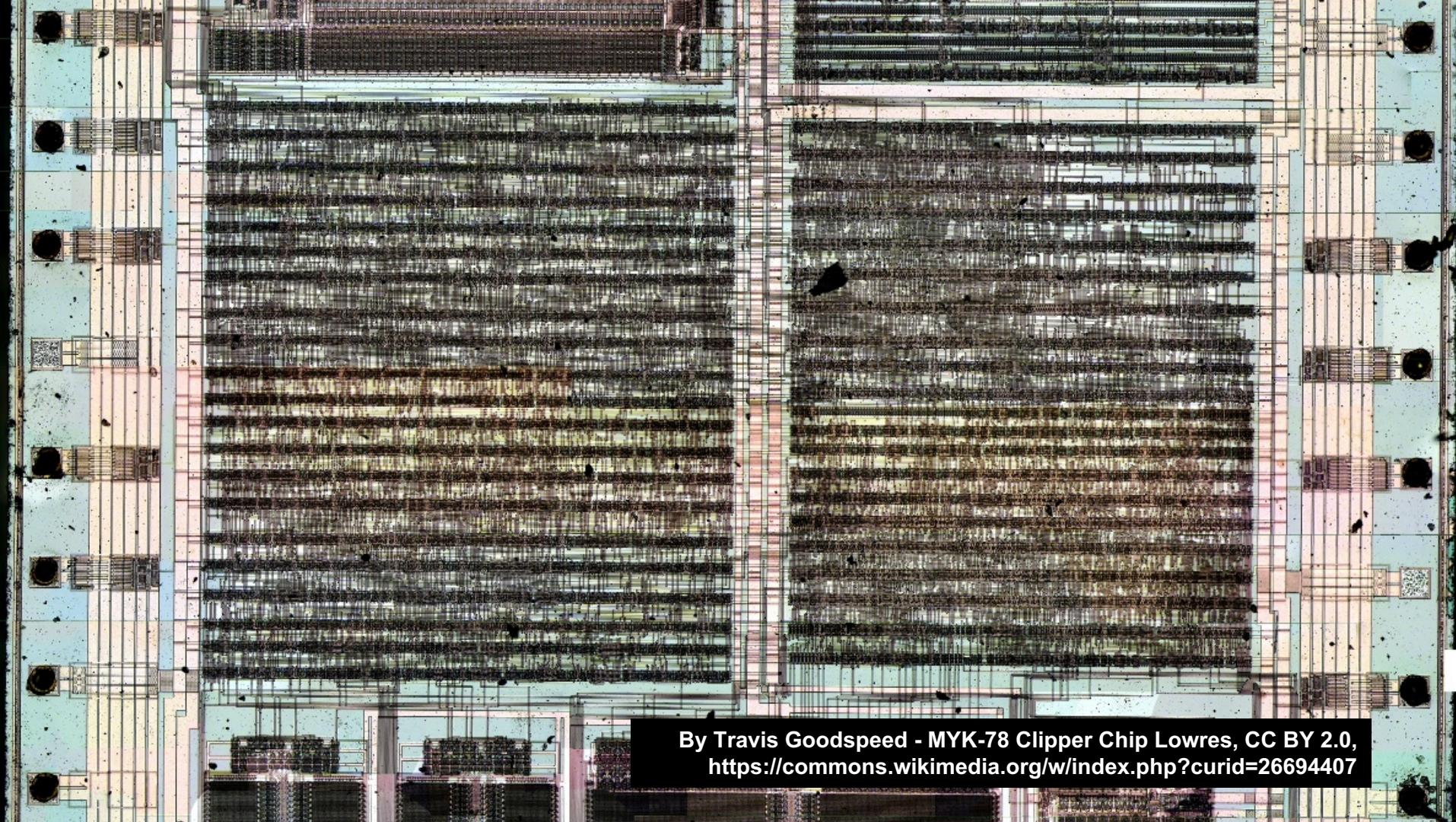


Revisiting the state

Maarten Van Horenbeeck
VP, Security Engineering
Fastly







By Travis Goodspeed - MYK-78 Clipper Chip Lowres, CC BY 2.0,
<https://commons.wikimedia.org/w/index.php?curid=26694407>

Crypto wars

- Should the government be able to read private communications?
- Do corporations have a duty to collect information?

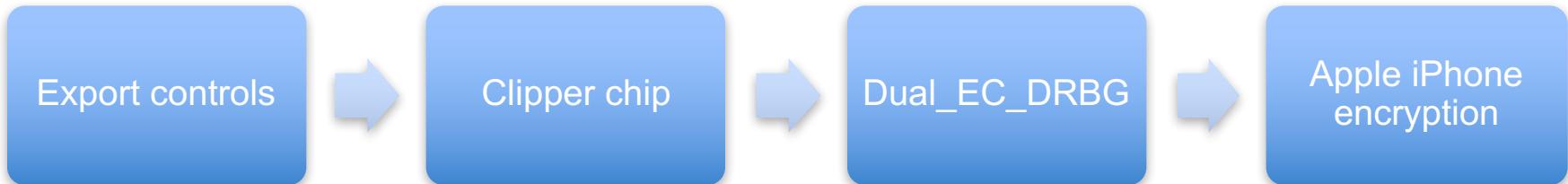
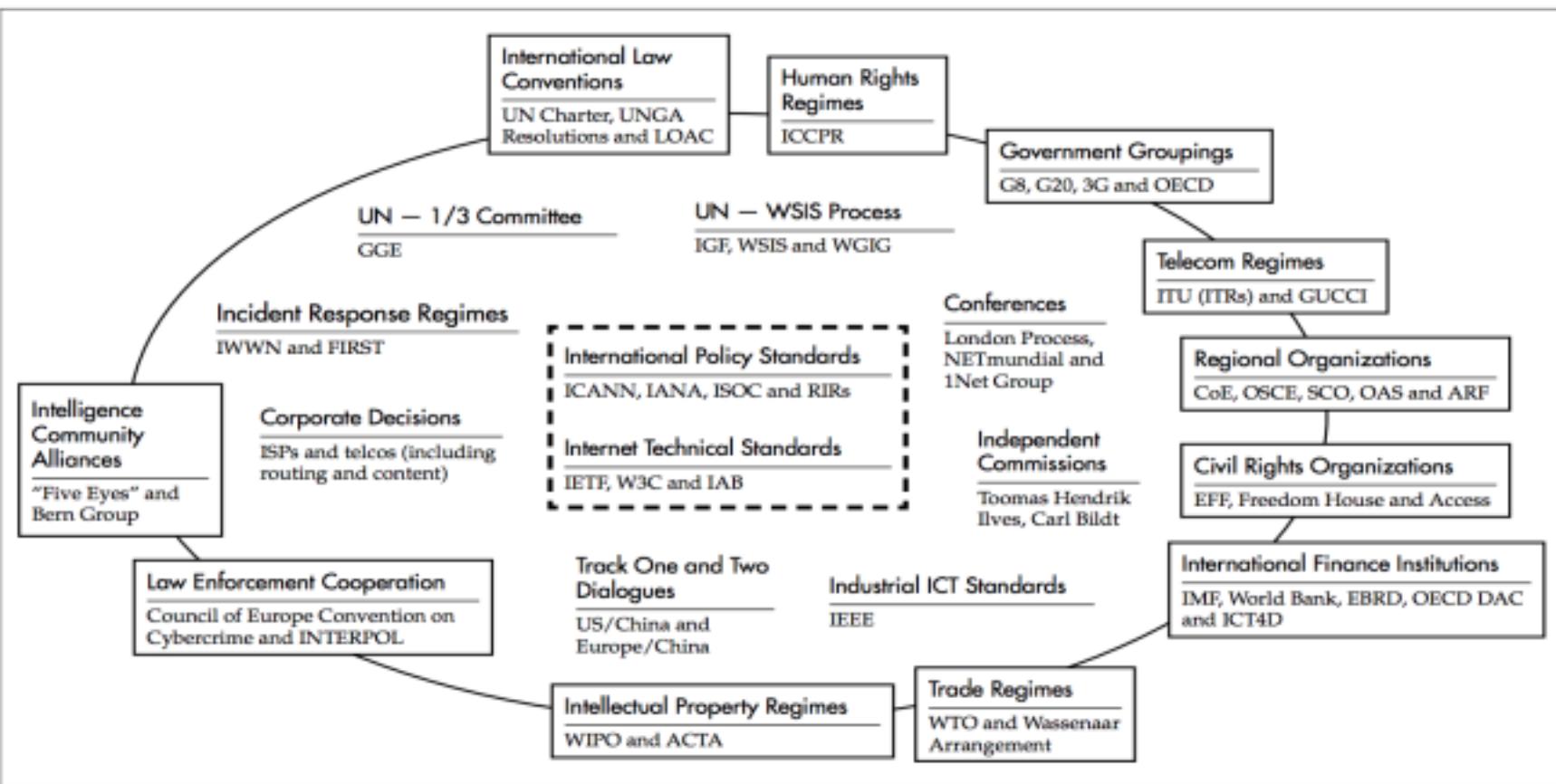




Figure 1: The Regime Complex for Managing Global Cyber Activities



Source: Joseph S. Nye, Jr. – The Regime Complex for Managing Global Cyber Activities

States

- Borders
- Law
- Ability to engage with other states
- Max Weber's "Monopoly on violence"
- States typically provide at least some services to their population





DigiNotar



★ Is This MITM Attack to Gmail's SSL ? ⓘ

[ADD A REPLY](#)

by alibo 8/27/11

Hi,

Today, when I tried to login to my Gmail account I saw a certificate warning in Chrome .
I took a screenshot and I saved certificate to a file .

this is the certificate file with screenshot in a zip file:

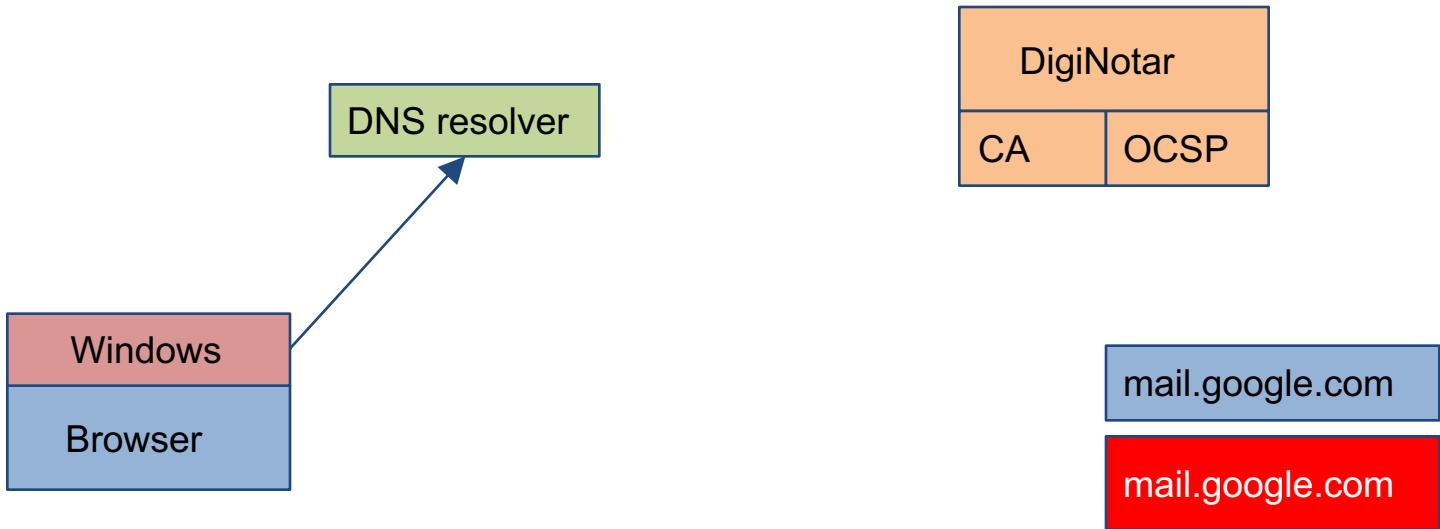
<http://www.mediafire.com/?mrkib17s1ctiyb>

and this is text of decoded fake certificate:

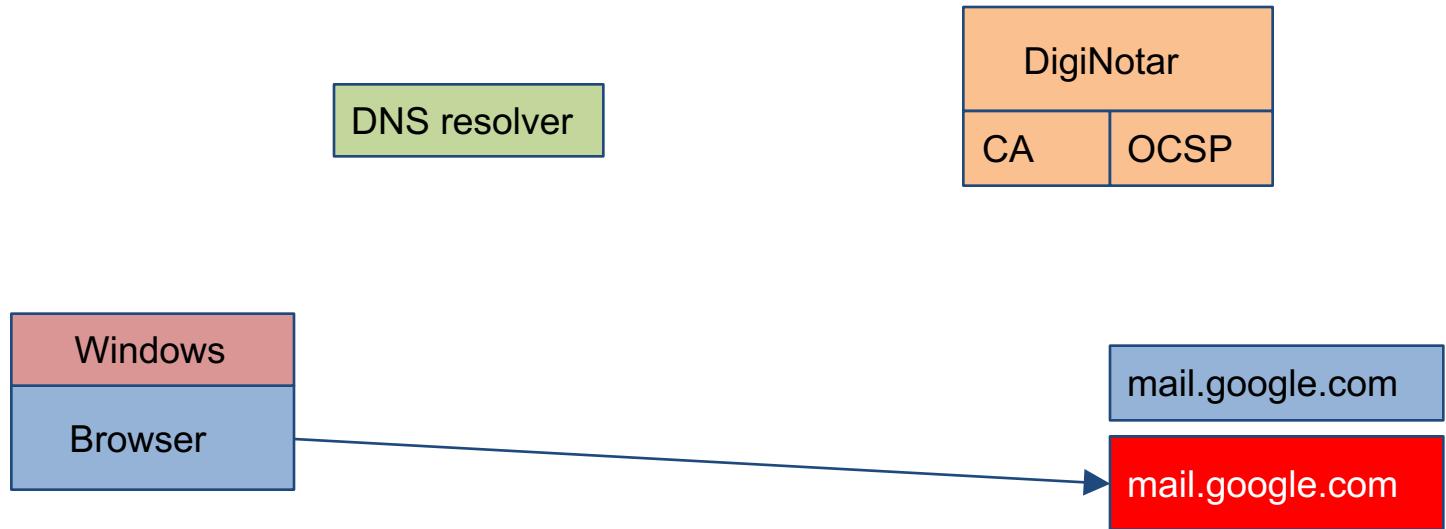
<http://pastebin.com/ff7Yg663>

when I used a vpn I didn't see any warning ! I think my ISP or my government did this attack (because I live in Iran and you may hear something about the story of Comodo hacker!)

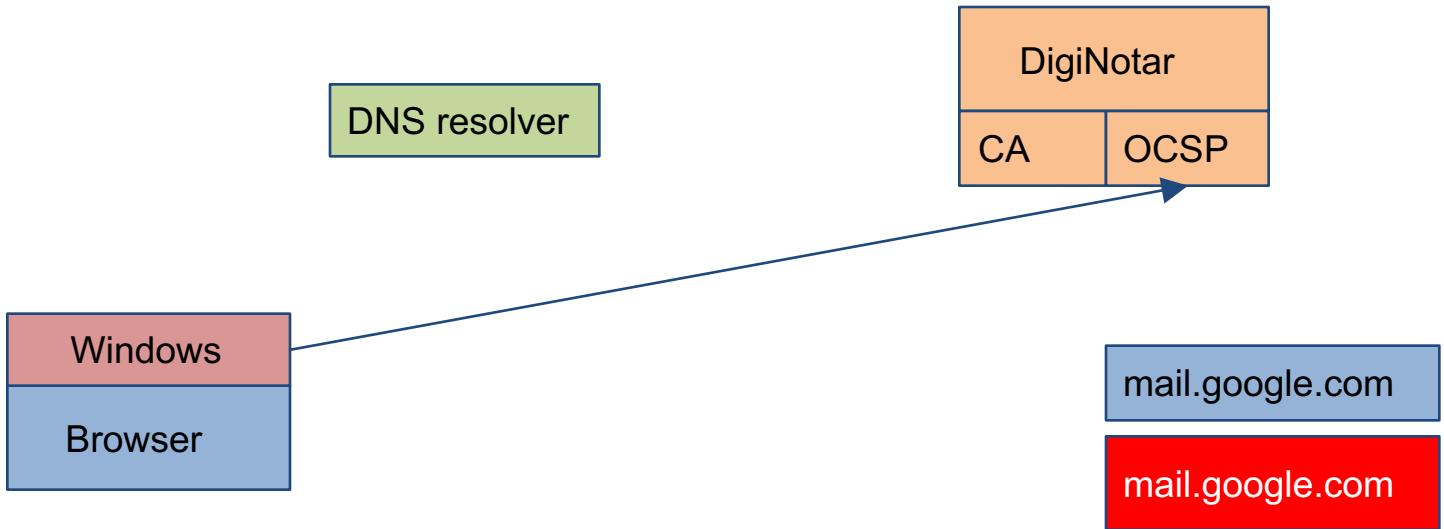
DigiNotar



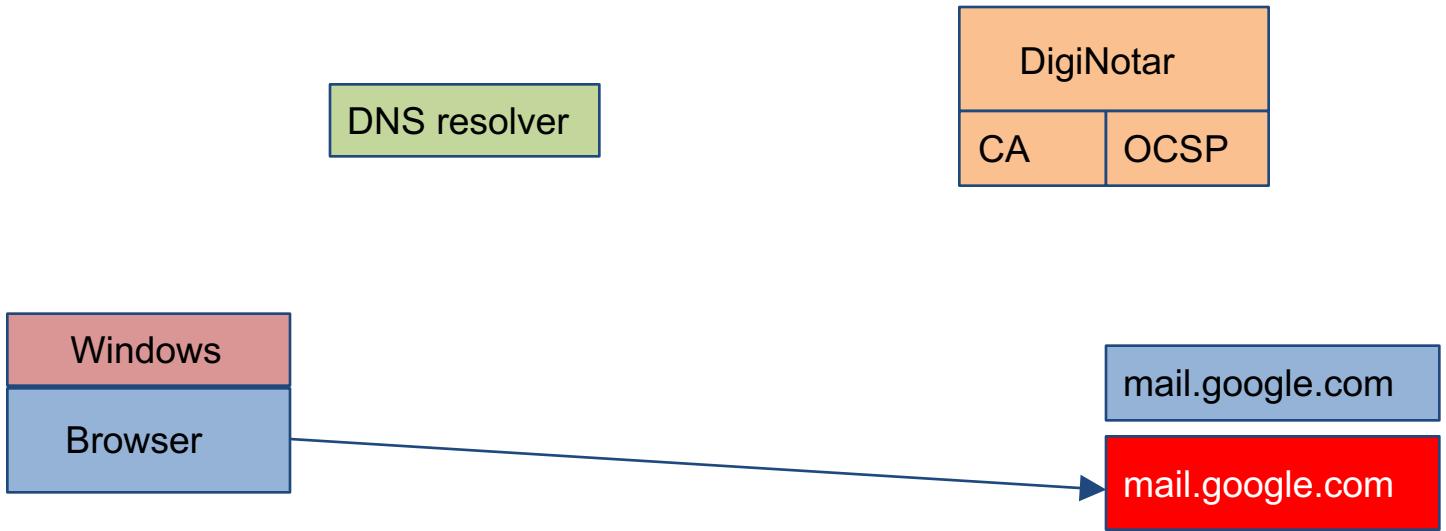
DigiNotar



DigiNotar



DigiNotar



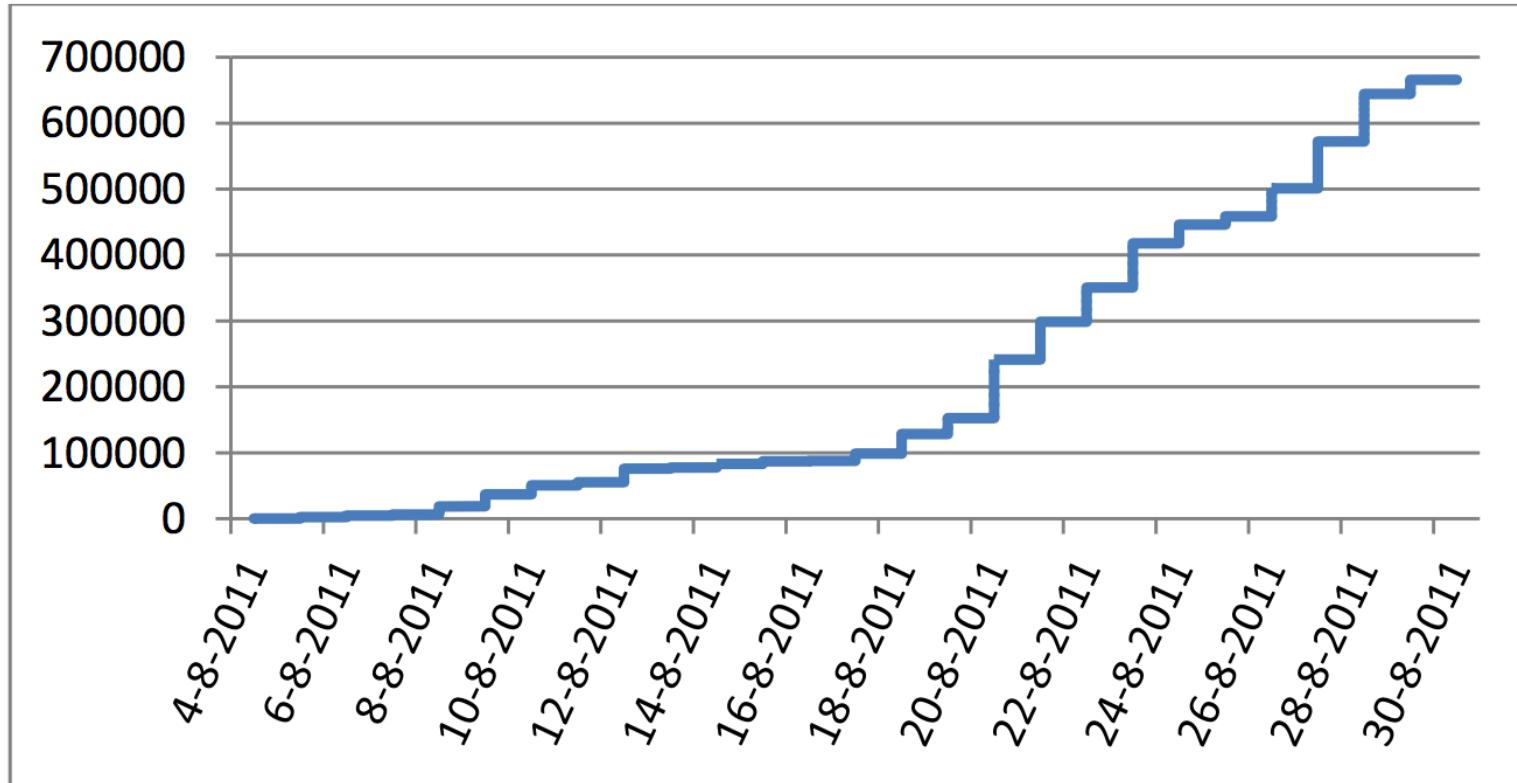
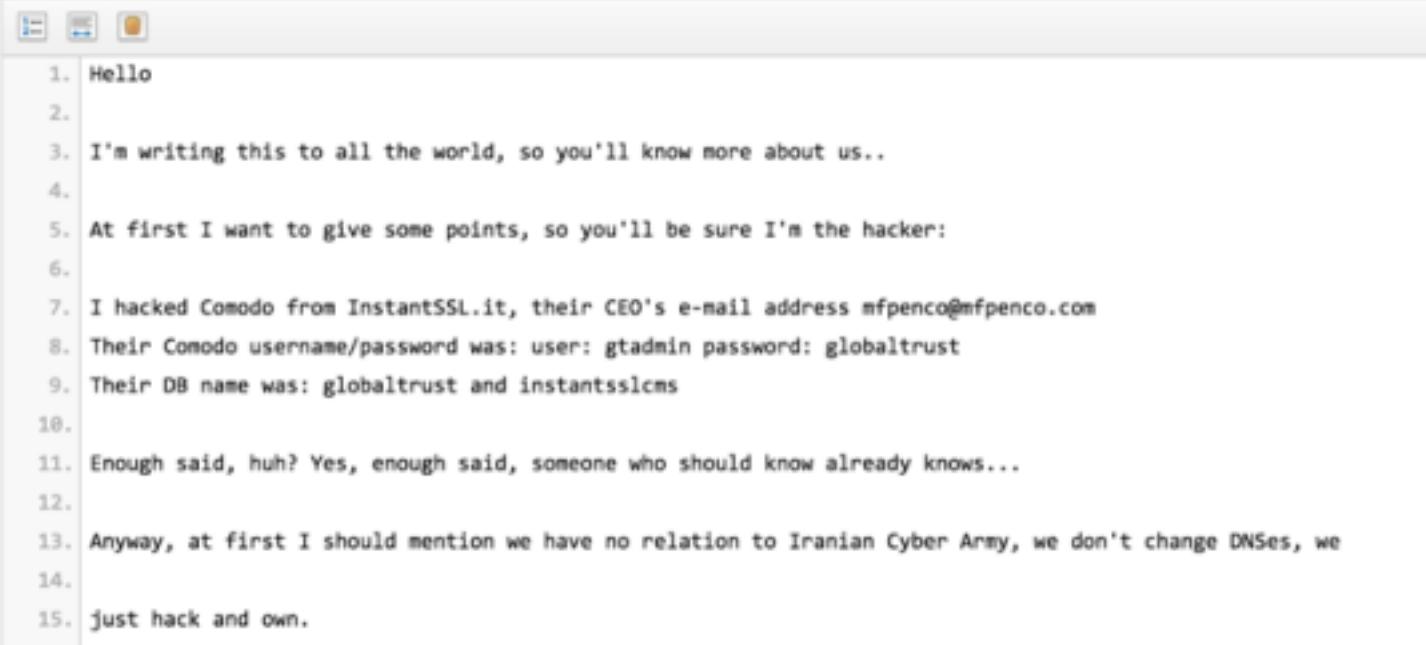


Figure 6 Cumulative number of originating IP addresses

Source: Fox-IT – Black Tulip: Investigation into DigiNotar

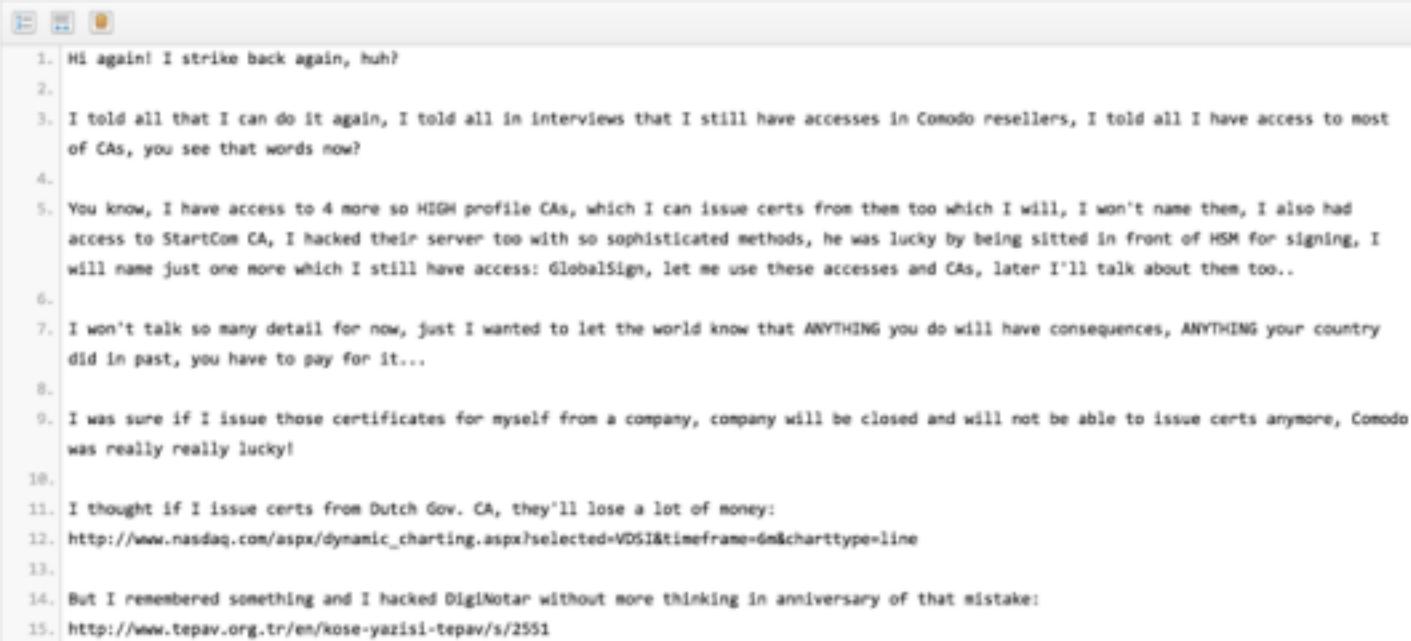
DigiNotar



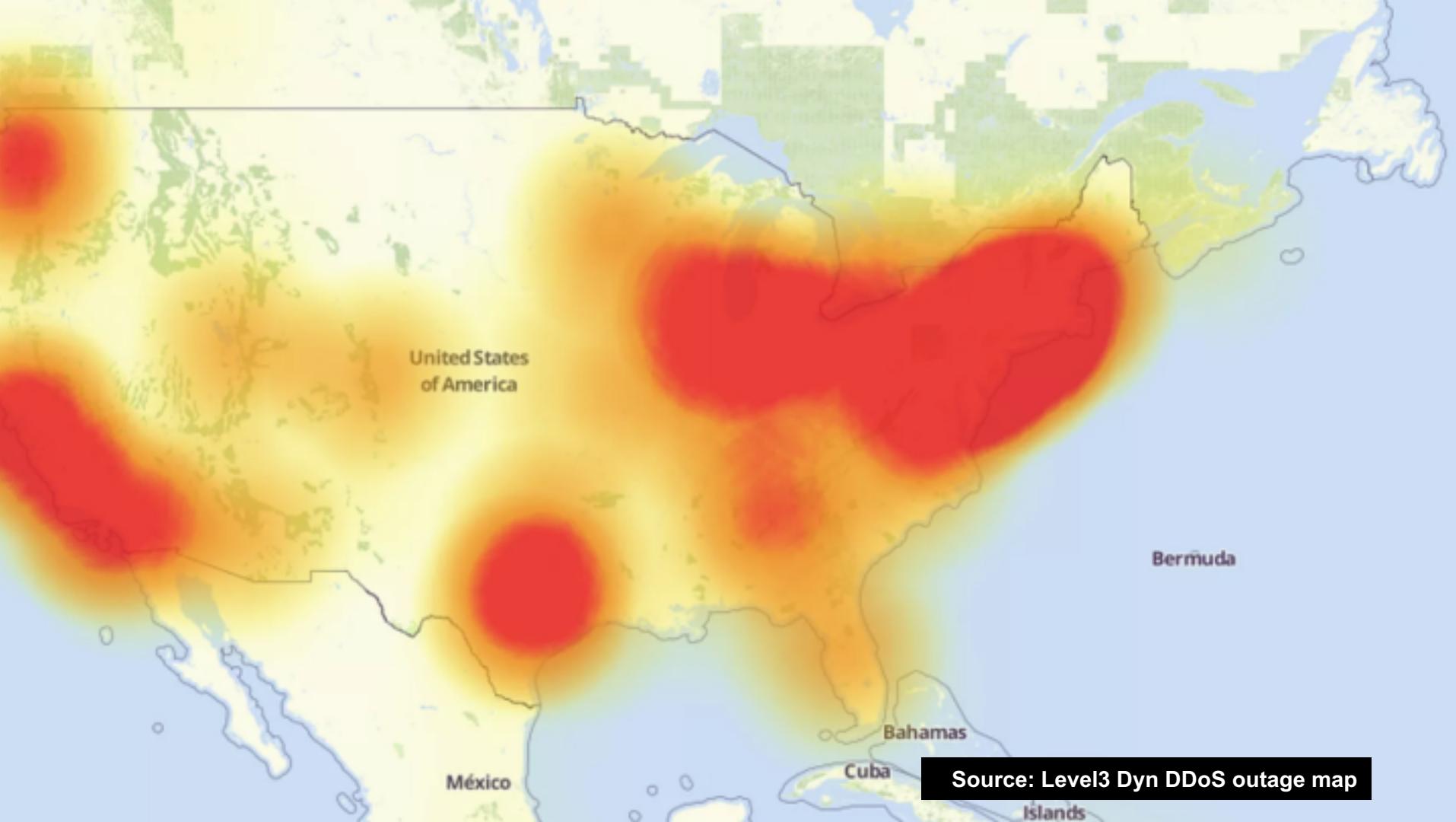
A screenshot of a Windows-style Notepad window. The window title bar is visible at the top. The main area contains a list of numbered points, each starting with a small black dot and followed by text. The text is in a monospaced font.

```
1. Hello
2.
3. I'm writing this to all the world, so you'll know more about us..
4.
5. At first I want to give some points, so you'll be sure I'm the hacker:
6.
7. I hacked Comodo from InstantSSL.it, their CEO's e-mail address mfpenco@mfpenco.com
8. Their Comodo username/password was: user: gtadmin password: globaltrust
9. Their DB name was: globaltrust and instantsslcms
10.
11. Enough said, huh? Yes, enough said, someone who should know already knows...
12.
13. Anyway, at first I should mention we have no relation to Iranian Cyber Army, we don't change DNSes, we
14.
15. just hack and own.
```

DigiNotar



1. Hi again! I strike back again, huh?
2.
3. I told all that I can do it again, I told all in interviews that I still have accesses in Comodo resellers, I told all I have access to most of CAs, you see that words now?
4.
5. You know, I have access to 4 more so HIGH profile CAs, which I can issue certs from them too which I will, I won't name them, I also had access to StartCom CA, I hacked their server too with so sophisticated methods, he was lucky by being sitted in front of HSM for signing, I will name just one more which I still have access: GlobalSign, let me use these accesses and CAs, later I'll talk about them too..
6.
7. I won't talk so many detail for now, just I wanted to let the world know that ANYTHING you do will have consequences, ANYTHING your country did in past, you have to pay for it...
8.
9. I was sure if I issue those certificates for myself from a company, company will be closed and will not be able to issue certs anymore, Comodo was really really lucky!
10.
11. I thought if I issue certs from Dutch Gov. CA, they'll lose a lot of money:
12. http://www.nasdaq.com/aspx/dynamic_charts.aspx?selected=VDG1&timeframe=6m&charttype=line
13.
14. But I remembered something and I hacked DigiNotar without more thinking in anniversary of that mistake:
15. <http://www.tepav.org.tr/en/kose-yazisi-tepav/s/2551>



Source: Level3 Dyn DDoS outage map

States, revisited

- Borders ?
- Law
- Ability to engage with other states
- Max Weber's "Monopoly on violence"
- States typically provide at least some services to their population

States, revisited

- Borders ?
- Law ?
- Ability to engage with other states
- Max Weber's "Monopoly on violence"
- States typically provide at least some services to their population

States, revisited

- Borders ?
- Law ?
- Ability to engage with other states ?
- Max Weber's "Monopoly on violence"
- States typically provide at least some services to their population

States, revisited

- Borders ?
- Law ?
- Ability to engage with other states ?
- Max Weber's "Monopoly on violence" ?
- States typically provide at least some services to their population

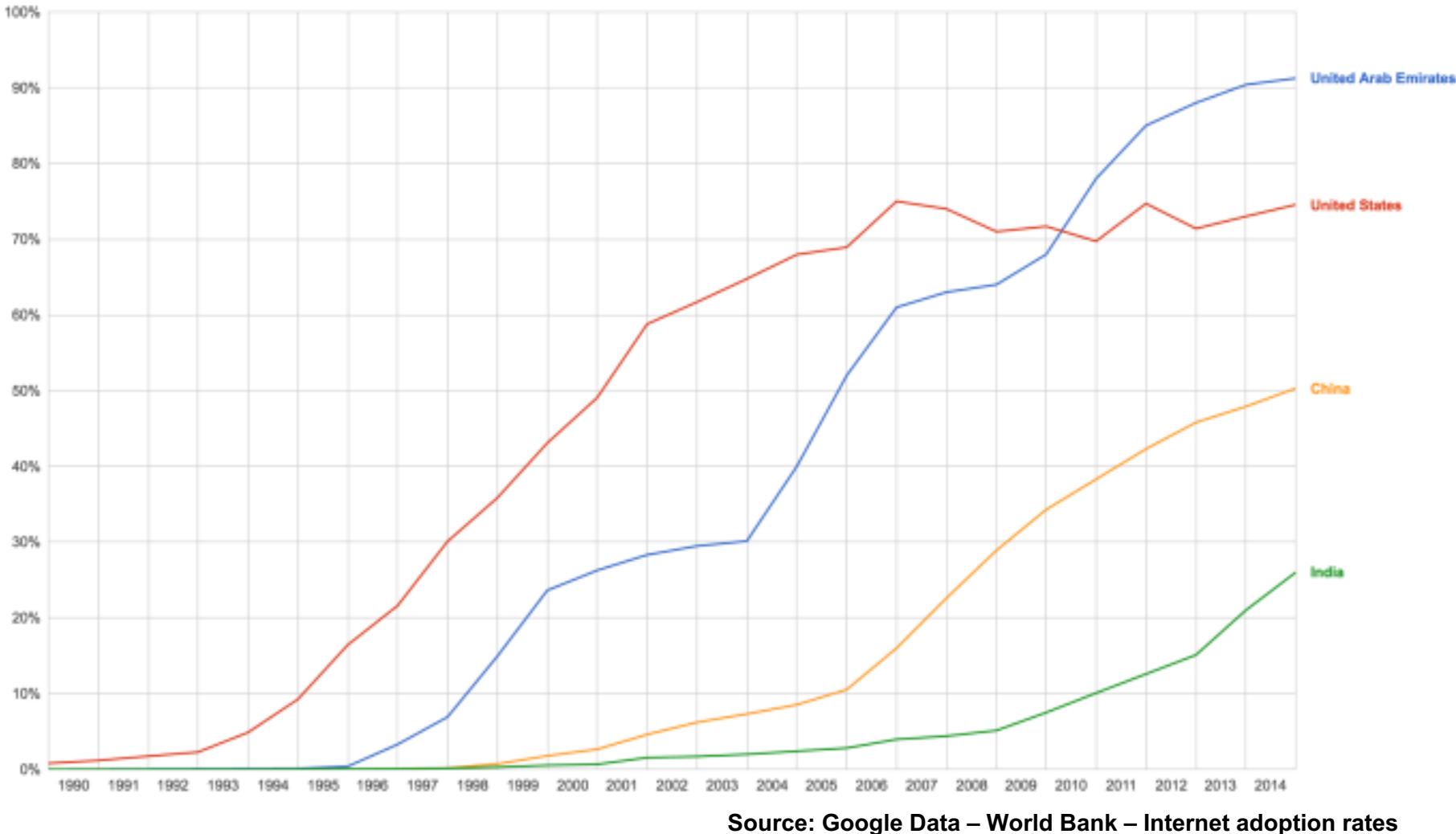
States, revisited

- Borders ?
- Law ?
- Ability to engage with other states ?
- Max Weber's "Monopoly on violence" ?
- States typically provide at least some services to their population ?

In comes the internet

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of the service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge, and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals.

You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.



A history of issues

- Different perspectives
 - National security
 - Social concerns
 - Economic impact
- No consistent **legal framework**
- Lack of clear **attribution**
- Lack of clear **intent**
- **Lack of trust** between governments

Budapest convention

- Council of Europe
- International treaty to harmonize national laws
- Adopted in November of 2001, with 52 states ratified so far
- Supports international law enforcement cooperation



United Nations

- **Call for input** from 2010 through 2016
 - Countries can share their own projects and progress
 - Flag issues they have that require international collaboration
- Government Group of Experts (**UNGGE**)
- **International Telecommunications Union**
 - Build confidence and security
 - Global Cybersecurity Agenda
- **Internet Governance Forum**



“Talinn Manual”

- Born out of 2007 Estonia cyber attacks
- Analysis of how existing law applies to cyberspace
- Cyber events incur rights and obligations on behalf of countries
- First edition covered important operations that involved states defending themselves, or stepping beyond regular international relations
- Second edition adds legal analysis of more common incidents

Global Conference on Cyberspace

- “*London Process*”
- **London:** Set of principles for “governing behavior in cyberspace”
- **Budapest:** emerging issues, internet rights and security
- **Seoul:** increased representation from countries,
“open and secure cyberspace”
- **The Hague:** greater representation from non-state actors
- **Hyderabad 2017**
- Outcomes include “Chair’s statement” and year specific goals

Wassenaar

- Export control for **dual use goods**
 - Includes **intrusion and surveillance** technologies
 - Consensus
 - Voluntary compliance
4. A. 5. Systems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".

Wassenaar

“Intrusion Software”—

Software specially designed or modified to avoid detection by ‘monitoring tools’, or to defeat ‘protective countermeasures’ of a computer or network capable device, and performing any of the following:

- a. The extraction of data or information, from a computer or network capable device, or the modification of data of a system or user; or
- b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions; or

Regional processes



ASSOCIATION
OF SOUTHEAST
ASIAN NATIONS



- **ASEAN:** ASEAN Way, develop more predictable relationships
- **SCO:** proposed international code of conduct under the UN
 - Focus on multilateral approach vs. multi-stakeholder
 - Highlights "sovereignty"
- Implications on where technology originates from

Mechanisms

- **Laws and treaties**
 - Signers accept roles and responsibilities
 - Ability to be held liable
- **Confidence Building Measures**
 - Opportunities for states to interact, often on a voluntary basis
 - Enables growth of interaction and cooperation
 - Developing shared approaches to problems
- **Norms of behavior**
 - Confirmed and enforced through behaviors between groups of actors
 - You distinguish norms through other's reaction when they are violated

Norms development

Proposer	Language	Affected party
UNGGE	states should not conduct or knowingly support activity to harm the information systems of another state's CSIRT and should not use their own teams for malicious international activity;	States
GCCS	States should establish hotlines to enable de-escalation for major cyber- incidents and these should enjoy special protected status.	States
Microsoft	Global ICT Companies should issue patches to protect ICT users, regardless of the attacker and their motives	Global ICT companies

A photograph of a dense crowd of people walking away from the viewer on a city street. The scene is filled with backs and profiles of people in various attire, suggesting a busy urban environment. The lighting is bright, creating strong highlights on the heads and shoulders of the people.

What can we do?

Make the internet safer

ANDREW GREENBERG SECURITY 07.31.16 8:45 AM

MEET MOXIE MARLINSPIKE, THE ANARCHIST BRINGING ENCRYPTION TO ALL OF US



fastly

Hold governments accountable



Emmanuel Macron, candidate in the French presidential election. Christian Hartmann REUTERS

MACRON

Macron Campaign Was Target of Cyber Attacks by Spy-Linked Group



AZERBAIJAN INTERNET AND SOCIAL MEDIA

Azerbaijan: Activists targeted by 'government-sponsored' cyber attack



Contribute to domestic discussion

TECHNOLOGY

Security Experts Oppose Government Access to Encrypted Communication

By NICOLE PERLROTH JULY 7, 2015



Peter G. Neumann, a computer security pioneer, says "there are more vulnerabilities than ever" that could be exploited through access to encrypted communications. Jim Wilson/The New York Times



Security researcher Dan Kaminsky answers reporters' questions following his keynote address at Black Hat 2016. Photo by Seth Rosenblatt/The Parallax

Hackers call for federal funding, regulation of software security

SETH ROSENBLATT × AUGUST 9, 2016

Contribute to international processes

ST. MAARTEN: The Wassenaar Arrangement must be renegotiated or the weapons control regulations will "break the Internet's ability to protect itself," a security expert has claimed.

The [Wassenaar Arrangement](#) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is an agreement between 41 countries which generally hold similar views on human rights.

Encompassing countries such as the United States, United Kingdom, Japan, and Russia, the Wassenaar Arrangement is not a legally binding construct, but rather one that encourages and expects similar export controls on weaponry, including banning certain products outright and requiring licenses for others.

The agreement's original intentions are ones you could consider "noble," according to Katie Moussouris, CEO of [Luta Security](#).

Q&A

Questions?

Maarten Van Horenbeeck
maarten@fastly.com