Crime, Social Control & Legitimacy

A Constructivist Approach of Cybersecurity/Cyberdefense Concepts: Lessons of Security Studies Theories and Discursive Analysis

Daniel Ventre

Univerza v Mariboru
Fakulteta za varnostne vede

1973–2013

A Constructivist Approach of Cybersecurity/Cyberdefence Concepts: Lessons of Security Studies Theories and Discursive Analysis

Daniel Ventre
CNRS – GERN

Director of the Chair in Cybersecurity & Cyberdefense (Ecoles de Saint-Cyr Coëtquidan

September 23, 2013 – Univ. Maribor

Object and purposes of the study

- The main object of my research is :
  - « War »
  - I try to analyse the mutual impacts between « new wars » and the evolution of the international system

Object and purposes of the study

- More especially my research is about what we call »cyber-war« or »cyber-conflicts«
  - Is there a new category of war (cyber-war)?
  - Is »cyber« introducing new national security issues?
- My domain of research is International Relations

Object and purposes of the study

The usual approach to analyse »cyber« (cyber-security, cyber-defense, cyber-war, cyber-attacks, cyber-threats…) is based on **realist theories of IR**:

The analysis is **focused on the role of states and the anarchy of the system**.

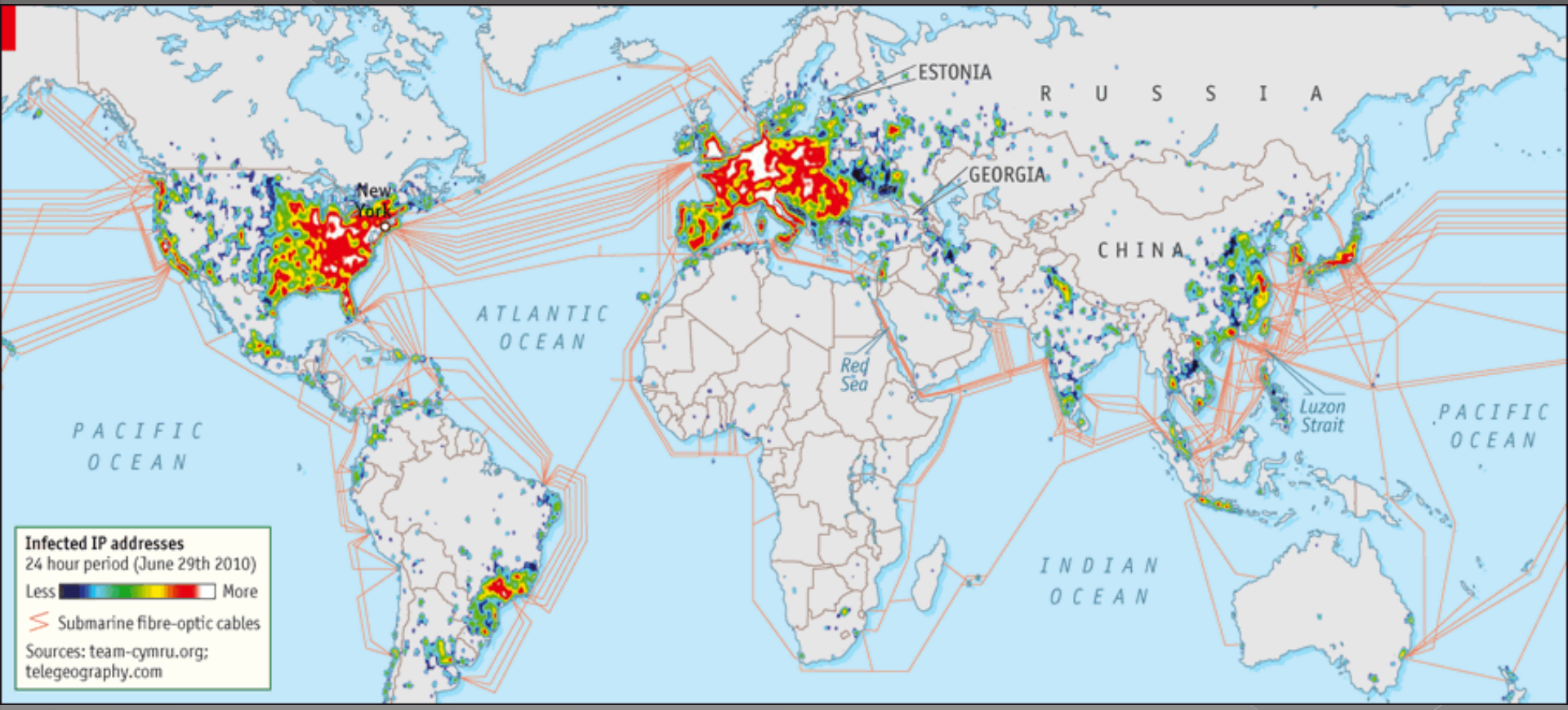
→ The main ideas of such approach are:

Object and purposes of the study

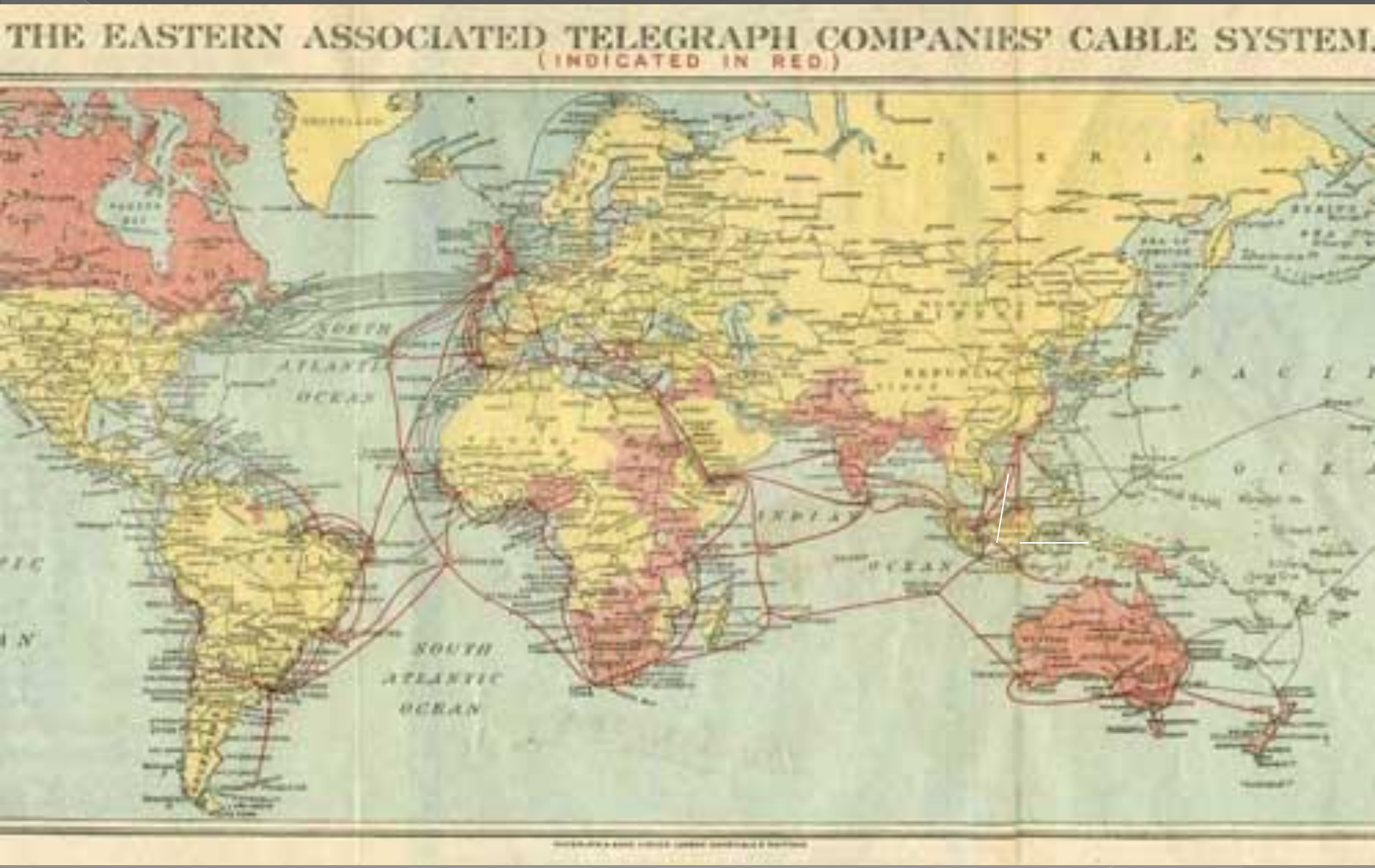
1 - States remain the main actors of cyberspace:

- States may have the control of infrastructures; contents, users …
- States may control the use of their »national« internet
- Several countries set up cyber-armies, cyber-militias, cyber-defence agencies, cyber-commands… There is a process of institutionalisation of cyber-security and cyber-defence
- The main struggles in the Internet are those between nation-states (USA, China, Russia, …)

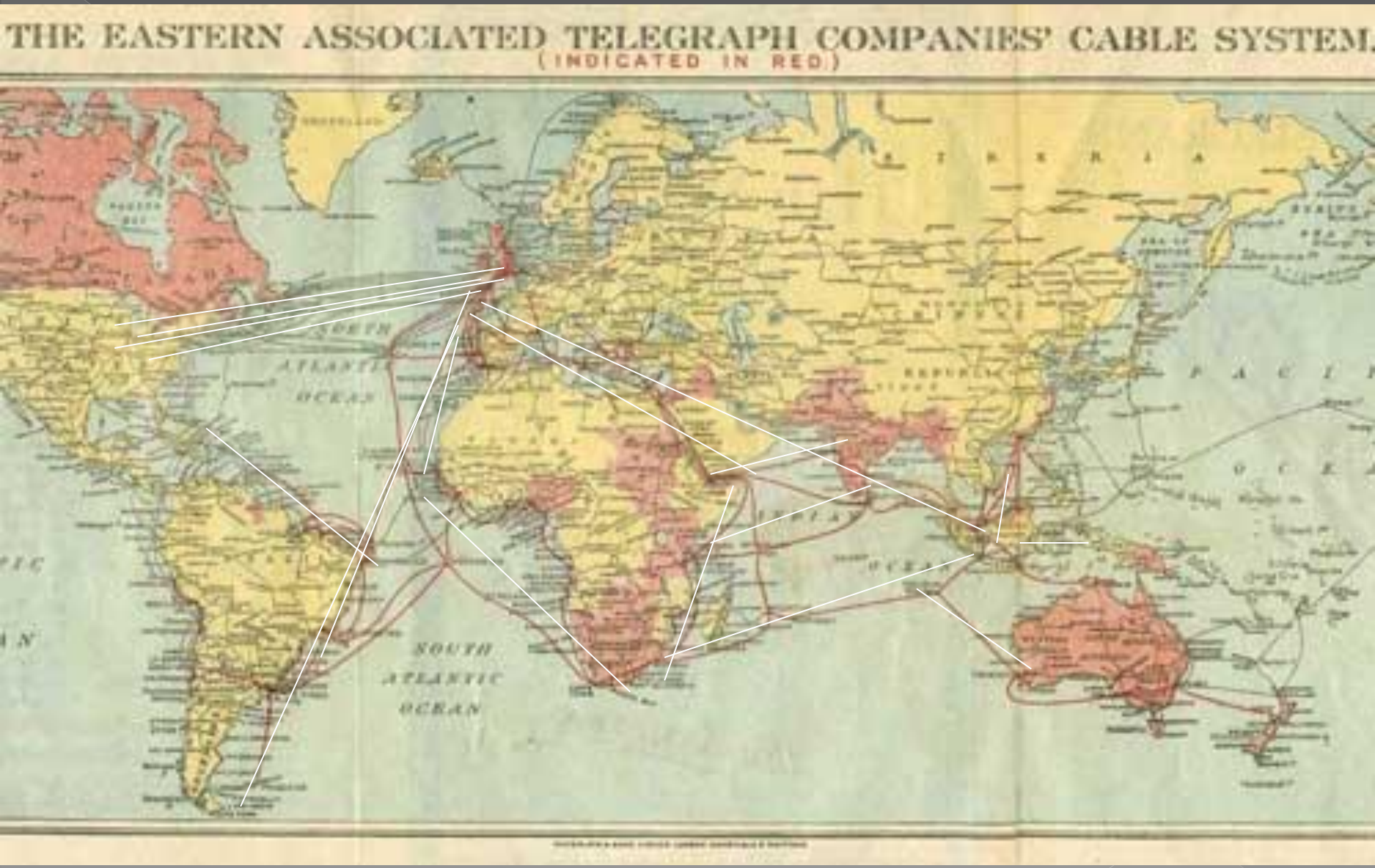
Cyberspace, cybersecurity, cyberdefense… are matters of industrialized countries



Very few things have changed since the origins of telecommunication networks un the 19th century…



Map of the world's telegraph cables prior to the rise of wireless and World War I



Map of the world's telegraph cables prior to the rise of wireless and World War I

Object and purposes of the study

2 - Cyberspace by its nature makes the international system even more anarchic. This anarchy is based on the power of **anonymity** that:

- Makes attribution of attacks impossible
- Encourages criminals but also States to use cyberspace for offensive/agressive actions.

Object and purposes of the study

Just remind some famous operations that confirm such approach:

- PRISM Program (*USA versus the rest of the world*)
- The 231 cyber-operations set up by NSA and CIA against foreign countries in 2011
- The Olympic Games operation (*Stuxnet attack from USA/Israël against Iran*)
- Use of cyberspace during the Russia-Georgia war in 2008
- Cyberattacks against Estonia in 2007

Object and purposes of the study

Anarchy because :

- There is no international law of « cyber » armed conflicts
- The law on cybercrime is not universal and remains mainly applied at national level

  → *The European Convention on Cybercrime is far from being a success of international cooperation!*

Object and purposes of the study

- There is no international cooperation in terms of cybersecurity and cyberdefense
- Lack of confidence;
- Our allies probably launch cyberattacks against our systems;
- National security and defense strategies remain secrets, confidential;
- Opacity of the strategies;
- Security dilemma;
- etc.

Object and purposes of the study

The question of this study was:

→ What may be the **contribution of constructivist theories** to the understanding of « cyber » security/defence issues?

Object and purposes of the study

To answer this question I used the concepts of »**securitization**« (Ole Waever)
and »**macrosecuritization**« (B. Buzan)

What is SECURITIZATION ?

A process that will **justify, legitimate new policies** :

→ An **actor** (elite) who talks
→ A **speech** act …
→ That **moves a topic** into an area of national security
→ Identifying a **threat** against…
→ A **referent objec**t (object to be protected)
→ An **audience** (who accepts/validates the securitization)
→ **Actions** that need to be taken

What is SECURITIZATION ?

→ Securitisation will have **consequences**:

- New national security strategies
- New laws
- New military doctrines
- Institutionalisation (*creation of security and defence agencies…)*
- Impacts on citizens, privacy, freedoms…
- …

What is SECURITIZATION ?

→ **Why**, **How** and **When** does a specific question become a national security issue?

→ *For instance: immigration → becomes a national security problem*

→ Is this securitization placed at political, societal, military, economic or environmental level?

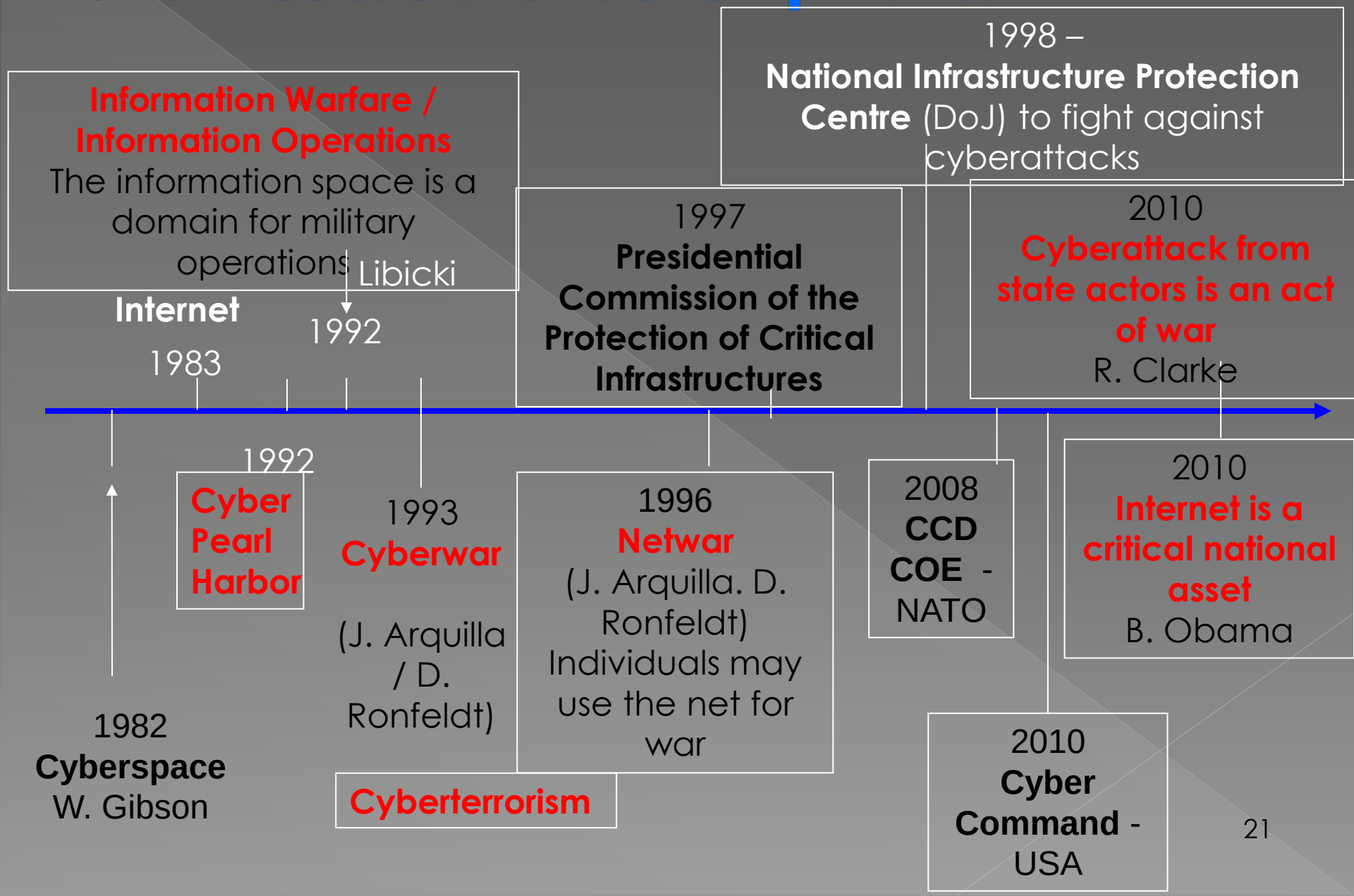
When did cybersecurity become a national security issue?

- Computers and national security are linked since WWII
- The first computers were created during WWII for military purposes, to win war
- Since the 1950's, national agencies such as NSA and CIA funded computer science research
- During the Cold War, computer industries were targeted by espionage
- The protection of computers and computer industries from foreign espionnage have been the basis of cybersecurity as a national security issue

When did cybersecurity become a national security issue?

- The »cyberthreat« debate is an old one too…
- It can be traced back to the Reagan administration (during the 1980's)
- But it was not yet a national security issue

Cybersecurity is securitized by speech and institutional developments



When did cybersecurity become a national security issue?

→ In the 1990's (post Cold War era; uncertainty…)
→ Mainly in the USA
→ In a context of terrorist threat

→ Around 2010, the main arguments and objects of cybersecurity are: cyberthreat against vital infrastructures, threat of State attacks, War, National Defense.

→ It is a military problem + a political, societal and economic issue.

What is Macrosecuritization?

- The **referent object** is staged in universalist terms:
  - *Human civilisation*
  - *Environment*
- Or the process is based on a **widespread sharing of the same threat**:
  - *Terrorism*
  - *Disease*
  - …
- *Examples: macrosecuritisation of the Cold War, GWoT, etc.*

Is there macrosecuritization of »cyber«?

Yes…

→ *Because cyberthreats are considered as **global**: a great number of States have the power to launch cyber operations*

→ ***Enemies** are everywhere*

→ *The attacks against the United States are not only attacks against a sovereign State, but also **against the values** of modern world (democracy, liberalism…)*

→*The world seems to be organized in **2 groups**:*

- → *The USA/allies* versus *China/Russia/Iran…*
- →*These countries do not share the same democratic values*

Is there macrosecuritisation?

No…

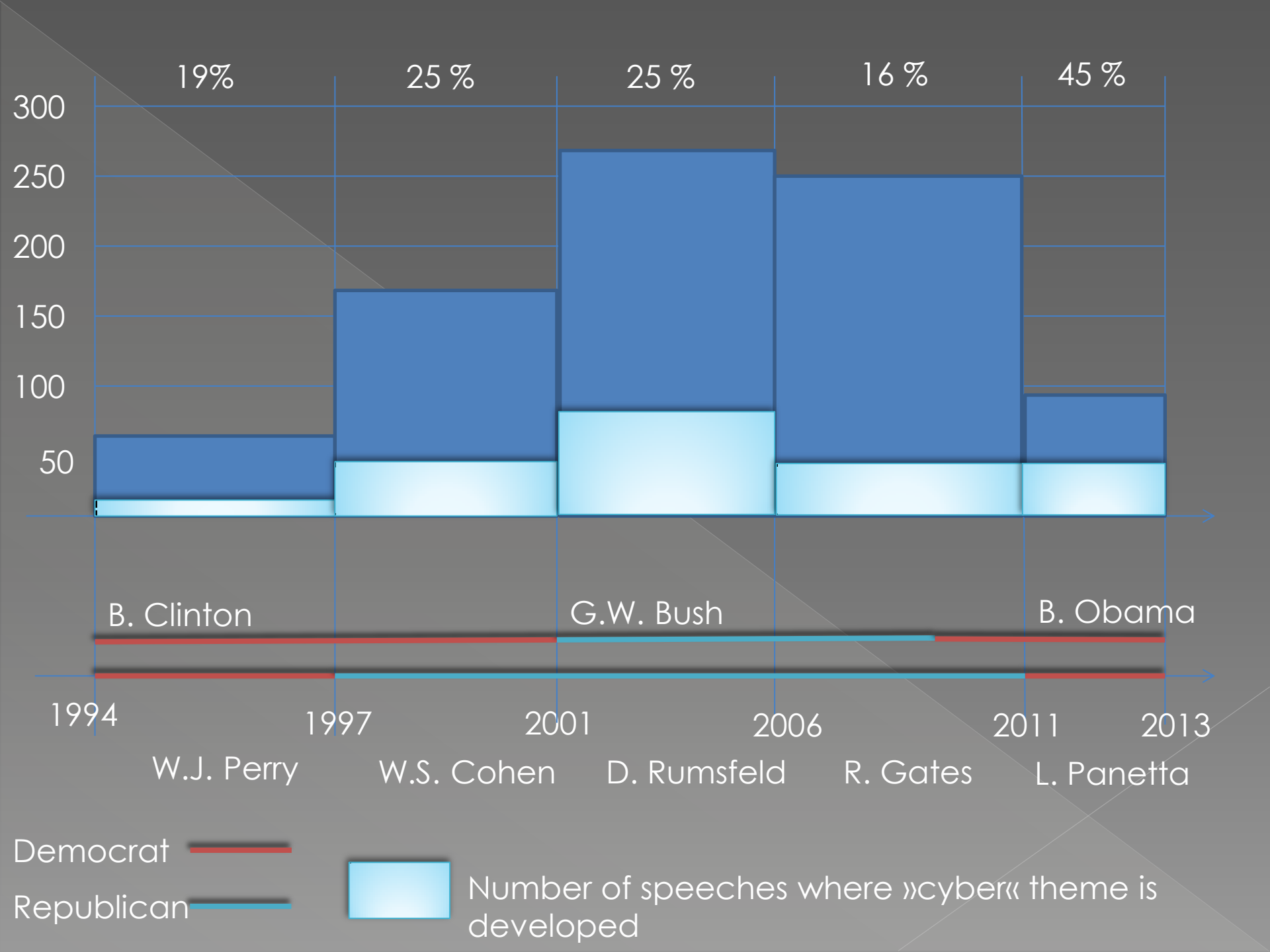
→ because nation-states may have their own perceptions of cyberthreat and their own solutions , depending on :

- *Their level of technological development,*
- *Their capability to propose independent solutions of security adapted to their own (national) cyberspace (self help)*
- *The USA discourse on cybersecurity is oriented towards its own interests (we need to protect and defend our own cyberspace against…)*
- *Even in cyberspace, the notion of « regional conflicts » is applicable. It means that a cybersecurity problem may be considered as a regional problem rather than a global problem.*

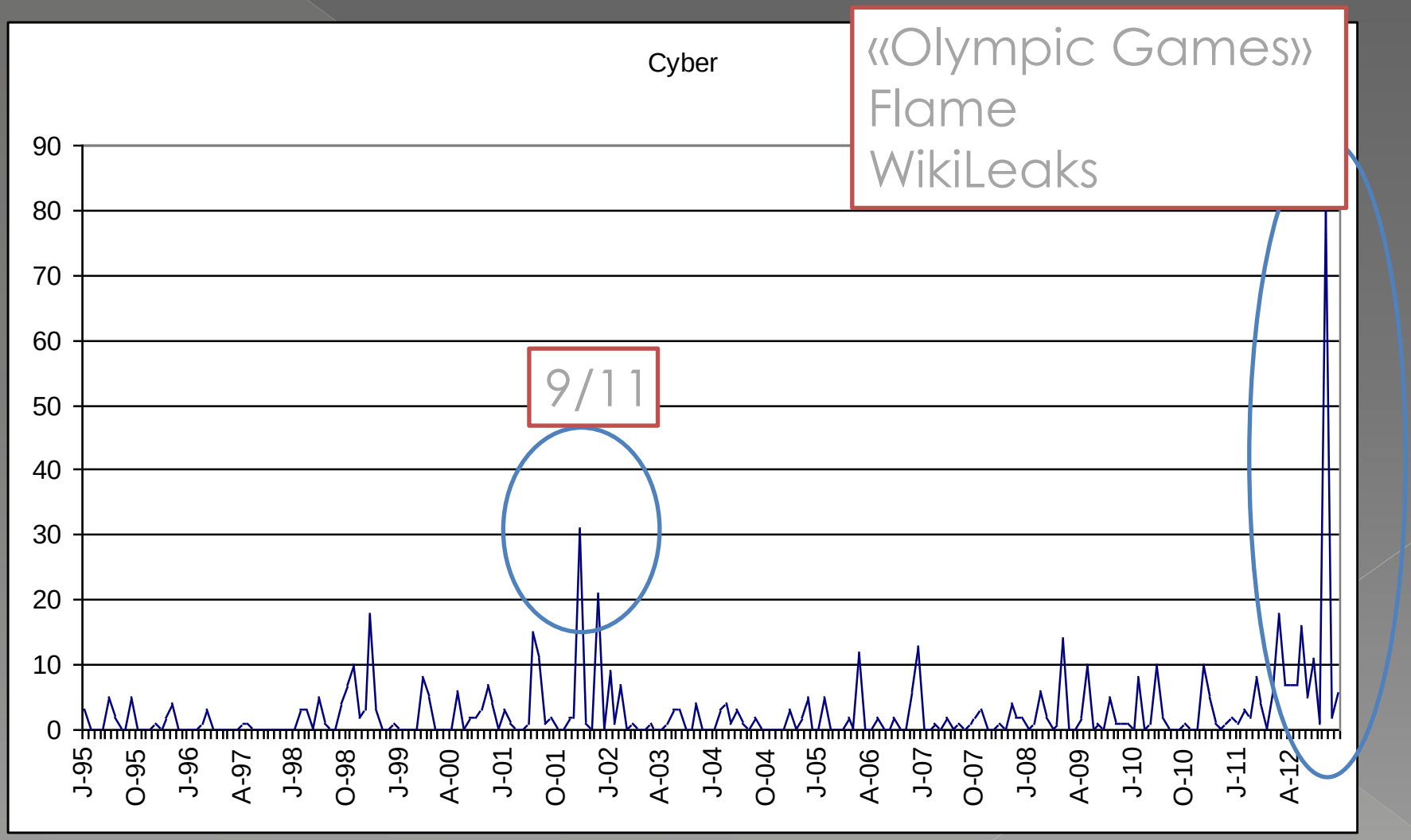
What kind of information do we read in the evolution of Secretaries of Defense' Speeches?

Corpus of data: speeches of Secretaries of Defense – DoD - United States

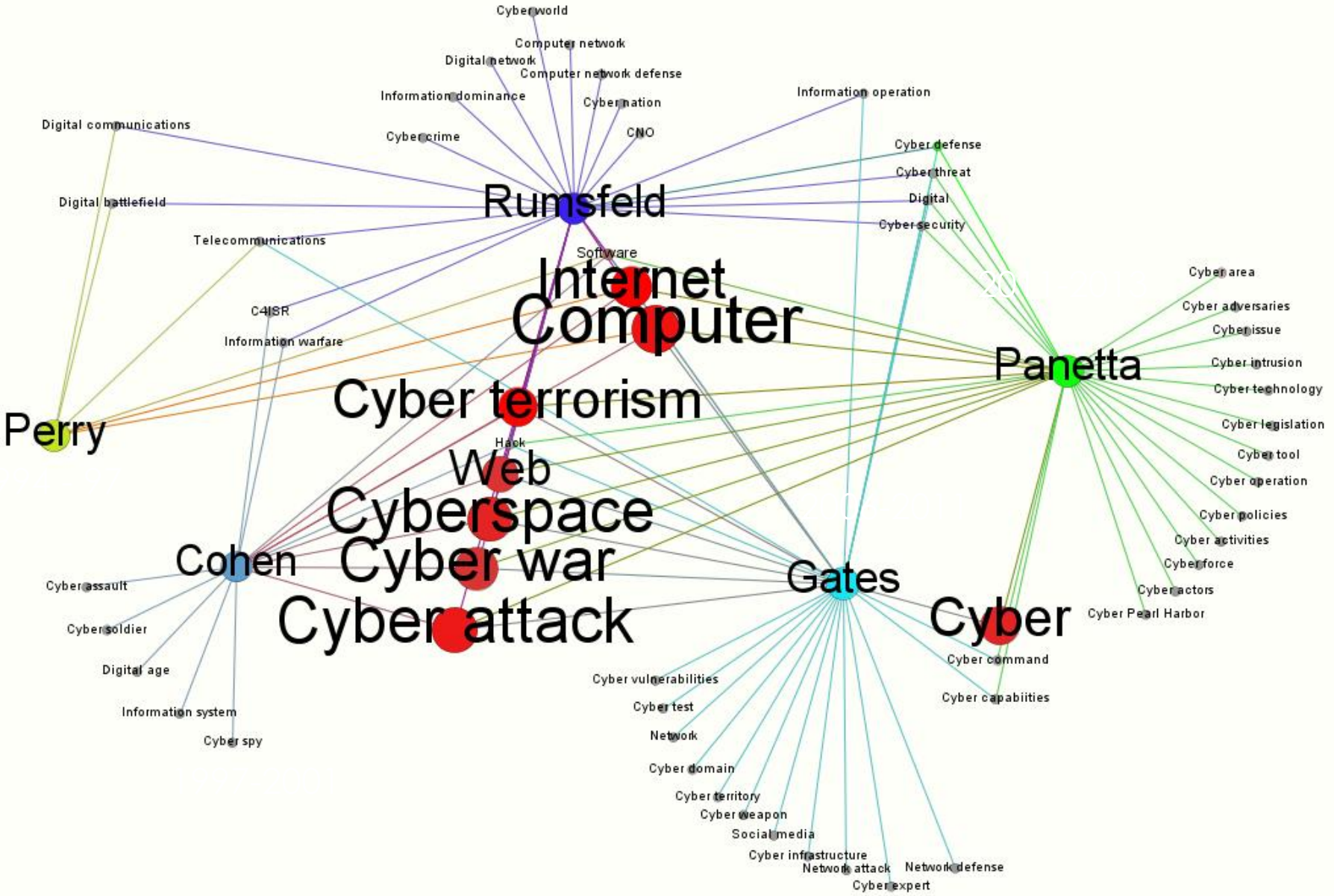
- Period: 1994 – end of 2012
- Number of speeches available: 841
- Total number of speeches involving cybersecurity issues: 203 (ie.24%)


19%
25 %
25 %
16 %
45 %
300
250
200
150
100
50
B. Clinton
G.W. Bush
B. Obama
1994
1997
2001
2006
2011
2013
W.J. Perry
W.S. Cohen
D. Rumsfeld
R. Gates
L. Panetta
Democrat
Republican
Number of speeches where »cyber« theme is developed

Number of words linked to »cyber« in Sec. DoD Speech.

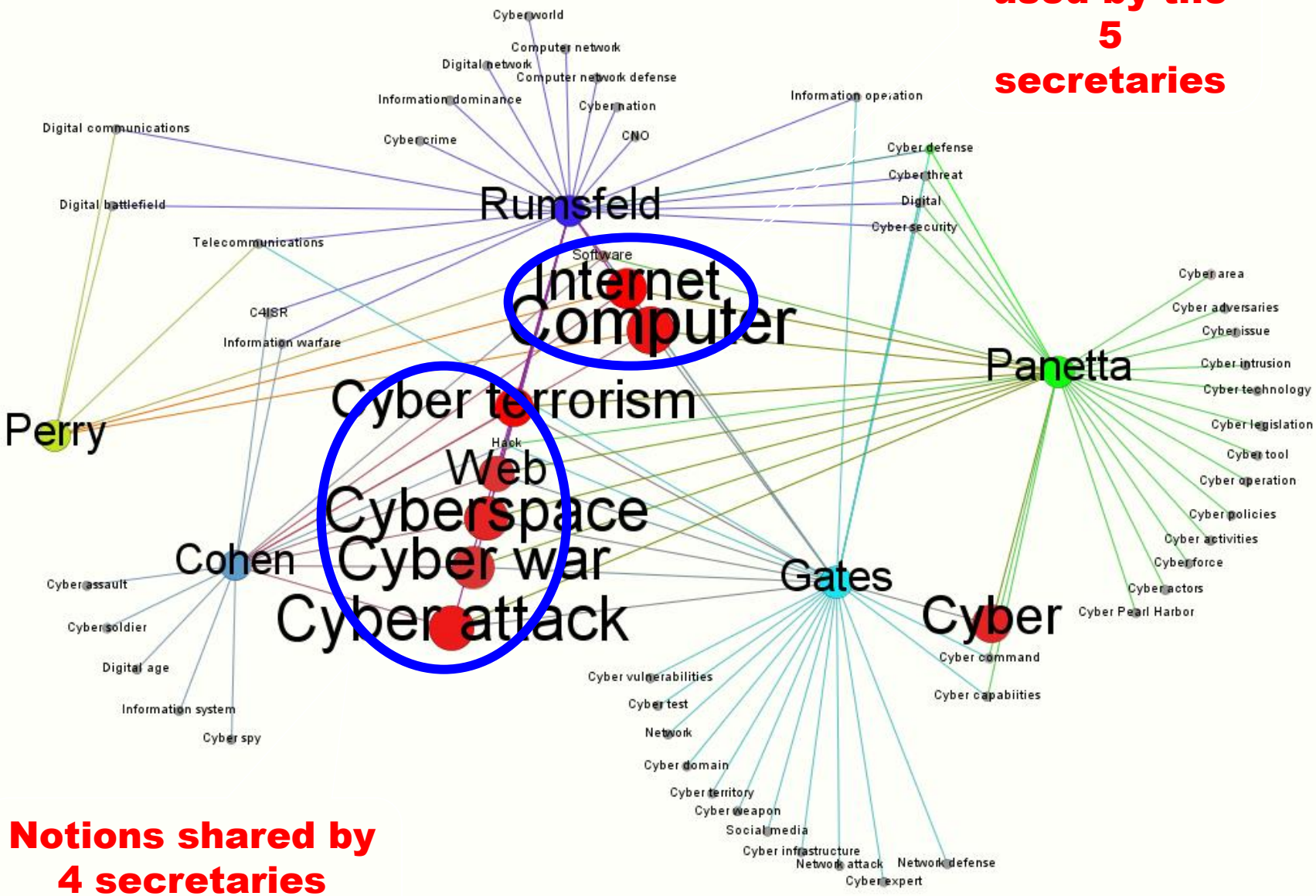


2001-2006

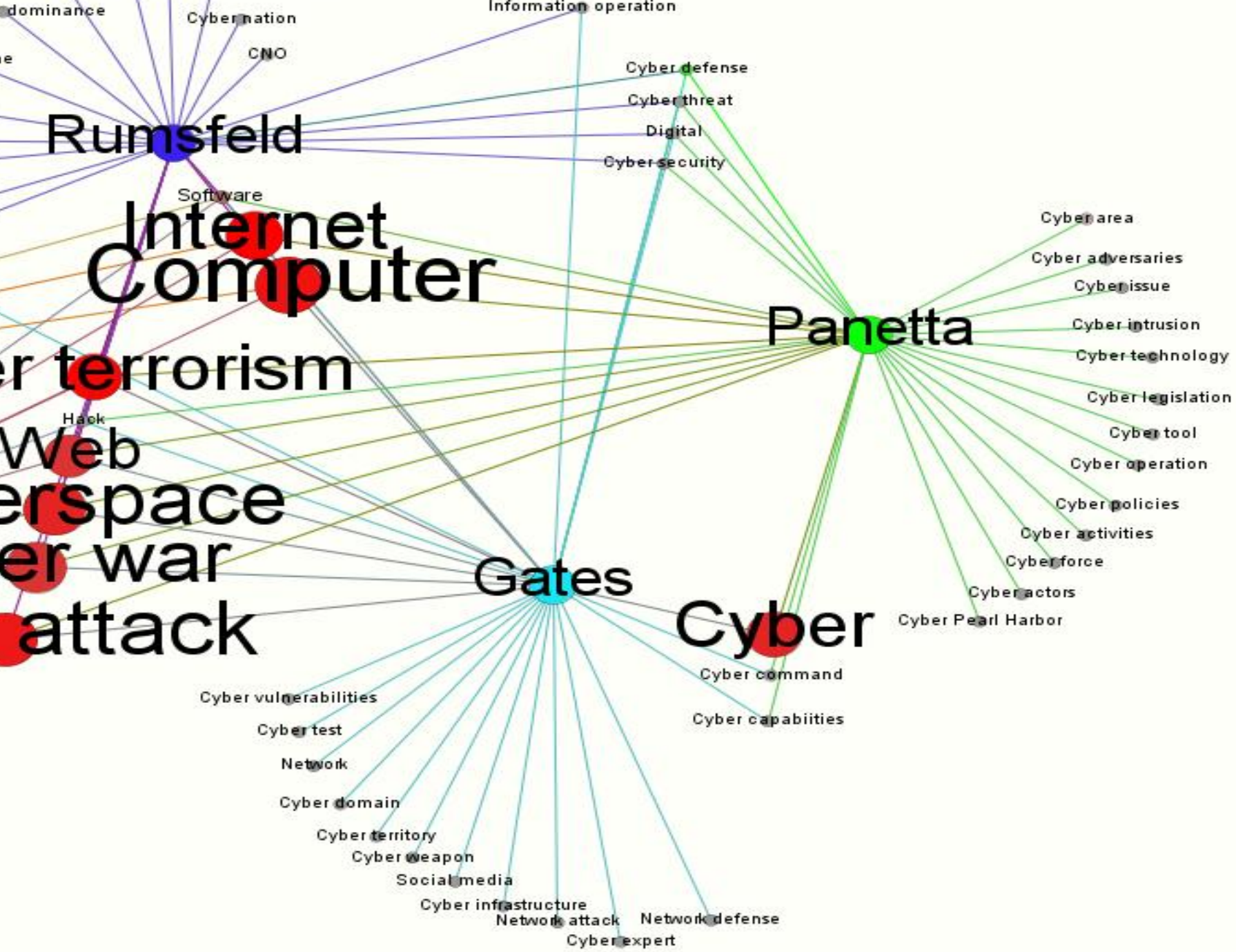

Cyber world
Computer network
Digital network
Computer network defense
Information dominance
Cyber nation
Information operation
Digital communications
Cyber crime
CNO
Cyber defense
Cyber threat
Digital battlefield
Rumsfeld
Digital
Cyber security
Telecommunications
Software
Internet
Computer
Cyber area
C4ISR
Cyber adversaries
Information warfare
Cyber issue
Panetta
Cyber intrusion
Cyber terrorism
Cyber technology
Perry
Cyber legislation
Hack
Cyber tool
Web
Cyber operation
Cyberspace
Cyber policies
Cyber activities
Cohen
Cyber war
Cyber force
Gates
Cyber assault
Cyber actors
Cyber
Cyber Pearl Harbor
Cyber attack
Cyber soldier
Cyber command
Digital age
Cyber vulnerabilities
Cyber capabilities
Information system
Cyber test
Cyber spy
Network
Cyber domain
Cyber territory
Cyber weapon
Social media
Cyber infrastructure
Network attack
Network defense
Cyber expert

A lot of words have very short life

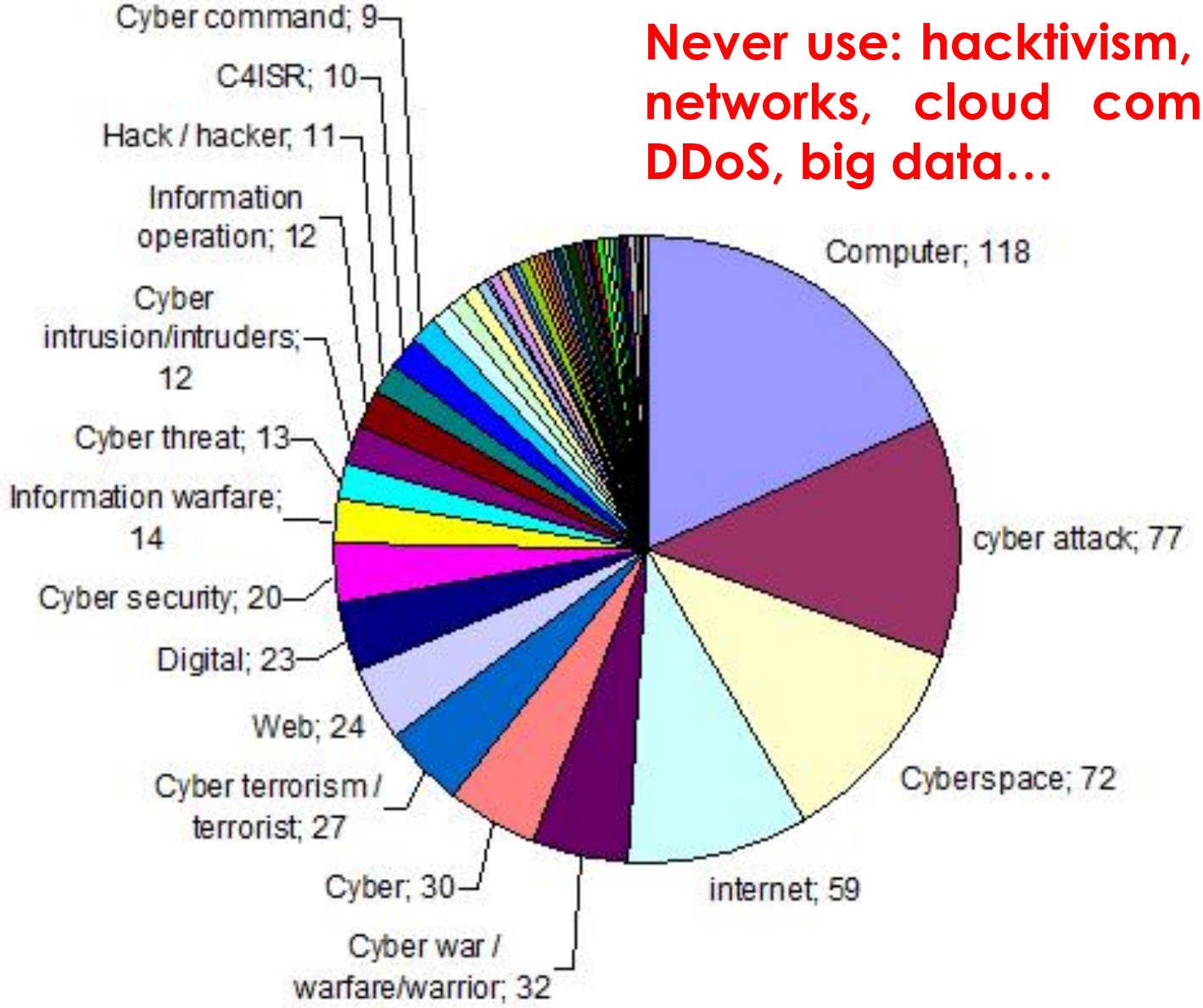
Notions used by the 5 secretaries



Notions shared by 4 secretaries


dominance
Cyber nation
CNO
Information operation
Cyber defense
Cyber threat
Digital
Cyber security
Rumsfeld
Software
Internet
Computer
r terrorism
Hack
Web
erspace
er war
attack
Panetta
Cyber area
Cyber adversaries
Cyber issue
Cyber intrusion
Cyber technology
Cyber legislation
Cyber tool
Cyber operation
Cyber policies
Cyber activities
Cyber force
Cyber actors
Cyber Pearl Harbor
Gates
Cyber
Cyber command
Cyber capabilities
Cyber vulnerabilities
Cyber test
Network
Cyber domain
Cyber territory
Cyber weapon
Social media
Cyber infrastructure
Network attack
Network defense
Cyber expert

Never use: hacktivism, social networks, cloud computing, DDoS, big data…



Key ideas and arguments

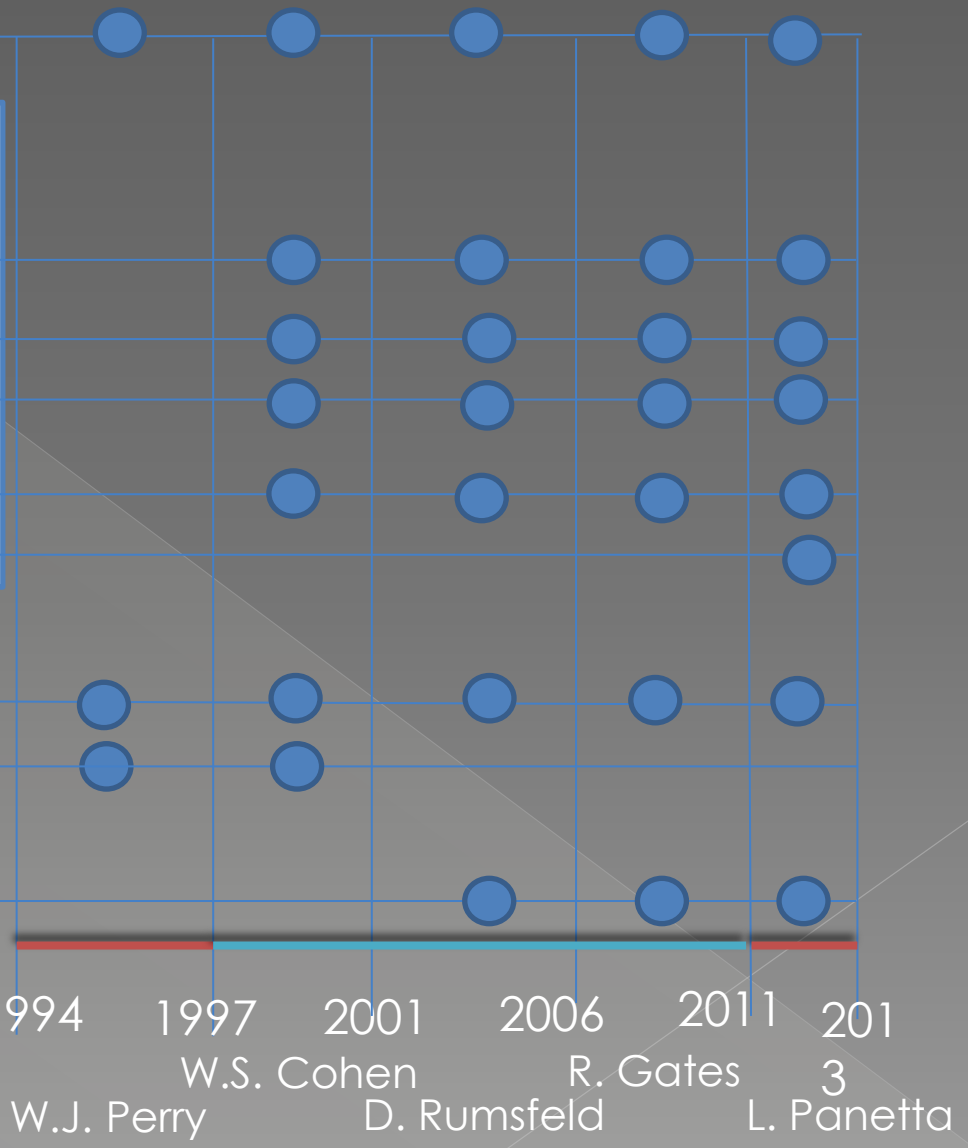
Technology is a tool for military power , information dominance…
Technology is the condition for victory against all kinds of enemies

Alarmist/catastrophist:

- Technology (cyber) is a source of new threats (cyberattacks against military, society, industry, peace ...)
- Cyberwar is a threat
- Cyberterrorism is a threat
- Risks from dependance (of society) on cyberspace
- Cyber Peal Harbord

»Solutions« requested:

- Increase investments in cyberdefense
- Private industry as a provider
- Cybersecurity is not limited to DoD. It is a national and international security issue



Conclusion

1 - I think that the process of making **cybersecurity a national security challenge is very conventional**, because:

- *The **referent objects are State** (its sovereignty) **and the Nation** (its identity, its values)*

Conclusion

2 - This securitization of »cyber«:

- Is mainly placed at State level ;
- Threats come from States; Sates are the victims
- National security and defence policies are legitimated by the international system itself
- The audience of States is the international community (ie. other States)
- Of course, cybersecurity issues sometimes become national problems → then governments need to justify their policies and gain confidence from their own citizens
- But most of the time, governments (military, security agencies) do not seek their national public confidence