# BIG DATA AND CYBERSECURITY:

## *Multi Stakeholder Threats and Opportunities*

*A US Speakers Program*
*Embassy of the United States, Serbia*
*September 20-25, 2015*

**Anne C. Bader**
**Founder**
**The International Cybersecurity Dialogue**

# Internet technology links all earth’s activities

Its power is unquestioned

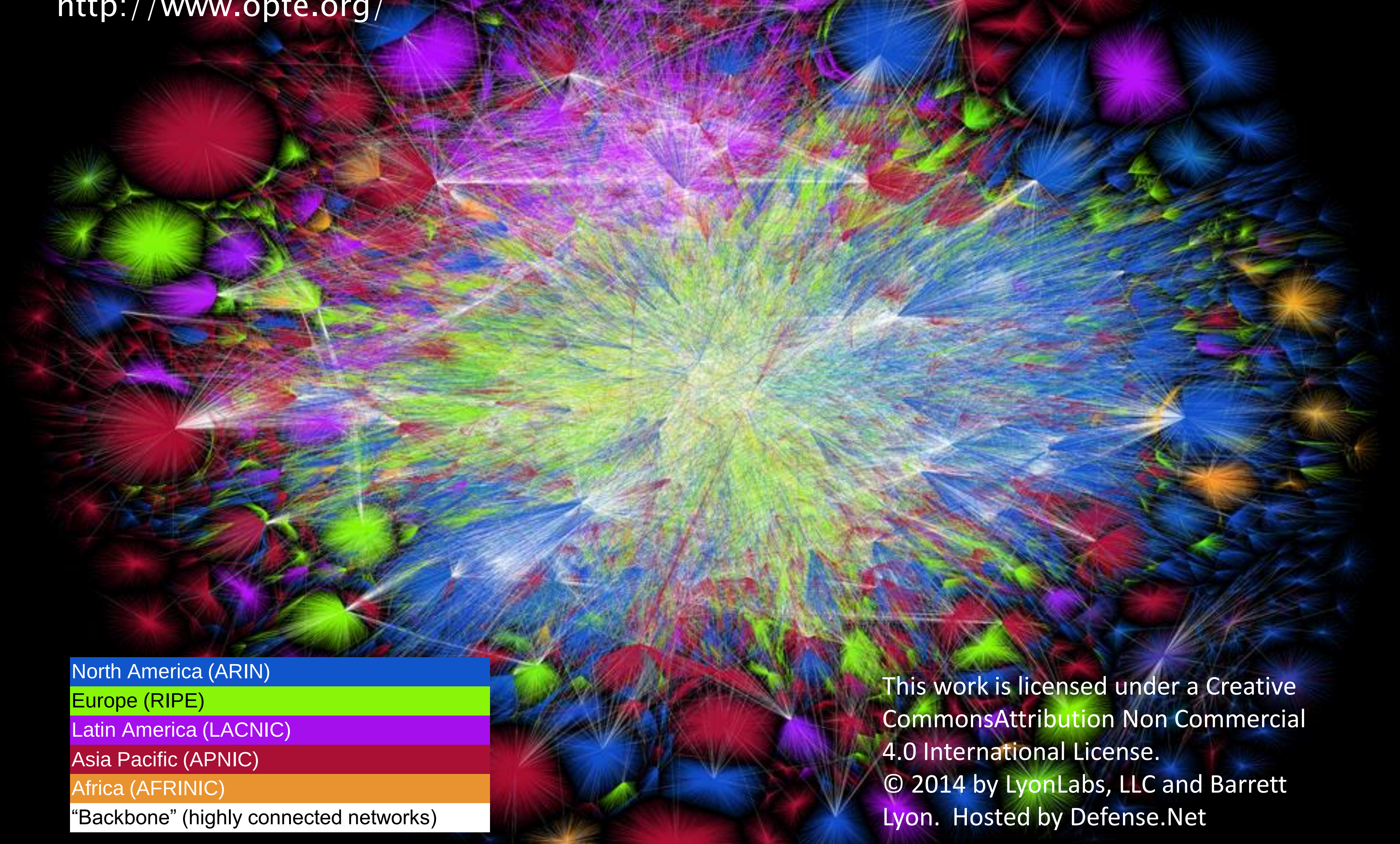
Its capacity is not fully understood

Its essential infrastructure supports security, telecommunication, commerce, energy, finance, transport.

**It is** the **newest 21st century weapon.**

# THE OPTE PROJECT 2015 An Internet Map by Barrett Lyon

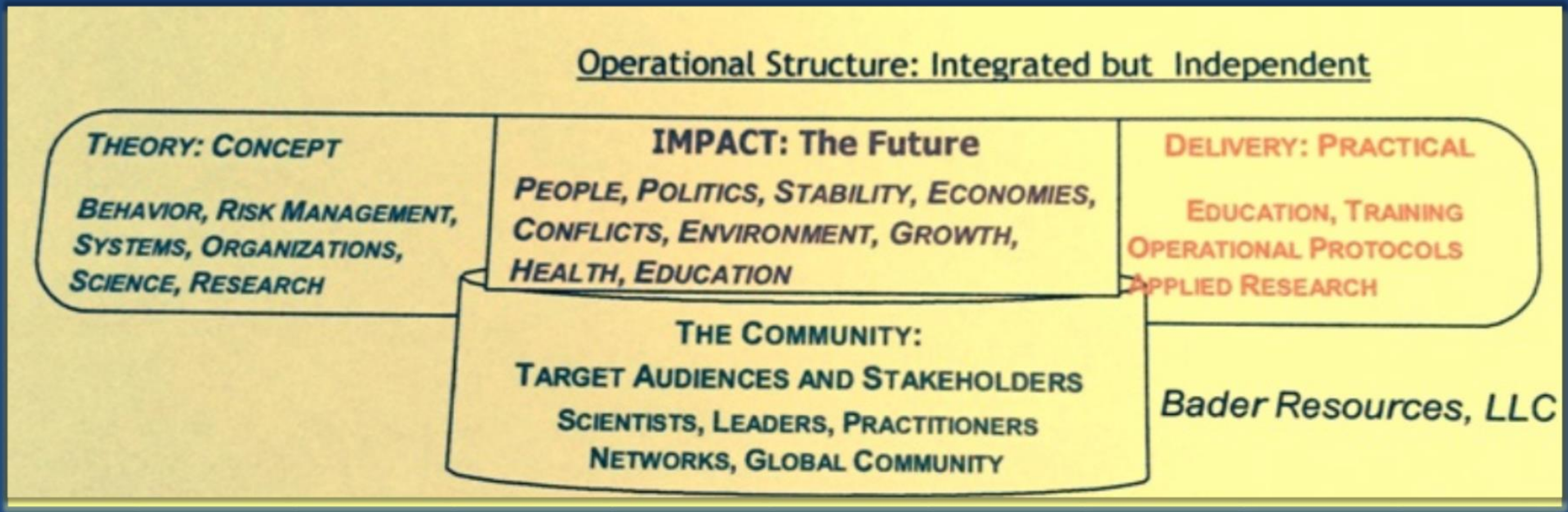
"The visualization is a collection of programs that collectively output an image of every relationship of every network on the Internet. This award winning representation of the Internet now hangs in the Museum of Modern Art in NYC. "
http://www.opte.org/



| | |
|---|---|
| 🟦 | North America (ARIN) |
| 🟩 | Europe (RIPE) |
| 🟪 | Latin America (LACNIC) |
| 🟥 | Asia Pacific (APNIC) |
| 🟧 | Africa (AFRINIC) |
| ⬜ | "Backbone" (highly connected networks) |

This work is licensed under a Creative CommonsAttribution Non Commercial 4.0 International License.
© 2014 by LyonLabs, LLC and Barrett Lyon. Hosted by Defense.Net

# Multi Stakeholder Approach:
# No One Organization Controls the Internet
# Integrated but Independent



Operational Structure: Integrated but Independent

Theory: Concept

Behavior, Risk Management, Systems, Organizations, Science, Research

IMPACT: The Future

People, Politics, Stability, Economies, Conflicts, Environment, Growth, Health, Education

Delivery: Practical

Education, Training
Operational Protocols
Applied Research

The Community:

Target Audiences and Stakeholders
Scientists, Leaders, Practitioners
Networks, Global Community

Bader Resources, LLC

# BIG DATA

“High Volume,
High Velocity and/or
High Variety information assets
that require new forms of processing to enable enhanced decision-making, insight discovery and process optimization.” Gartner Glossary

# CYBERSECURITY IS

# A MANAGEMENT ISSUE

# BIG DATA OPPORTUNITIES

- Information!
- Innovation!
- Return on Investment (ROI)
- Control
- Competition
- Cooperation
- Collaboration
- Scientific and commercial intelligent systems
- Systems management and advanced processing.
- Open source research.

# BIG DATA THREATS BECOME OPPORTUNITIES

Richard Stiennon

Liability- “40 million records of US government employees stored in an Oracle data base becomes a big file system. Adversaries can draw a big picture of intel groups and mix with other files on travel, email to target specific individuals and groups.”

Assets-It is a huge asset for security. The amount of information, alerts, security events become our Big Data repository. We derive intelligence from who is attacking.

“Tells me when a packet from Russia comes though and gives us the ability to extract information through Security Analytics.”

“By combining information with an email address of a target and user name and password in another breach a hacker can send an email from some that site that the target knows and gain access to his systems.”

# CYBERSECURITY THOUGHTS

Here is an example of how Data Science software uses consumer buying trends.

- **A woman went to her pharmacy. Shortly afterwards, she began receiving offers for baby products, diapers etc. Based on her buying activity the software was tracking her as pregnant. She was pregnant at the time but did not know until several weeks later when she saw her doctor!**

- **Privacy: Ownership: Who owns Data?** **Do you own your birthday? It is one of your unique identifiers. In the United States it is ambiguous: individuals can protect their health information from other individuals or organizations but in some states the government can sell our health information to third party vendors for commercial use!** In Estonia, each individual owns his own identity. Their security is designed to support that across all sectors and locations.

- **Can someone else use your birthday to drive information about you? How about your DNA?** Who can use that information about you? Do hospitals have the right to share your DNA tests with third parties such as insurance companies without your permission or knowledge? "Doctors, insurance companies, pharmacies, blood test labs, hospitals and middlemen we know nothing about sell our most intimate medical records.

# What Policy Changes to Secure and to Protect Big Data?

Agree on the principles of information sharing between the Public and Private Sector.

- The proposed EU General Data Protection Regulation is a single set of rules for everyone. The EU Commission on a Digital Single Market seeks to eliminate the roaming charges for using phones, internet. How is this compatible?

Governments need to build in Encryption and Information Rights Management into their systems.

- The bigger the data the better the target. Our most recent example is the breach of the Office of Personnel Management.

Government must have the ability to audit and control access in the best way.

- Most Big Data is run on insecure or inadequately secure systems both in the private and the public sector.

Develop legislation and conventions that benefit and protect, the public, private and academic sectors and each individual.

- White House Report on Privacy and Cybersecurity; EU-US Umbrella Agreement; EU General Protection Regulation.

Require universal accountability on compliance with the most up to date security protection.

- Internet of Things delivers personalized information to each user and gathers newly developed personal information without protecting it. Smart phones, Smart Watches, Fitbits, are some examples.

# What are the most common security issues/concerns related to Big Data?

- Liability– What are your assets that you need to protect?
- Oversharing of Data–generational divide
- Personal Identifiable Information –PII
- Lack of control of your Data
- Digital Footprint–lack of control how much is given away
- How to secure all data

# What are the most common security issues/concerns related to Big Data?

- Rationalize your Data Policies

1. Understand the assets you need to protect
2. Educate and evaluate enterprise risk.
3. Consolidate security policy; secure all the data
4. Harmonize uncoordinated and inconsistent policies
5. Who are the stake-holders?
6. What is the business need?
7. What are the data processing needs?
8. Update older equipment and software
9. Training, Incident response teams, regular practices

# How is Big Data used to address cybersecurity and security threats?

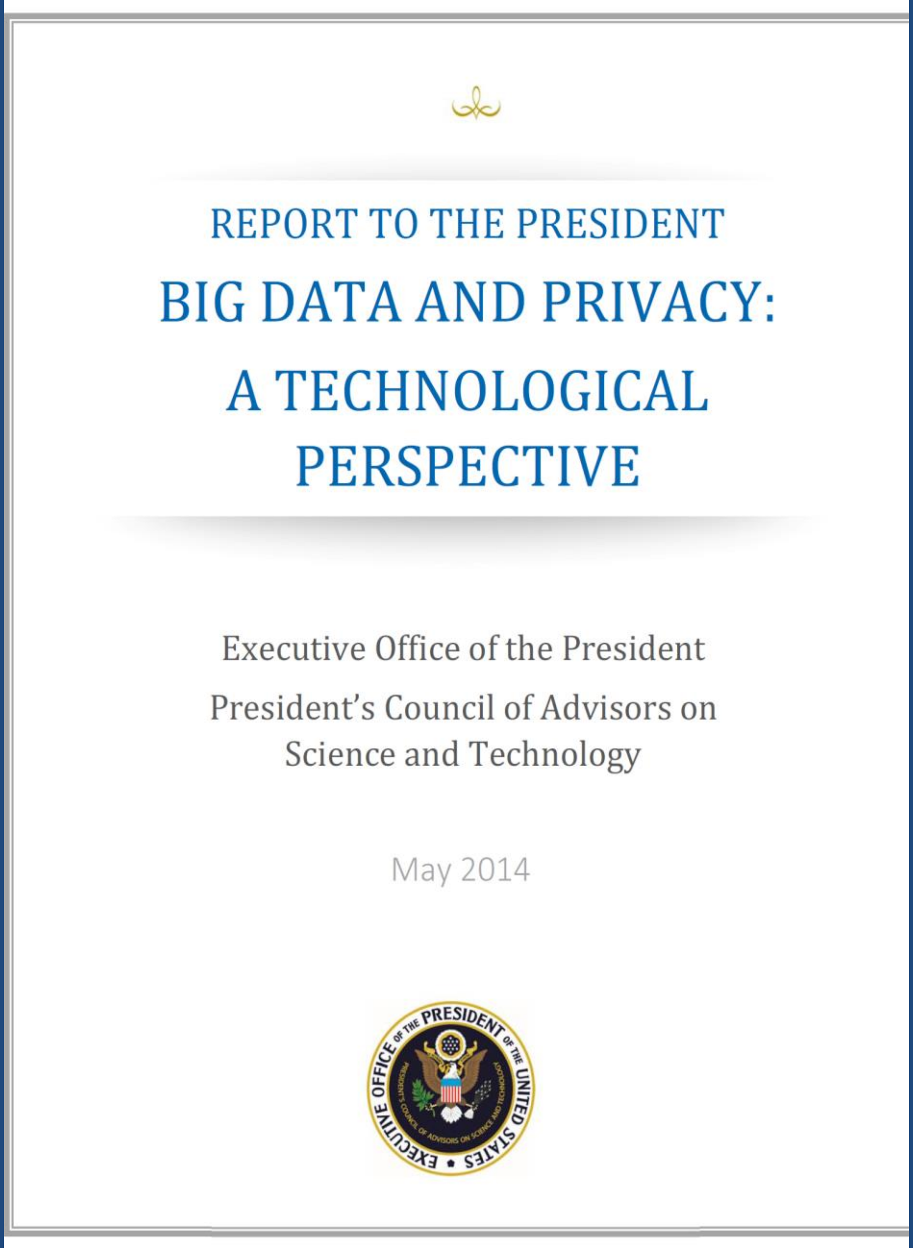
## BIG DATA ≠BIG ANALYTICS≠ BIG SECURITY

- What do I need? Build a system to collect the threat information
- Increase the time on Incident Response and practicing (What happens if our data is taken, system collapses etc.)
- Data Analytics. Huge cost of not using appropriate analysis. Primarily a Return on Investment ( ROI)Issue both in government and business.
- Biggest shared concerns are Branding and Costs
- Data analytics companies: I Sight Partners, Digital Shadows, SQRRL
- Management, Keeping every system up to date
- Training,  Red Team exercises, Incident Response team regular practices

# How is Big Data used to address cybersecurity and security threats?

- First and foremost, it’s a Management Issue
- Safety in Design
- Build a system to collect the threat information
- Concepts and processes important to support risk-informed decision making
  - Threat environment
  - Threat actors
  - Where am I vulnerable?
  - Operating Systems–Up to Date
  - How do you access the data?
  - What am I trying to protect is the most important
  - What are the consequences of Data Loss?

WE ARE MAKING PROGRESS!



REPORT TO THE PRESIDENT

# BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

Executive Office of the President

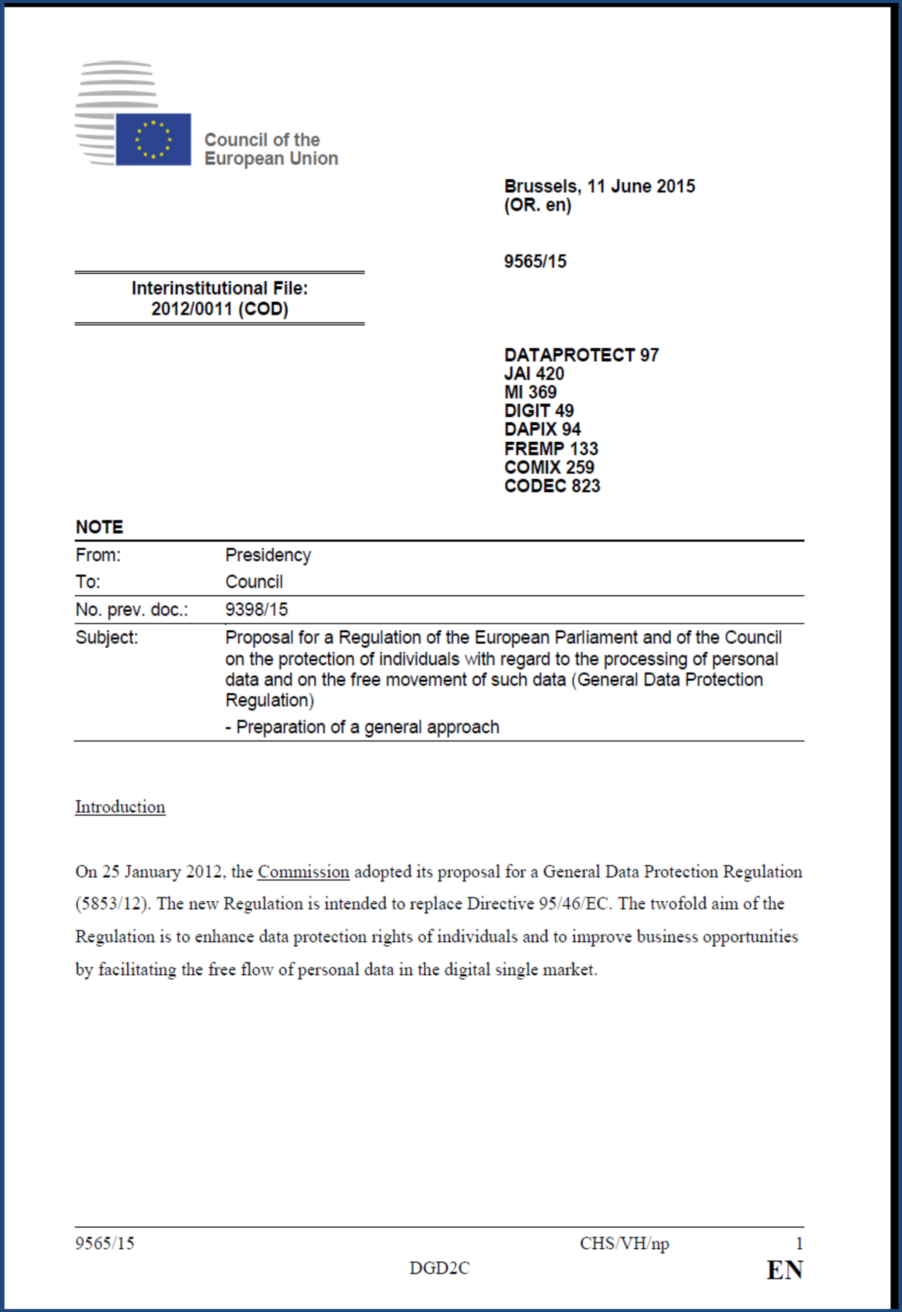
President's Council of Advisors on
Science and Technology

May 2014

# Five White House Recommendations Big Data on Privacy Initiative

- Uses
- Government Policy and Regulations
- Outcomes
- Education
- Take the international lead to convene, cooperate and collaborate

Prepared by the Science and Technology Council, Executive
Office of the President and the US Department of Energy
National Initiative for Technology and Development



Council of the European Union

Brussels, 11 June 2015
(OR. en)

9565/15

Interinstitutional File:
2012/0011 (COD)

DATAPROTECT 97
JAI 420
MI 369
DIGIT 49
DAPIX 94
FREMP 133
COMIX 259
CODEC 823

**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Council |
| No. prev. doc.: | 9398/15 |
| Subject: | Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)<br>- Preparation of a general approach |

Introduction

On 25 January 2012, the Commission adopted its proposal for a General Data Protection Regulation (5853/12). The new Regulation is intended to replace Directive 95/46/EC. The twofold aim of the Regulation is to enhance data protection rights of individuals and to improve business opportunities by facilitating the free flow of personal data in the digital single market.

# Finalisation of the EU-US negotiations on the data protection "Umbrella Agreement"

08-09-2015

Réunion des hauts fonctionnaires de l'UE et des États-Unis chargés de la ...ice et des affaires intérieures
Luxembourg
© 2015 SIP

"

Today, on finalising the negotiations on the EU-US data protection "Umbrella Agreement", Věra Jourová, EU Commissioner for Justice and Consumers made the following statement:

"I am very pleased that today we have finalised negotiations with the US on high data protection standards for transatlantic law enforcement cooperation.

Robust cooperation between the EU and the US to fight crime and terrorism is crucial to keep Europeans safe. But all exchanges of personal data, such as criminal records, names or addresses, need to be governed by strong data protection rules. This is what the Umbrella Agreement will ensure."

# North Atlantic Treaty Organization

- “As cyber threats do not recognise state borders, nor organisational boundaries, cooperation with partners on cyber defence is an important element of the revised NATO policy..

- NATO also recognises the importance of harnessing the expertise of the private sector and academia in this complex area where new ideas and new partnerships will be key.”

http://www.nato.int/cps/en/SID-312C4364-5F166FAE/natolive/topics_78170.htm

# REPETITION FOR EMPHASIS

CYBERSECURITY IS

A MANAGEMENT ISSUE

# SPECIAL THANKS

- This report was the result of more than 25 interviews with US and International leaders in technology, government, intelligence, military, academe, international organizations, hackers, non governmental organizations and think tanks and journalists most of whom agreed on the main points I stress. I am happy to expand after the talk.

# International Cybersecurity Dialogue

*Bridging the Gap Between Security Technologist and Policy Makers*

phone photo Anne C. Bader

"We believe that national policies and laws governing the new cyber domain must be made with the public and private sector technologists who create and manage the networks and systems."

Anne C Bader and Richard Stiennon

ACBader@cybersecuritydialogue.org
www.cybersecuritydialogue.org