Nomos & Khaos

The 2011-2012 Nomisma report on economic-strategic horizons

Observatory on Strategic and Security Scenarios

Nomos & Khaos
Copyright © 2012 Nomisma Spa
published by A.G.R.A. srl
via Nomentana 257
00161 Roma
tel +39 0644254205
fax +39 0644254239
e-mail info@agraeditrice.com
www.agraeditrice.com

Printed
in September 2012

Translation by: Legal English sas

Composition by: Agra srl
Graphics by: Blu omelette
Printed by: CSR – Roma

Nomisma Società di Studi Economici SpA
Strada Maggiore 44, Palazzo Davia Bargellini
40125 Bologna
tel +39 0516483111, fax +39 051232209
www.nomisma.it

All rights are reserved for Nomisma SpA.
No part of this book may be reproduced
or utilised in any way whatsoever without
written authorisation from Nomisma Spa,
whether using mechanical or electronic means,
including photocopying, recording or
reproduction by any data processing system
whatsoever.

Board of Directors
Pietro Modiano (Chairman)
Luciano Sita (Vice Chairman)
Piera Magnatti (Director)

Members of the Board
Antonio Calabrò
Bruno Calzia
Maurizio Carfagna
Carlo Cimbri
Luciano Colombini
Emanuele Degennaro
Luca Lucaroni
Enzo Mignarri
Rodolfo Ortolani
Giovanni Pecci
Juan Enrique Perez Calot
Samuele Sorato
Giordano Villa
Francesco Cozza (Secretary)

Scientific Committee
Gian Maria Gros-Pietro (Chairman)

Nomisma Scientific Committee
Felice Adinolfi
Giovanni Ajassa
Paolo Bruni
Roberto Camagni
Giuseppe Cucchi
Rita Finzi
Marco Fortis
Elisa Luciano
Giulio Napolitano
Giorgio Prodi
Filippo Taddei
Gianfranco Viesti
Piera Magnatti (Segretario)

**Director of Observatory for Strategic
and Security Scenarios (Osss)**
Giuseppe Cucchi

Osss Research Group
Felice Adinolfi, Gian Paolo Calchi Novati,
Lucio Caracciolo, Emanuele Castelli,
Paolo De Castro, Jorgelina di Pasquale,
Federico Eichberg, David Gosset, Domenico
Lombardi, Fyodor Lukyanov, Roberto Menotti,
Paolo Migliavacca, Pietro Modiano, Riccardo Monti,
Roberto Nigido, Carlo Pelanda, Alessandro Politi,
Riccardo Redaelli, Daniele Riggio, Francesco Sisci,
Davide Tabarelli, Francesco Vitali.

Scientific Coordination of the Report
Germano Dottori

Editing and Cartographic Support
Vanessa Albertini, Olana Bojic, Eulàlia Rifé i Soler

Index

Introduction

Part One

Overview of the year's events

Part Tow

Towards a new economic/financial equilibrium

Part Three

Towards a new political/strategic equilibrium

Part four

Conclusions

Part Five

Annex

2.8 The economic geopolitics of data and the future of dominance

From control to forecasting
Power, social media and manipulation of social action

Francesco Vitali

The profound changes which have occurred over the last two years have come as a complete surprise to most analysts: seemingly unpredictable developments, marked by the chaotic juxtaposition of socio-economic events fraught with difficulty for analysts. A year later, it appears clear that the course of events during this epoch-making period was generated not only by a natural coincidence of catalysts. In 2010 and 2011, starting with the Wikileaks publications and culminating in the uprisings in North Africa and the Middle East, falling under the definition of the so-called Arab Spring, we have been able to observe the initial effects of a new type of geopolitical conflict fought out with instruments which hitherto were unimaginable.

In coming years, pre-eminence will be fought for not only in the media, new media and social media, as may have appeared to be the case from a cursory interpretation of recent international events. Certainly the role played by these information models in the building of societies will not decline, but their scope for action will be closely tied to and, will probably be the result of a different form of power which runs deeper and is more subtle: “data control”.

One cannot fully appreciate the phenomenon without studying in greater detail the type and quantity of information garnered, as well as the new, existing data processing models. The balance of power between states and between multinationals aiming to promote or hinder the new world order is already being redefined around the ability to use data. This is the new key geopolitical and economic power factor. Soon, we will be able to classify nations into three categories: those able to exercise control through external assistance, those equipped with autonomous control tools and those capable of progressing from control to forecasting and manipulation of individual and social behaviour.

FROM DATABASES TO THE EXTRAPOLATION OF COMPLEX KNOWLEDGE

Wishing to summarise several decades of research and technological innovation in data classification and management sciences, we can identify three main lines of development.

Initially, research focused chiefly on the corporate area, on the ability to store and manage structured sets of information. In such case, the quality of the database was determined largely by the programmer's ability to correctly envisage a system for classifying information before it was entered, making it possible to later retrieve and process the information when needed.

In the 90s, we gained greater awareness of the value of tacit or implicit knowledge[1], in other words all those technical, relational and professional skills which though unwritten, constitute the main asset of complex organisations with a widely distributed knowledge-base. This approach ushered in new tools for interacting and collaborative work: "cooperative learning", and the first examples of "Wikis". When successfully implemented, these procedures make it possible for "non-accessible" knowledge to rapidly come to light and to be formalised, but only if users, for example, researchers and network workers, decide to cooperate.

We have now come to a third stage where, through the pervasive use of technology, we can combine the previous approaches whilst overcoming their limitations. Neural networks and complex algorithms for statistical and semantic analysis make it possible to reorganise unstructured sets of data, achieving levels of efficiency which are similar to those obtained with perfectly organised databases. It thus also becomes possible to extract information from undefined flows of data such as those that can be obtained from traces of "packet" transmissions on Internet, from possible combinations of email and web surfing, graphics, audio, video or from financial transactions. Above all, it becomes possible to extract implicit knowledge from and on people without it being necessary to obtain their explicit consent. It is no longer necessary for users to interact within a predefined platform, asking them to clearly express concepts, practical skills and relational information. Given that by using the current tools any form of communication, research, reading and social interaction may be sent digitally, one need merely monitor the online activity of the individual in question. Contrary to expectations, in order to monitor somebody, it is hardly ever necessary

[1] I. Nonaka, H. Takeuchi, The Knowledge Creating Company, University Press, Oxford, 1995.

to conduct Echelon[2]-style electronic espionage. Most information in fact is made accessible, almost always unbeknownst to the data subjects, by users or sent automatically by machines.

In order to understand the impact of these tools for monitoring and analysing knowledge and to realise just how pervasive they are, we must first analyse the state of the network, its nodes and its connections.

THE NEW INTERNET

On 6 June 2012, the main global companies operating on Internet started to migrate their systems based on the IPV4 (Internet Protocol version 4) protocol to the new IPV6 (Internet Protocol version 6) protocol, interrupting the allocation of old addresses. The IP is the beating heart of Internet as it makes it possible to allocate a unique address (irrespective of whether or not it is static or dynamic) to any Internet connected device, making it possible to identify the device and connect it with others, thereby allowing for the constant exchange of data.

The global launch of this new protocol has gone almost unnoticed because, in reality, the two systems will continue to coexist for many years to come and most users will not even notice the changeover, except when they encounter a browsing problem caused by the use of technologies which have not yet been upgraded. 6 June 2012 however marked the Internet's coming of age and was a sign of just how all-pervasive it has become. IPV4 was based on 32-bit codes, and so was "only" able to handle 4.3 billion numerical addresses, too few for today's needs. Instead, the new protocol, based on 128 bit codes, will not only be able to handle an almost unimaginable number of alphanumeric addresses (2^{128} around 340 billion billion billion billion), but will make it possible to manage mobile devices connected directly to Internet in a more efficient manner.

Experimentation of the new protocol has been going on for over one decade but no one could have foreseen that the network would have saturated the available addresses so quickly, in other words, the number of connected devices and published websites. In order to gain a clearer understanding of the state of In-

[2] Global system for the interception of private and commercial communications, designed by the United States with the cooperation of Canada, United Kingdom, Australia and New Zealand. The existence of Echelon was revealed to the public in 1997 following the first report presented to the European Parliament by the STOA (Scientific and Technical Options Assessment programme office). See, for example, the European Parliamentary "Report on the Existence of a Global System for the Interception of Private and Commercial Communications" (ECHELON Interception System) (FINAL A5-0264/2001 PAR1).

ternet one need merely analyse the latest forecasts by Cisco (a leading global provider of networking solutions): global Ip traffic[3] is forecast to quadruple over the 2011–2016 five-year period, from 369 exabytes[4] of data transmitted to 1.3 zettabytes (110 exabytes per month), as shown in table 2.8.1. The number of Internet users throughout the world is set to increase to 3.4 billion, covering 45% of the world population estimated in 2016 by the United Nations[5]. Network connections will surge from 10.3 billion to 18.9 billion: around 2.5 connections for each inhabitant on earth.

Table 2.8.1. Global Ip Traffic - Exabytes per Year as of Year End 2016

	CONSUMER	BUSINESS	TOTAL
Internet	881.5	85.2	966.7
Managed IP	175.1	42.5	217.6
Mobile data	99.8	29.9	129.7
Total	1,156.4	157.6	1,314

Consumer: Includes fixed Ip traffic generated by households, university populations, and Internet cafés.
Business: Includes fixed Ip Wan or Internet traffic generated by businesses and governments.
Mobile: Includes mobile data and Internet traffic generated by handsets, notebook cards, and mobile broadband gateways.
Internet: Denotes all Ip traffic that crosses an Internet backbone.
Managed Ip: Includes corporate Ip Wan traffic and Ip transport of TV and VoD
Source: "*Cisco Visual Networking Index (Vni) Forecast (2011-2016)*", Cisco White Paper, May 30, 2012.

There are also set to be significant changes with regard to the international development of Internet, with major shifts in traffic and access figures. The highest rate of growth[6] will be recorded in the Middle East and in Africa (traffic is set to increase tenfold in five years) and in Latin America (traffic will increase sevenfold in five years). In 2016 the Asia-Pacific region will account for most Ip traffic (40.5 exabytes per month), outstripping North America (27.5 exabytes per month). In 2016 the two leading countries in terms of the quantity of traffic produced, will be the United States (22 exabytes per month) and China (12 exabytes per month). It will however be India which records the highest rate of Ip traffic growth, with an annual average of 62%, followed by Brazil and South Africa.

Over the next four years, there will be a significant change in the way in which Internet is accessed, so much so that the greatest growth rate will not be in global fixed Ip data traffic, but in wireless networks[7]. While in 2011, 55% of traffic was

[3] Cisco, Visual Networking Index (Vni) Forecast (2011-2016), Cisco White Paper, 30/5/2012.

[4] One exabyte corresponds to 10^{18} byte. Using a byte as the unit of measurement, we have the following: kilobyte kB 10^{3}, megabyte MB 10^{6}, gigabyte GB 10^{9}, terabyte TB $10^{12,}$ petabyte PB $10^{15,}$ exabyte EB 10^{18}, zettabyte ZB 10^{21}, yottabyte YB 10^{24}.

[5] The Un estimates that the world population in 2016 will amount to 7.4 billion.

[6] Cisco, White Paper, 30/5/2012, *op.cit*.

[7] Cisco, *Visual Networking Index: Global Mobile, Data Traffic Forecast Update, 2011-2016*, White Paper, 14/2/2012.

generated by wired devices, in 2016 this will drop to 39%, making way for Wi-Fi and mobile devices. Global mobile data traffic will increase 18-fold the volume recorded in 2011, reaching a monthly volume of approximately 10.8 exabytes (10,804,321 terabytes).

This dramatic growth will be in part due to the increase in the number of wireless devices connected, which will exceed the number of people on Earth. In fact, the number of mobile Internet users will soar from 3.7 billion in 2011 to 4.5 billion in 2016. Over 10 billion mobile Internet devices connected: over 8 billion mobile devices will be connected and approximately 2 billion M2M[8] module connections.

There will be interesting developments in networked smart objects in machine–machine mode, starting with GPS systems for cars, resource tracking systems for the shipping and manufacturing sectors, industrial devices, biomedical devices to monitor the health of patients or to report, for example, whether pharmaceutical products in a pack have been taken at the right time.

These objects will enable new forms of communication which will also be useful for managing "intelligent digital billboards", capable of modifying advertising messages according to the time of day or the person in front of the billboard. Without migration to the new network protocol, this evolution would have been unthinkable, so much so that the number of fixed and mobile IPV6 devices throughout the world will rocket from 1 billion in 2011 to 8 billion in 2016.

Despite the many technological tools which are constantly connected, it will be smartphones, laptops and other portable devices which are set to generate approximately 90% of global mobile data traffic by 2016.

BIG DATA

The data presented so far only refers to the transmission of information over Internet or private networks. In reality, the world of digital data is much broader than can currently be measured during transit from one node to another one within a network. There is an enormous quantity of information that is generated every day within companies, public authorities and agencies, and other types of organisation, and such information is not automatically transmitted over IP.

[8] Machine-to-machine.

The McKinsey Global Institute[9] has estimated that every American company with over 1,000 employees holds data assets averaging approximately 200 terabyte, twice the size of the entire data warehouse belonging to the American retail giant, Walmart, in 1999. We have entered the era of Big Data[10], in other words, collections of data measured in petabytes, exabytes, zettabytes, vast amounts of information which can no longer be stored and analysed in standard databases using traditional tools.

The hyper-proliferation of data and greater transmission capacity have also contributed to the growth of new remote storage and processing technologies: cloud computing. With cloud computing it is possible to transfer the storage and processing of data from users' computers to providers' systems, or one can use complex services without necessarily needing advanced computers and other hardware systems or personnel capable of programming and managing the system.

With a common smartphone, used as a simple terminal, it becomes possible to handle complex analysis of large collections of data such as data used by telephone companies. It is precisely this simplicity, efficiency and the fact that outsourcing these new technological solutions is now so affordable which is encouraging both business markets and public authorities and agencies[11] as well as individuals, to transfer their data to the few global companies which are able to attain sufficient critical mass. In this way, companies are transferring client databases, financial services, CRM (customer relationship management), cash flow monitoring data and inventory management to these large multinationals. Ordinary citizens, almost always unbeknownst to them, are transferring a clone of their lives.

ENABLING TECHNOLOGIES

In order for data to be analysed, it must be collected by sensors spread over the territory. For years the American Defence Advanced Research Projects Agency has been working to develop cyber insects and other forms of sensors to disseminate across enemy territory in order to spy on electronic data transmissions

[9] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, A. Hung Byers, "Big data: The next frontier for innovation, competition, and productivity", *McKinsey Global Institute,* Report May 2011.

[10] Also according to IBM estimates, every day approximately one Exabyte of data is generated every day in the world. See "What is Big Data?", http://www-01.ibm.com/software/data/bigdata/ (24/6/2012).

[11] In Western countries, the Public Sector is undergoing profound change, related not only to the huge volume of data being processed, but also to all that information which in the name of transparency is now being made available on Internet for citizens to freely consult: the so-called Open Data doctrine.

and troop movements. If this type of technology can prove to be useful in areas of wilderness and territory which is largely inaccessible, such as the mountainous areas in Afghanistan or areas which are off-limits for military reasons, it proves to be totally superfluous in gathering data in developed countries where there are "intelligent networks". One example of this is the electricity smart grid which makes it possible to manage distributed forms of electricity production and distribution, but also to garner real-time information about the consumption habits of a specific user and thus to establish whether people are at home or in the office, if a domestic appliance is turned on (perhaps even determining which appliance). The electricity grid, inter alia, is capable of carrying so much information that it has been used in many projects for the transmission of Internet data[12] as an alternative to the telephone line).

There are also video surveillance systems in many cities, including public and private video cameras. Citizens are likely to be filmed every 200 or 300 metres with systems which now have facial recognition and movement analysis capabilities or which have all manner of inbuilt microphones or sensors. There are records generated by electronic payment instruments such as credit cards and debit cards, PayPal and suchlike, Google and Facebook "electronic money" and new payment systems through NFC (Near Field Communication) via cellphone technologies: they record who acquired a product or service, from where and sometimes also who it is for.

There are GPS technologies (Global Positioning System) in satellite navigator devices, mobile phones and other commonly used devices. Or there are RFID (Radio Frequency Identification) technologies, miniscule microchips with antennas that can be applied to all kinds of products, from clothing to waste, identity documents and loyalty cards, animals and motor vehicles. It is generally thought that RFID only works over very short distances, whereas in actual fact it is sufficient to have a suitable "illuminator[13]" to allow the chip to transmit its identifier and its data to a reader located not just a few centimetres away but tens of metres away[14], including near a border. It is thus possible to check who is sitting inside a cinema or find out who is taking part in a demonstration[15].

[12] This characteristic has also been exploited for espionage purposes. By measuring the electromagnetic variations produced on the electricity grid by typing on a computer's keyboard, for example, in certain cases, it is possible to remotely detect what has been written.

[13] Antenna which, due to its electromagnetic RF emissions, "activates" microchip communication.

[14] RFID reading distance is linked to the type of chip, the illuminator and reader used.

[15] It is sufficient to remotely read the chip contained in one of the cards carried by people, or one of those applied to their clothing, possibly tracked since the time of purchase with a credit card.

Now that the IPV6 era has formally kicked off, M2M "talking objects" will become increasingly popular. They will be capable of exchanging data autonomously. The future "Internet of things[16]" holds out the promise of much more than just a new generation of appliances. Television sets equipped with advanced set-top boxes which recognise users and their activities and home automation which has finally become reality.

The current princely objects of desire[17] amongst "enabling" objects are smartphones and tablets, as well as all the services used through Internet, ranging from simple browsing on Internet to use of social networks. Until a few years ago, mobile phones only transmitted information on phone calls and text messages sent and received as well as geographic positions, recorded by triangulating transmitting antennas. All data used after a specific event was handled only by telephone companies or on their behalf. With the latest generation of mobile phones, tablets or the new gamepads which are always connected, two phenomena been noted: the incredible pervasiveness of instruments for accessing users' data and the proliferation of entities that are able to acquire this information.

With regard to the former phenomenon, in addition to traditional telephone data, these technologies can collect, to provide a few examples, information about appointments, a complete contact list (sometimes with the image of our contact), private and work correspondence, photographs accompanied by a host of metadata[18], films watched and music listened to, data on bank accounts accessed online or payments made through technologies integrated with one's mobile phone. In addition, there are even smartphones equipped with sensors to monitor our heart rate or other physiological data, triaxial accelerometers to measure spatial movement for games or other advanced purposes. All this information is geo-located through triangulation of cellular networks or local Wi-Fi networks, or otherwise directly through the integrated GPS. These instruments make it possible to read books and newspapers and in fact have attracted large publishing investments as well as the associated advertising. The latest models of smartphone, introduced in 2012 integrate advanced tools to analyse natural

[16] See also S. Ackerman, CIA Chief: We'll Spy on You Through Your Dishwasher, *Wired.com*, 15/3/2012. http://www.wired.com/dangerroom/2012/03/petraeus-tv-remote/ (24/6/2012).

[17] Of course this brief classification only applies to "wearable objects" or objects which surround us. Massive use is increasingly being made, chiefly in Britain and the United States, of sophisticated airborne audio–video–radio monitoring instruments such as drones used for "civil purposes". In fact,, Google has long been rumoured to be working on the use of drones to generate new "maps" of the territory.

[18] The new cell phone models allow users to activate automatic face recognition functions in respect of people in photos or augmented reality, to recognise and enrich information on objects/monuments shot, as well as to record the position where images are shot.

language in different languages, allowing one to control certain features of the phone via a simple gaze, thanks to eye movement analysis tracked by a micro-camera in the front of the device.

With regard to the proliferation of players, the range of entities who can access data has increased significantly. Alongside the classic telecommunications companies which manage traditional phone traffic, there are two types of player who are much harder to monitor: the providers of the operating systems which allow the phone to work, such as Microsoft, Apple for systems based on iOs such as iPhones and iPads, or Google for those systems based on Android, and companies developing "apps", independent applications offering additional features on top of those provided by the mobile phone platform.

It can happen that a simple game, or the tiny program which alerts us to birthdays in our calendars or which allows for faster connection to a social network, for some reason, downloads photos taken with the mobile phone or a copy of our personal address book. Or otherwise, the program which enables us to find the nearest pizzeria, records and analyses the user's movements and what he or she did with his mobile phone in that location. These "extra features" allowing for the acquisition of data which is certainly not indispensable for the service and in any case not even strictly relevant, are almost never the result of "outright theft" of data by the software designer but, on the contrary, are almost always inadvertently authorised by the smartphone/tablet owner who accepts, without even reading it, the program's "user agreement".

Amongst other things, with the new generation of smartphones based on Cloud Computing, it becomes increasingly hard for users to discover whether the telephone's operating system provider or the various programs installed have made inappropriate or unauthorised access to their data, as most data is no longer stored or processed on the "telephone[19]", but remotely on the computer network[20] of the company providing the service.

[19] For example, in April 2012 an It expert discovered that some Apple devices left an unencrypted trace of the precise location of the cell phone in the time. By accessing this data it was very easy to generate a map of users' movements and activities (see for example C. Miller, "An iPhone or iPad file keeps track of all movements", http://www.theapplelounge.com/hacking-pirateria/iphone-ipad-spostamenti-privacy/). Apple justified itself claiming that this information was stored to allow for enhanced geo-localisation services. However, this file was discovered only because it was stored, unencrypted, on the cell phone. Instead, if it had been kept by Apple on the "cloud" or on the company's servers, no geek would have been able to open it and study it.

[20] The risks for privacy in remote processing models were well-known before the arrival of cloud computing. See for example: "Some Thoughts about the Social Implications of Accessible Computing", R. M. Fano, E. E. David Jr., *Proceedings of the Fall Joint Computer Conference*, 30 November 1965,

ANALYSIS AND FORECASTING SCIENCES

The amount, the pervasiveness and the constant flow of available data places us before new challenges and raises questions regarding the sciences used for studying them. What is happening to statistics? Hitherto, one of the basic concepts of statistical analysis has been the use of a "sample". Analysis of the sample allows us to study the structure of the entire population in question, starting from its small representative subset. The basis of all statistical analysis is thus "designing the sample", identifying elements in the population which, once placed together and studied, allow analysts to imagine the structure of the population in its entirety as well as its behaviour when confronted with certain stimuli. The success of this effort has always depended on the information available at the outset and, chiefly, the economic resources available for structuring the research programme.

The type of analysis may then be qualitative, quantitative or a combination of both models, but always based on a small subset of elements. For these reasons, so far no research and marketing institute has ever contemplated systematically analysing the entire statistical population to discover whether it prefers one type of chocolate or another type, if a presidential candidate is using the most convincing keywords or whether an event may adversely affect share performance on the stock exchange. Complex mathematical instruments have thus been developed to assist in the selection of the components of the sample, according to the type of strategy adopted and available resources. The sample or samples identified, are then used for studying their response to specific questions.

Instead, the start of the Big Data era and the capacity to monitor reactions to specific events in real time at the outset, allows researchers to almost completely abandon the concept of "statistical sampling" and to forget the uncertainty of those collective phenomena which in social psychology and social psychology are called, for example, "mass" and "crowd". There are no longer extemporaneous aggregates of individuals. Every single individual has become analysable both in terms of his or her uniqueness and in terms of his or her social behaviour in virtual aggregations (see social networks) or in real aggregations (as in the case of protests) with other individuals.

The current ways in which data is gathered, inter alia, make it possible to get around many of the problems which once emerged in social research. An example of this is the possibility of overcoming the many distorting biases which oc-

pp. 243-247.

cur in surveys, for example, the tendency known as “social desirability”. In fact, there are no more “questions” that the user can reply to truthfully or by seeking to adapt to what he or she imagines is the most appropriate collective trend. The “responses” are now inferred, without the consent of the person concerned, directly from what he or she reads or writes while imagining that they can hide behind a pseudonym or freedom of anonymity on Internet. Even statistical samples no longer make any sense provided the analyst has the information processing capacity and sufficient economic resources to analyse the behaviour of the entire population at any time[21].

Analysis tools provided by the most advanced statistical surveys have thus been switched to new challenges: defining the identity of those few people who cannot be directly monitored due to the fact that they do not use technology or because they endeavour to hide behind it. Another even more important new challenge is to predict and influence the behaviour of people as an individual or as a member. It is no longer of interest to discover where we are or to have the map of where we have been, but it is now more important to find out where we will be in a few minutes, hours or days, depending on the transport system used, the level of predictability of daily movements, or the purchase we have just made. It is interesting to discover who we are going to meet because they are going in the same direction after contacting us by phone, by email or chat. Or “guessing” if we intend to re-tweet a message, based on the words it contains. Statistical science can also enable us to identify those users who cannot immediately be identified by their cell phone ID, or Sim card, or MAC address of the Wi-Fi network that they connect to, or the hardware identifier of the digital camera revealed in the metadata of the photo posted online.

Thanks to special procedures known as “data enrichment”, in other words the cross-referencing of personal data which has previously been anonymised with statistical data which has maybe been geo-localised, it is possible to perform de-anonymisation[22], in other words, the reverse process. The era of multiple identities is over. That stage in Internet’s history when a person could use various nicknames, depending on the context is over. This eventuality is considered

[21] It is no coincidence that Hal Varian, Google Chief Economist, declared to The McKinsey Quarterly “*I keep saying the sexy job in the next ten years will be statisticians. People think I’m joking, but who would’ve guessed that computer engineers would’ve been the sexy job of the 1990s?*” The McKinsey Quarterly, January 2009.

[22] P. Ohm, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization”, University of Colorado Law School, UCLA Law Review, 2010, 57, p. 1701. University of Colorado Law Legal Studies Research Paper, pp. 9-12. See also: G. Wondracek, T. Holz, E. Kirda, C. Kruegel, A Practical Attack to De-Anonymize Social Network Users, Technical Report TR-iSecLab-0110-001, Technical University Vienna, Austria, 2009.

of particular concern by those civil rights associations[23] who seek to safeguard the last regulatory barriers remaining to protect privacy in a hyper technological world.

The use of these analysis instruments makes it possible to determine a person's mood at any given time[24]. It is also possible to generate an accurate profile for that person, analysing his or her sexual and political preferences in detail, pinpointing people who may influence him or her. It is even possible to generate profiles of people who are not registered on Facebook or other social networks, simply by cross-referencing information published indirectly by their network of friends, just starting with an email address, a tagged photo or any other identifying elements referring to them.

The data and technological tools available, amongst other things, are also a contributory factor in engendering a generational leap in progress in the fields of cognitive psychology and neuroscience. Until 10 years ago, in order to conduct an experiment in the field of attention or, for example, memorisation, it was necessary to organise a specialised laboratory with volunteers. Special tools, including even special eye and gaze tracker devices which identified and measured movements of the pupil were needed to analyse individuals' physiological reactions when faced with certain stimuli.

Nowadays, in order to study a person's behaviour, special equipment is no longer needed: a researcher can simply use a web cam and the other sensors with which all new tablets and smartphones are equipped. Every user can be continuously analysed in the same way as a laboratory guinea pig. As all manner of texts are now consumed directly on digital media, researchers can glean not only on which page attention was most focused[25], but on which word and for how long. It is the camera with which the technological gadget is equipped which records (ballistic type) eye movement around the image or text being observed.

[23] See for example Papers from the "e-privacy 2010 – Deanonimizzazione e Censura" [Deanonymisation and Censorship] conference, http://e-privacy.winstonsmith.info/2010/interventi.html (24/6/2012).

[24] See for example the article: R. Kotikalapudi, S. Chellappan, F. Montgomery, D. Wunsch, K. Lutzen, "Associating Depressive Symptoms in College Students with Internet Usage Using Real Internet Data", Missouri University of Science and Technology (currently being published in *Ieee Technology and Society Magazine*).

[25] In the past, attempts had been made to carry out similar analysis on browsing and the reading of texts online through monitoring the position of the mouse's cursor. These experiments were not particularly successful due to the difficulty of implementation and the users' negative reaction when they realised they were being monitored.

It is therefore possible to discover which details aroused our attention, which colour, which term, what our facial reactions are and what activity was performed immediately afterwards, for example whether the message or tweet on the subject was then posted, or whether the message was ignored[26]. This is key data for determining appropriate "collative stimuli[27]" or for gaining a better understanding of what our "executive attention[28]" is influenced by, or for determining the type of routine that we adopt.

Knowing the identity of users however, must be seen as part of a dynamic process, if the intention is to build customised messages to predict and guide their behaviour, to influence or persuade. Hence the added value of the permanent monitoring capability provided by new technologies which can accompany a person throughout the entire day.

The great technological juggernauts, these models for gathering and processing data in such an accurate way, now make it possible to monitor the cognitive and social processes which hitherto seemed far too complex to be directed in a unique way. It is as if, paradoxically, we had returned to behaviourism[29] from the early years of the 20th century, with the opportunity, this time, to determine what stimulus we must provide to get a precise response.

FOLLOW THE MONEY

To gain an understanding of which research fields are most affected by these trends, there is no need to convince secret service agencies to reveal unmentionable secrets; one need merely follow the public flow of investment funds and acquisitions around the world of Big Data.

[26] *Cfr*. M. Howard, *Sappiamo cosa vuoi [We know what you want]*, Minimum Fax, Rome, 2005. See also L. Andrews, *I know who you are and I saw what you did*, Free Press, New York, 2011.

[27] Reference is made, for example, to intense colours, irregular shapes or shapes taken out of context, improvised movements or acute sounds. Collative stimuli also capture the attention of children and are not filtered by different cultural experiences.

[28] Amongst the "executive attention" functions there is the inhibition of certain responses and the facilitation of others. It makes it possible to block information which is not needed and to enhance the availability of information which serves a particular purpose. As the researcher, Bagnara, states: "Executive attention, when used to seek information, reveals a person's psychological identity: all we need to know is what a person is paying attention to in order to reconstruct his or her identity"". S. Bagnara, "L'economia e la società dell'attenzione" [The economy and the Attention Society] in F. Butera, S. Bagnara, R. Cesaria, S. Di Guardo, *Knowledge working*, Mondadori, Milan, 2008.

[29] In 1903, the Russian researcher, Ivan Pavlov, published an important piece of research on "conditioned reflex". For example, in an experiment, he managed to induce a form of conditioning in a dog to the extent that when the animal heard a particular sound, it started to salivate, irrespective of the presence of food.

After the 2008 election campaign, at a meeting of analysts on the results achieved, Joshua Ross, one of the online communication gurus used by Barack Obama and Hillary Clinton, declared that by means of the analyses conducted by his staff, they were more or less able to predict what type of "resonance" a certain news item would have had on the social networks, chiefly Twitter, and on the web, but that it was not yet possible to accurately channel this information. In his opinion, a further pivotal point would come with greater penetration of mobile traffic. Major stock exchange investors discovered this before Obama perhaps, so that simple reputation analysis has given way to psycho-finance. Analysts are no longer only interested in what people think about a particular brand, or share, but they want to know whether consumers will buy or sell that share shortly.

In this way statistical analysis based on multi-factorial regression is combined with semantic analysis, derived from the study of applied linguistics, together with stock exchange trend analysis. The objective is no longer to find out where one is at a particular moment in time, but where the best place to be is shortly afterwards, predicting a fall or rise of a financial instrument. In order to be able to monetise this competitive advantage, the right calculation algorithms are needed together with access to data, huge computing power, and very high-speed data connections. In this regard, it is interesting to note that much attention is currently being paid to High-Frequency Trading, where these factors are intensely exploited in order to allow cyber broker software, in just a few milliseconds, to optimise trading in packets of shares[30].

Those deprived of access to data, have no access to knowledge and are unable to "foresee the future". Amongst the first investors in Facebook, prior to its controversial listing on the stock exchange[31], there were some Russian oligarchs. Google's[32] knowledge and information assets have also received much attention from Russians and Chinese. And where direct investments fail to conquer "databases", or key roles in the management of a company, hackers may make an

[30] In this sector, the "time factor" is so essential that a new trans-oceanic backbone has been laid between New York and London, high-speed connection cables which will allow investors in the two stock exchanges to gain up to 5 ms in financial transactions. The situation in the financial sector is so explosive that in March 2012, the Sec (Securities and Exchange Commission) in America decided to initiate an enquiry into brokerage firms specialised in high-frequency trading and into the way in which technological platforms used in this type of financial trading work.

[31] The results of Facebook's Ipo on the stock exchange fully confirmed the market's awareness as to the enormous value of data collected by the company. Its controversial share performance is linked primarily to speculation before and after valuation of its presumed market value.

[32] There is an interesting article written by Varian, Google's Chief Economist: H. Choi, H. Varian, "Predicting the Present with Google Trends", *The Uc Berkeley School of Information*, 18 December 2011.

attempt, carrying out very precise actions. Alongside software hacking, there are now more subtle types of "pre-emptive hardware hacking techniques[33]" implemented by private companies or state companies directly onto chips used both in military electronics and in mass-market electronics. Popular electronic devices equipped with sophisticated built-in "hidden" features providing the espionage client with secret access to a user's data any time it is needed.

The major Internet multinationals are investing huge sums in research and development into technologies for analysing data. An interesting patent registered by Google[34] relates to a technology enabling users to analyse the sounds in the background of a telephone call so as to identify the environmental conditions where the user is calling from, in order to produce more targeted advertising. According to the type of information published, the technology also includes analysis of photos and videos captured with the integrated photo camera and analysis of the speech and voice of the user, from which a special software would extract keywords in order to further enhance the effectiveness of the advertisement.

Instead, Microsoft has registered a patent[35], tied to its Kinect technology making it possible to use the tiny video-camera in its main electronic devices[36] to scan the user's facial expressions so as to interpret his or her mood[37]. If they are sad, laughing or tense. The data gathered by this technology, associated with the other information available on the user could be used to propose "empathetic" or "emotional" forms of advertising, designed to match the person's mood, maybe whilst they are visiting a website on particular illnesses. Facebook has recently finalised the acquisition of face.com, an Israeli company which deals with automatic facial recognition solutions, a technology making it possible to

[33] Two British researchers apparently recently discovered a hardware backdoor directly implemented on a Chinese microchip (proasic3 a3p250) used throughout the world inside "sensitive" devices ranging from air traffic control to monitoring military systems or high-frequency financial operations. The backdoor, as it is an integral part of the chip, cannot be removed, and would allow the key holder both to steal the contents and to take control of operations. See: S. Skorobogatov, C. Woods, "Breakthrough silicon scanning discovers backdoor in military chip" (DRAFT of 05 March 2012), *University of Cambridge*, http://www.cl.cam.ac.uk/~sps32/Silicon_scan_draft.pdf.

[34] The patent "Advertising Based on Environmental Conditions" was filed in 2008, but registered on 20 March 2012. See US patent number: 8138930 B1.

[35] The patent "Targeting Advertisements Based on Emotion" was filed in 2010, but registered on 7 June 2012. See US Patent Application 20120143693, *US Patent & Trademark office*, http://patft.uspto.gov/.

[36] PDA, *smartphone*, *notebook*, PC, videogame consoles for games like Xbox; every connected device now comes with a web cam.

[37] There are many other similar examples, such as the "MindReader" software created by a group of researchers from the Massachusetts Institute of Technology Media Lab, which analyses the position of 22 points on the face in order to determine emotions expressed by the user.

automatically give a name to the faces in the tens of millions of photos which are uploaded to the site every day. Acxiom[38] too has made huge investments to deploy its 23,000 servers in Conway, in Arkansas, where every year it analyses 50,000 billion transactions made by over 500 million consumers throughout the world.

And if the data is unavailable or insufficient, a company can go and gather it, as Google did with its vehicles for the StreetView service, whilst it took images of streets to be linked to its maps, it saw the opportunity to monitor and analyse not only strategic infrastructure but also private citizens, collecting hardware and software data on the cell phone communications network and on the Wi-Fi networks in the areas the vehicles drove through[39]. Or as the American government has done, opening 64 bases in America to launch drones[40], those silent flying robots which, though not necessarily armed, are used to monitor the geographical area with their multitude of sensors.

THE NEW LINE OF POWER

Most States are perfectly well aware of the enormous challenge they face. States can already be divided into three categories. Those which are able to monitor only local data sent, with foreign assistance. Those able to implement autonomous regional systems for monitoring and blocking data sent. Those which are able to access data and to use it to make forecasts, often simultaneously, on the behaviour of individuals or groups.

With regards to the events which have unfolded over these last three – four years and the so-called Arab Spring[41], we can find many similar cases. The majority of countries in the Maghreb and the Middle East have been capable of imple-

[38] See N. Singer, "You for Sale: Mapping, and Sharing, the Consumer Genome", New York Times, 16/6/2012, http://www.nytimes.com/, (24/6/2012).

[39] If this type of operation had been conducted during the Cold War it would probably have led to life imprisonment or capital punishment for the perpetrators for reasons of espionage or high treason. Now in the era of global connection, this massive collection of confidential data has been trivially dismissed by most people as a mere commercial operation.

[40] A study carried out by the no-profit group, Public Intelligence, indicates the presence in the United States of 64 bases used to launch drones. According to privacy organisations they are used for spying on citizens, "violating limits for airborne monitoring and citizens' rights" and privacy". See: Public Intelligence, DoD Current and Future Us. Drone Activities Map, http://publicintelligence.net/dod-us-drone-activities-map/ as well as "Talk of drones patrolling Us skies raises fear Americans' privacy may be at risk", *Associated Press*, 19/6/2012, www.washingtonpost.com.

[41] See F. Vitali, "The evolution of the infosphere. New sources for news stories – networked journalism_and social networks", in *Nomos & Khaos –2010-2011 Nomisma Report on economic and strategic prospects*, Agra, Rome, 2011, p.189-202.

menting forms of monitoring and blocking telephone and Internet communications thanks to the technical support and technological equipment provided by a number of European countries as well as by the Americans. These are technologies which have enabled governments to monitor people in an extremely invasive but unsophisticated manner and are more similar to methods adopted by Stasi in the former East Germany.

Even Iran, which boasts autonomous economic and technological resources, a generation of engineers and technicians which is considerably more advanced than in neighbouring countries, and is capable of carrying out sophisticated hacking operations on an autonomous basis, is unable to go beyond the traditional Big Brother approach.

The system for monitoring and blocking specific words, implemented by Iran in respect of its Internet communications, similar to the Chinese system, often commits obvious, very trivial errors. Amongst these there is the case of an automatic censoring episode in May 2012[42] which apparently affected the country's Supreme Leader, Ayatollah Ali Khamenei. Apparently the filtering system blocked the very fatwa with which Khamenei denounced the systems enabling Iranians to circumvent the block on "blasphemous" sites imposed by the regime. In fact, the document published by the supreme leader contained the term "anti-filtering", one of the prohibited words which is automatically blocked by the security system, precisely because it is often sought by dissidents seeking ways[43] to circumvent the domestic censors.

In Egypt, analysts have noted the use of more primitive as well as more advanced instruments. Mubarak relied on technologies which were similar to those used in Libya or Syria and he managed to monitor the population quite effectively. But others in the country had managed to circumvent monitoring and to anticipate events, aware that the "wave" of revolt was about to strike. They knew where and how to take action, what words to use, what tools to use to coordinate young people on Internet together with those who were not online. One of these key individuals was at the very heart of American "knowledge": Wael Ghonim, then head of marketing for Google in the Middle East and Asia. In his book of

[42] This interesting piece of news on the "censor" who was censored by his own system went global on 12 May 2012. The account, taking into due consideration the fact that the situation requires a certain dose of caution due to possible propaganda or counter propaganda purposes, appears to be credible as it was reported by information sources close to Khamenei, i.e. Tabnak. *Cfr.* http://basijbabeanar.mihanblog.com/post/257 (24/6/2012) and *cfr.* http://www.asriran.com/fa/news/212662 (24/6/2012).

[43] For example, the use of encrypted transmissions, VPN (virtual private networks) or proxies.

memoirs on the Arab revolution he wrote: *"My skills and experience were enriched by Google. And I marveled at its culture, which was all about listening to others. Data and statistics ruled over opinions. Most of the time, authority belongs to the owners of information, or as W. Edwards Deming once said," In God we trust; all others must bring data*[44]*".*

The Western and Asian powers are generally at the second level, having autonomously put in place a host of tools for monitoring Internet. Often however they are hamstrung by the fact that they must respect democratic constitutions and have established institutions which are accountable to the nation's citizens. Any form of monitoring must be justified in accordance with specific, formally democratic objectives, such as the fight against paedophilia, terrorism, protection of copyright or the promotion of international trade and "national security". All these purposes are legitimate but they have frequently crossed the fine line separating them from constitutionally protected rights such as the freedom to obtain information and provide information, freedom of speech, confidentiality of correspondence. In the United Kingdom, Australia and Italy, just to give a few examples, there are almost daily discussions on new national and international bills, such as the recent British Communications Data Bill, whose final purpose is to intercept any form of electronic communications[45].

France has set up an authority tasked with monitoring and punishing the exchange of files covered by copyright: Hadopi (Haute autorité pour la diffusion des oeuvres et la protection des droits sur l'Internet). France is able to operate independently, throughout its territory. China too is able to block almost all "banned" information circulating only in its "portion of Internet"[46].

France and China[47] can monitor data transmission through Deep Packet Inspection[48] tools. They have research centres which are able to cross reference Pattern-Based Aggregation algorithms, Sentiment Classification algorithms, ge-

[44] G. Wael, Revolution 2.0, Harper Collins Publishers, London, 2012, p.26.

[45] It was none other than the Englishman, George Orwell, the pseudonym for Eric Arthur Blair (1903–1950), one of the most oft-cited defenders of privacy, who pointed out that one of the key elements distinguishing democracies from dictatorships is the fact that they protect and respect citizens' privacy, based on the assumption that it is not necessary to monitor citizens, check them or spy on them unless there are indications of guilt in respect of specific offences. Actually, the Big Brother concept of "Orwellian control" was named after this English writer.

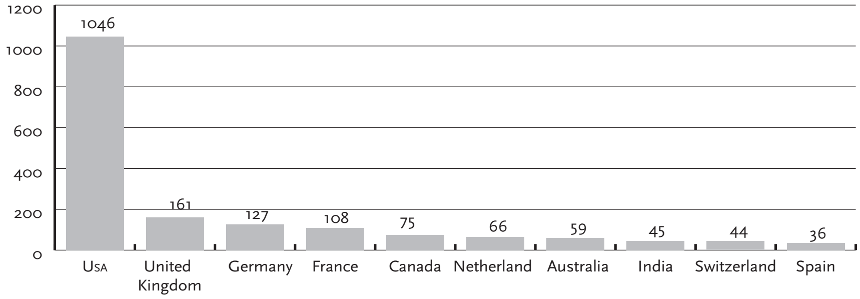
[46] China has already successfully experimented with hacking techniques to redirect the bulk of global Internet traffic through its servers, seriously alarming the Pentagon.

[47] This pairing of nations naturally provides no combined assessment as to their completely different monitoring activities.

[48] This is a procedure for analysing the content of data packets which transit within a network.

netic algorithms and neural networks. They have advanced statistical capabilities, but lack a sufficiently broad network of global "sensors" to enable them to study events unfolding throughout the world in real time. They lack the database and the calculation capability to be able to efficiently transform this information into strategic actions having geopolitical and geoeconomic value. They are able to conduct specific data mining[49] actions on information which is freely accessible on Internet, advanced Open Source Intelligence actions, but they lack the computational power enabling them to carry out forecasts in the same way as the American State and private companies are able to. If one looks at the distribution map for the main global data centres, the technological and informational gap between the United States and the rest of the world appears even more striking (see figure 2.8.1 and figure 2.8.2). The leading country in terms of the number of main dedicated data centres is the United States[50] with 1,046 centres for storing and processing data. The United States is followed by the United Kingdom with 161 centres, Germany with 127; Russia has only 28 and China 9.

Figure 2.8.1 The top ten countries by number of business data centres



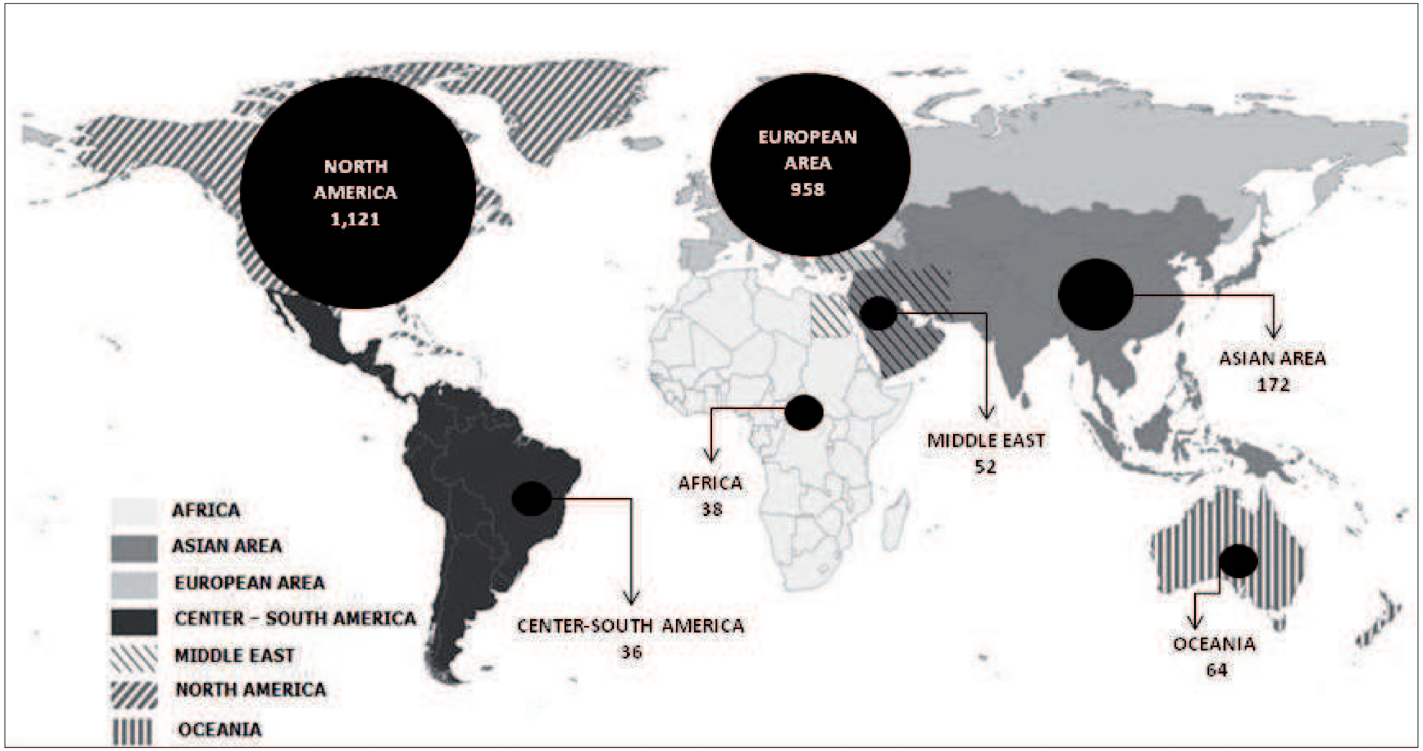
Source: Elaborated by F. Vitali on the basis of http://www.datacentermap.com data from14/6/2012.

This data is incomplete by reason of the fact that it does not include cloud computing centres or multi-functional data processing centres; neither does it compare the importance of each specific data centre, in other words its capacity to store and process data. The figures also fail to include centres linked to the various domestic and external security agencies. They do however give immediate insight into a country's superiority over another one in this industrial, strategic sector.

[49] To understand data mining techniques in greater detail one can refer to the papers of the *Proceedings of the International Conference on Data Mining* (DMIN'11), CSREA Press, Editor Robert Stahlbock; 2011. http://www.dmin--2011.com/.

[50] See: http://www.datacentermap.com/datacenters.html del 14/6/2012.

Map 2.8.1 World Map of Commercial Data Centres - Geographic location of the world's main business data centres*



* The Middle East includes the data centres in the following countries already considered in the other geographical areas: Saudi Arabia, Bahrain, Cyprus, Egypt, United Arab Emirates, Jordan, Iran, Iraq, Israel, Kuwait, Lebanon, Oman, Palestine (present in the database) Qatar, Syria, Turkey and Yemen.

Source: Elaborated by F. Vitali on the basis of http://www.datacentermap.com data from14/6/2012.

THE FUTURE SEEN BY THE AMERICANS

The possibility of predicting future "social political" events has always been of great interest for the Americans, for their companies and government and semi-government agencies. The FUTUREMAP[51] Project (futures Markets Applied to Prediction) funded by DARPA (Defence Advanced Research Projects Agency) was amongst those of greatest interest in 2001.

The Defence Department Agency had devised a sort of "betting system" regarding international events. "Players" were supposed to lay wagers as to the likelihood that political and economic events such as terrorist attacks, assassinations of leaders and key figures and changes to leadership would occur in the Middle East. This project was underpinned by the idea that the economic stimulus provided by betting would have allowed useful information to surface, such information being known to insiders who were aware of confidential information, possibly on future terrorist attacks. The experiment was rapidly shut down after senators and experts complained, contending that this type of incentive could have given rise to a sort of self fulfilling prophecy, encouraging unscrupulous people to organise terrorist attacks only to win the bet, rather than contributing to forecast these events.

There are currently numerous monitoring and event forecasting projects which have been implemented by the American government after this first initial experience and in the aftermath of the 11 September 2001 attacks. They are predominantly based on the potential yielded by social networks and possible "information enrichment" of information freely available on Internet with information contained in American super-databases. In January 2009, Obama inaugurated the new Social Networking Monitoring Centre (SNMC)[52], promoted by the Department of Homeland Security. In February 2010, IARPA (Intelligence Advanced Research Projects Activity) funded a project named Crowdsourcing for Intelligence to develop forecasting scenarios based on analysing the perceptions and mood of Internet users[53]. It was again IARPA which contributed to the creation of the Centre for Collective Intelligence (CCI) at the MIT (Massachusetts Institute of Technology). In 2011 it was DARPA which launched the Social Media in Strategic Communication (SMISC) programme, a call for tender for research projects to

[51] *Crf.* Y. Puong Fei, "Using Prediction Markets to Enhance US Intelligence Capabilities", *CSI Publications*, vol. 50, n. 4, 2006, https://www.cia.gov/.
[52] See https://www.eff.org/files/filenode/social_network/DHS_SNMC_Inauguration_monitoring.pdf.
[53] See also A. Teti,"Dai 'think tanks' al 'Crowdsourcing for Intelligence'" [From 'think tanks' to 'Crowdsourcing for Intelligence'], Gnosis, vol 1, 2012.

fund "revolutionary"[54] projects in the field of strategic communications on social networks, developing new sciences and technologies, with the aim of "creating and averting unexpected events in the strategic sphere"[55]. These are the "highly improbable events described by Nassim Nicholas Taleb, the author of "The Black Swan"[56], one of the leading experts in the subject of analysing the impact of rare, highly unlikely occurrences. In the era of interconnection, social networks and global finance, black swans never arrive on their own, but in "formation": episodes, behaviours which grouped together generate social political and economic shocks, events which "destroy" the status quo.

American universities are also bolstering their presence in this sector. The San Diego Supercomputer Centre (SDSC) at the University of California, for example, has launched a new "Centre of Excellence" which is specialised in analysing Big Data. It will concentrate on the Predictive Analytics Centre of Excellence Program (PACE), with the objective of developing and distributing a complete suite of cyber infrastructures to accelerate research and training into predictive data analysis, ranging from interpreting economic to health phenomena and including pharmaceutical products, financial services, insurance and telecommunications sectors. Naturally, the project is also open to cooperation and projects set up in the industrial and government sector.

But the San Diego technologies centre, including the Gordon supercomputer, will certainly not be able to compete with the performance levels at the new mega-datacentre, possibly the largest in the world, which the NSA (National Security Agency) is scheduled to complete at Bluffdale in Utah[57] by 2013.

American investments in the area of gathering and analysing data will be even more useful for global strategic purposes within 3 to 4 years, when the penetration of mobile communication instruments and devices in the East and in the

[54] "Proposed research should investigate innovative approaches that enable revolutionary advances in science, devices, or systems".

[55] The slogan is *"Creating and Preventing Strategic Surprise"* with the objective of "developing a new science of social networks built on the basis of emerging technology". Many specific objectives are indicated: "1. Detect, classify, measure and monitor (a) training, development and dissemination of ideas and concepts (including memes), as well as (b) vexatious or misleading messages and misinformation. 2. Recognise the structure of campaigns of persuasion and operations designed to exert influence developed on social media and in online communities. 3. Identify the key players and objectives, measure the effects of campaigns of persuasion. 4. Counter operations identified and carried out by the enemy to exert influence by means of specific messages". See: Social Media in Strategic Communication (SMISC) in FedBizOpps.Gov, https://www.fbo.gov/, or in http://www.darpa.mil/.

[56] N. N. Taleb, The Black Swan: The Impact of the Highly Improbable, Random House, New York, 2007.

[57] Vedi http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1.

developing countries will be even more marked. According to the Cisco report on mobile data traffic[58], the flow of mobile data in the Middle East and Africa, between 2011 and 2016, will increase 36 fold, with a CAGR (Compound Annual Growth Rate) of 104%. The Asia-Pacific area will follow with growth rates of 84%, followed by Central and Eastern Europe with 83%. Latin America (+79%) and North America (+75%) will expand at a slower rate. The area which in percentage terms will see the slowest growth will be Western Europe, which will record a CAGR of 68% (see Table 2.8.2).

Table 2.8.2. Global mobile data traffic. 2011-2016

	2011	2012	2013	2014	2015	2016	CAGR* 2011-2016
BY APPLICATION CATEGORY (TB PER MONTH)							
Data	174,942	329,841	549,559	864,122	1,349,825	2,165,174	65%
File sharing	76,764	114,503	154,601	204,617	261,235	361,559	36%
Video	307,869	736,792	1,545,713	2,917,659	4,882,198	7,615,443	90%
VoIP	7,724	10,327	12,491	15,485	22,976	35,792	36%
Gaming	6,957	13,831	24,388	40,644	77,568	118,330	76%
M2M	23,009	47,144	92,150	172,719	302,279	508,022	86%
BY DEVICE TYPE (TB PER MONTH)							
Nonsmartphones	22,686	55,813	108,750	196,262	357,797	615,679	94%
Smartphones	104,759	364,550	933,373	1,915,173	3,257,030	5,221,497	119%
Laptops and netbooks	373,831	612,217	917,486	1,340,062	1,963,950	2,617,770	48%
Tablets	17,393	63,181	141,153	300,519	554,326	1,083,895	129%
Home gateways	55,064	108,073	180,562	267,545	376,494	514,777	56%
M2M	23,009	47,144	92,150	172,719	302,279	508,022	86%
Other portable devices	525	1,460	5,429	22,966	84,204	242,681	241%
BY REGION (TB PER MONTH)							
North America	118,972	259,283	493,323	844,416	1,304,870	1,964,477	75%
Western Europe	180,370	365,722	683,843	1,160,571	1,704,596	2,437,922	68%
Asia Pacific	205,624	437,601	831,616	1,502,748	2,614,055	4,322,879	84%
Latin America	40,171	77,242	145,794	267,327	455,463	737,808	79%
Central and Eastern Europe	34,317	67,722	133,716	252,930	439,143	706,469	83%
Middle East and Africa	17,810	44,868	90,610	187,254	377,953	634,765	104%
TOTAL (TB PER MONTH)							
Total Mobile Data Traffic	597,266	1,252,438	2,378,903	4,215,246	6,896,080	10,804,321	78%

* CAGR (Compound Annual Growth Rate). It is a geometric mean of annual growth rates.
The Cisco VNI Global Mobile Data Traffic Forecast relies in part upon data published by Informa Telecoms and Media, Strategy Analytics, Infonetics, Ovum, Gartner, IDC, Dell'Oro, Synergy, ACG Research, Nielsen, comScore, Arbitron Mobile, Maravedis and the International Telecommunications Union (ITU).
Source: *The Cisco VNI Global Mobile Data Traffic Forecast*, Cisco, February 14, 2012.

In expectation of further growth in the use of smartphones and their global penetration, "the exchange of data" between American security and intelligence agencies and the giant multinationals will be further bolstered. In March 2012

[58] Cisco, White Paper, 14/2/2012, op.cit.

Regina Dugan, the first woman appointed to head Darpa, after three years in the job, left her position as head of technological projects at the Pentagon to take up the position of "Senior Vice President – Advanced Technology and Projects" at Motorola, the Tlc and cellphones company recently acquired by Google.

CONCLUSIONS

In the course of the Cold War and the confrontation between the Western and the Russian blocs, two technological leaps, more than any other, sealed the Soviet Union's fate: the conquest of space, starting with Sputnik and culminating in the moon landing, and investments in so-called "Star Wars". Making a huge effort, the Americans succeeded in opening up a scientific and technological gap which for years was impossible for the other global powers to close. The success of this experience had repercussions not only in the military sector, but also in private industry, with spin-offs of capabilities and instruments.

This gap, which in recent years had shrunk, has once more started to widen again thanks to investment in Big Data. The new technological capabilities and accumulated "knowledge", through the massive gathering of data, make it possible both to alter the balance of power between States and to reshape the borders between territories in accordance with parameters which were totally unknown to the politicians and geographers of the 19th and 20th centuries: "virtual" maps, based on measuring relations, exchanges, movements, the sharing of interests and centres of influence which are much more real and current than the existing borders. The leader of this new global order is still the United States of America. Unless Taleb's "Black Swan" arrives on the scene to unleash major changes in the technological scenario, in particular relating to "private" companies which are set to handle and access user data, the United States is bound to further increase its capacity to monitor and above all analyse, forecast and manipulate "strategic behaviour"[59] on a global scale, in respect of individuals and entire populations, including those not yet reached by smartphones and by other "enabling technologies". This activity will continue to be supported, with regard to gathering data, by the old allies in the echelon system, with Britain as the bridgehead for European and African data, with the addition of Australia, New Zealand and Singapore for the Southeast Asian sector, with a more marginal role for Canada, should its most important mobile phone company, Blackberry, be forced to quit the telephone market, and possibly with an indirect role for Italy as well, by reason of the fact that across Italy there are crucial data transmission grids running to the Middle East and Asia.

[59] In memory of key research carried out by Ferrante Pierantoni, precursor of the "black swans".

The American State Department has just announced a five-year agreement with Amazon for the purchase of a significant number of Kindles, a reader of books and other electronic material, equipped with over $10 million in e-books, videos and other digital products which quite conceivably will be available on the Amazon Cloud. These tablets should be distributed in libraries, public reading rooms and cultural centres throughout the world, with the idea of immediately reaching six million young people outside the United States.

This new public diplomacy operation has prompted misgivings on the part of many experts such as Morozov[60] who are worried that American activism in the digital sector may be a contributory factor in the further politicisation of the digital world and Internet in general, urging Russia, China and other states to raise additional barriers against free access to Internet and implementing counter-propaganda operations.

Who knows whether the American government has decided to use the new Kindles merely to "inform" foreign youths, or whether it has also put instruments in place – especially involving psychological analysis and cognitive ergonomic analysis – to study, for example, the way in which users read and write, gathering data which could, for example, be useful for implementing future communication and strategic influence operations. Hillary Clinton and President Obama are engaged in a worldwide battle to foster freedom to access Internet, freedom of information and expression and the fight against censorship. And yet it is the United States which is leveraging its enormous technological supremacy to enable operations which make George Orwell's nightmares seem like trivial tales from the distant past. Furthermore if the United States presses ahead in this direction, the greater will be the risk of losing credibility, and thus the capacity to influence others throughout the world, and even worse, the risk of forgetting the elementary rules of democratic life which they claim to promote.

[60] E. Morozov, "La Casa Bianca alleata di Amazon: gli e-book invaderanno il mondo" [The White House as Amazon's ally: e-books will invade the world], Corriere della Sera, 22/6/2012.

Industry Minister in 1995. He was a member of ministerial commissions for energy policy in 2003 and 2005. He has published approximately 60 articles in journals specialising in the energy and oil sectors, and since 2000 has been an editorialist for Il Sole 24 Ore on energy problems. He is a contract Professor at Bologna University and at Milan Politecnico University.

Francesco Vitali is an expert in Information & Communication Technologies and strategic studies. After studying at university in Italy and England, he specialised at the University of Texas in Austin (Usa). He has worked for the Rai television station on various investigatory and in-depth analysis programmes, for the Prime Minister's Office, for consultancy companies and in the marketing and communications sectors. He has been an advocate of strategic studies at Luiss Guido Carli and Senior Research Fellow for the Economic Geopolitics Study Centre. He currently works with the Data Protection Authority and is a member of the Board of Teaching Staff for the research doctorate in Geopolitics and Economic Geopolitics at the Marconi on-line University in Rome.

In ancient Greek, the word "nomisma" means the real value of things. It is in this spirit that Nomisma has been operating for more than 25 years in monitoring and analysing local, national and international economic trends, with particular attention to concrete developments in the real economy. Nomisma is recognised as one of the leading private research institutes at national and European levels.

As an initiative promoted by Nerio Nesi and Francesco Bignardi, then president and managing director of BNL (Banca Nazionale del Lavoro), Nomisma was founded in Bologna in 1981 as a joint stock company, which gained the support of major Italian and some international banks and entrusted Romano Prodi with the task of organising scientific research activities.

Besides its traditional role as a research institute, Nomisma has a substantial track record in the provision of policy advice to national and regional governments and administrative bodies, devoting particular attention to the identification and understanding of their needs by developing models and professional tools to analyse and study economics.

Nomisma's development has reflected its interdisciplinary vision of the economy. The company comprises several research and consultancy units, each specialising in different fields (agriculture and agri-food, industrial and territorial policy, real estate and urban studies, international cooperation programmes, local public services, energy and sports) and operating autonomously, but able to work together on the basis of an integrated approach. This allows the company to employ a cross-sectoral and flexible, yet targeted approach in addressing the requirements of its varied clientele.

Nomisma is one of the leading companies operating in the market of economic research at national and European levels. Its strength lies in the internal expertise of around 60 researchers and an extensive network of national and international partners.